

GAO

Report to the Honorable Wm. Lacy Clay,
House of Representatives

May 2005

INFORMATION SECURITY

Federal Agencies Need to Improve Controls over Wireless Networks



G A O

Accountability * Integrity * Reliability

Highlights of [GAO-05-383](#), a report to the Honorable Wm. Lacy Clay, House of Representatives

Why GAO Did This Study

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

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

What GAO Recommends

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

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

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

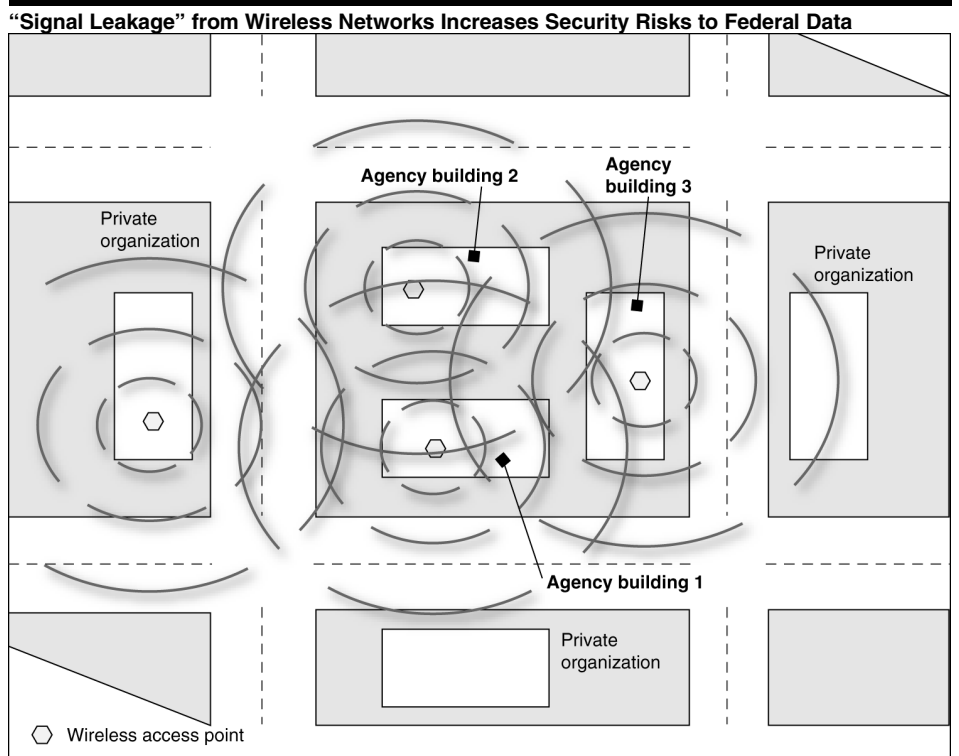
INFORMATION SECURITY

Federal Agencies Need to Improve Controls over Wireless Networks

What GAO Found

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

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



Source: GAO.

Contents

Letter

Results in Brief	1
Background	3
Wireless Networks Provide Benefits and Present Challenges to Agencies	8
Controls Can Mitigate Wireless Network Security Challenges	12
Federal Agencies Lack Key Controls for Securing Wireless Networks	16
Selected Agencies Did Not Implement Wireless Networks Securely	18
Conclusions	19
Recommendation for Executive Action	20
Agency Comments	21

Appendixes

Appendix I: Objectives, Scope, and Methodology	23
Appendix II: Contacts and Staff Acknowledgments	26

Tables

Table 1: Examples of Wireless Network Security Threats	9
Table 2: Policies for Managing Wireless Network Risks	13
Table 3: Examples of Wireless Security Tools That Can Be Configured to Meet Agency Policies	14

Figures

Figure 1: Example of a Wireless Infrastructure Mode Network	4
Figure 2: Example of Wireless Ad Hoc Networking	5
Figure 3: Wireless Networks Detected in a Section of Downtown D.C.	6
Figure 4: Example of Signal Leakage at Federal and Private Facilities	11

Abbreviations

CFO	Chief Financial Officer
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, D.C. 20548

May 17, 2005

The Honorable Wm. Lacy Clay
House of Representatives

The use of wireless networks is increasingly popular among personal, academic, business, and government users. Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and personal digital assistants. Spurred on by increasing bandwidth and decreasing costs of laptops and mobile computing, wireless networks are becoming widely available in “hotspots” in cafes, retail centers, hotels, schools, airports, and businesses.

Wireless networks can offer federal agencies many potential benefits—including flexibility and ease of installation. However, wireless networks are widely known to be vulnerable to attack or compromise, and as a result they can pose significant information security risks to agencies. Various procedures and tools are available to secure these networks for use within federal agencies.

In response to your request, our review had the following objectives: (1) describe the benefits and challenges associated with securing wireless networks, (2) identify the controls (policies, practices, and tools) available to assist federal agencies in securing wireless networks, (3) analyze the wireless security controls reported by each of the 24 agencies covered by the Chief Financial Officers (CFO) Act of 1990,¹ and (4) assess the security of wireless networks at the headquarters of 6 federal agencies in Washington, D.C.

We performed our work in the Washington, D.C., metropolitan area from September 2004 to March 2005, in accordance with generally accepted government auditing standards. Appendix I provides further detail about our objectives, scope, and methodology.

Results in Brief

The availability of wireless networks presents federal agencies with both opportunities and challenges. These networks offer agencies increased flexibility and ease of installation over their traditional wired networks.

¹31 U.S.C. 901(b).

However, agencies face unique challenges securing wireless networks—such as protecting against wireless network attacks, establishing physical control over wireless-enabled devices, and preventing unauthorized deployments of wireless networks.

Federal agencies can implement various controls, including policies, practices, and tools, to secure their wireless networks. For example, wireless network security can be enhanced by establishing comprehensive information security policies that address wireless security, configuring security tools to meet defined agency policy requirements, implementing comprehensive wireless monitoring programs, and training employees and contractors on wireless policies. Without effective security controls for wireless networks, agency information is at risk of unauthorized disclosure, modification, or destruction.

Despite the risks associated with wireless networks, federal agencies have not fully implemented key controls for securing these networks. For example, nine federal agencies reportedly have not issued policies on wireless networks. In addition, 13 agencies reported not having established requirements for configuring or setting up wireless networks in a secure manner. Further, the majority of federal agencies lack wireless network monitoring to ensure compliance with agency policies, prevent signal leakage, and detect unauthorized wireless devices. Finally, 18 agencies do not provide training programs in wireless security for their employees and contractors.

The wireless networks at the six federal agencies we tested were not secure. Specifically, we were able to detect wireless networks at each of the agencies from outside of their facilities. Wireless-enabled devices were operating with insecure configurations at all six of the agencies. For example, in one agency we found over 90 laptops that were not configured appropriately. Finally, there was unauthorized wireless activity at all of the agencies that had not been detected by their monitoring programs.

We are recommending that the Director of the Office of Management and Budget (OMB) instruct agencies to ensure that wireless network security is addressed in their agencywide information security programs. OMB officials generally agreed with the report's content and identified planned actions to address the recommendation.

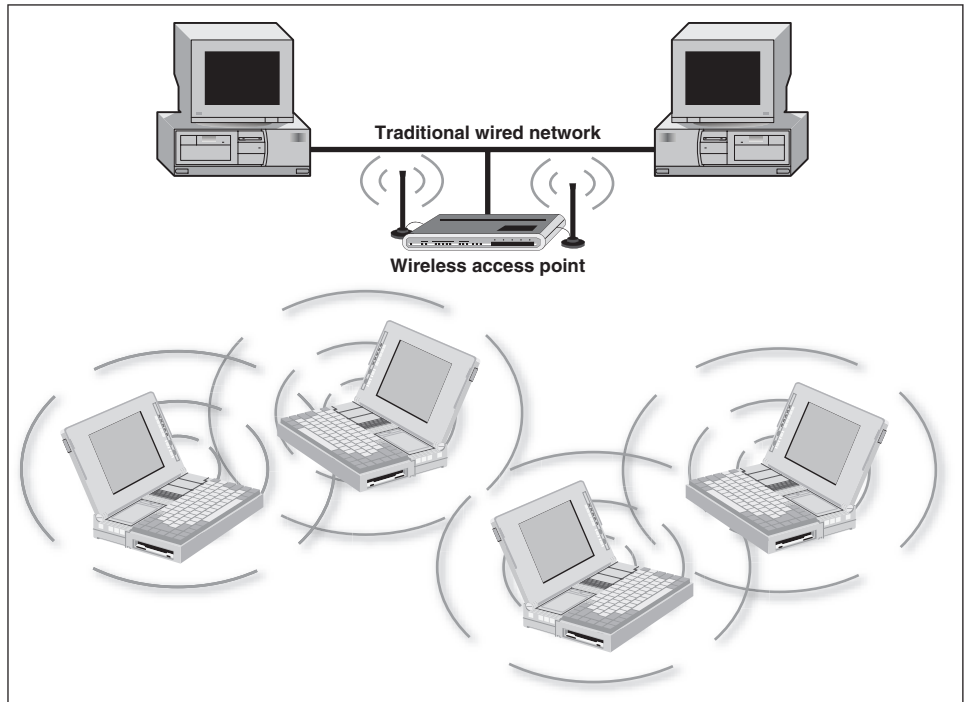
Background

Wireless networks extend the range of traditional wired networks by using radio waves to transmit data to wireless-enabled devices such as laptops and personal digital assistants. Wireless networks are generally composed of two basic elements: access points and other wireless-enabled devices, such as laptops. Both of these elements rely on radio transmitters and receivers to communicate or “connect” with each other. Access points are physically wired to a conventional network, and they broadcast signals with which a wireless device can connect. The signal broadcast by the access point at regular intervals—several times per second—includes the service set identifier, as well as other information. Typically, this identifier is the name of the network. Wireless devices within range of the signal automatically receive the service set identifier, associate themselves with the wireless network, and request access to the local wired network.

Wireless networks are characterized by one of two basic topologies, referred to as infrastructure mode and ad hoc mode.

- **Infrastructure mode**—By deploying multiple access points that broadcast overlapping signals, organizations can achieve broad wireless network coverage. Commonly used on campuses or in office buildings, 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).

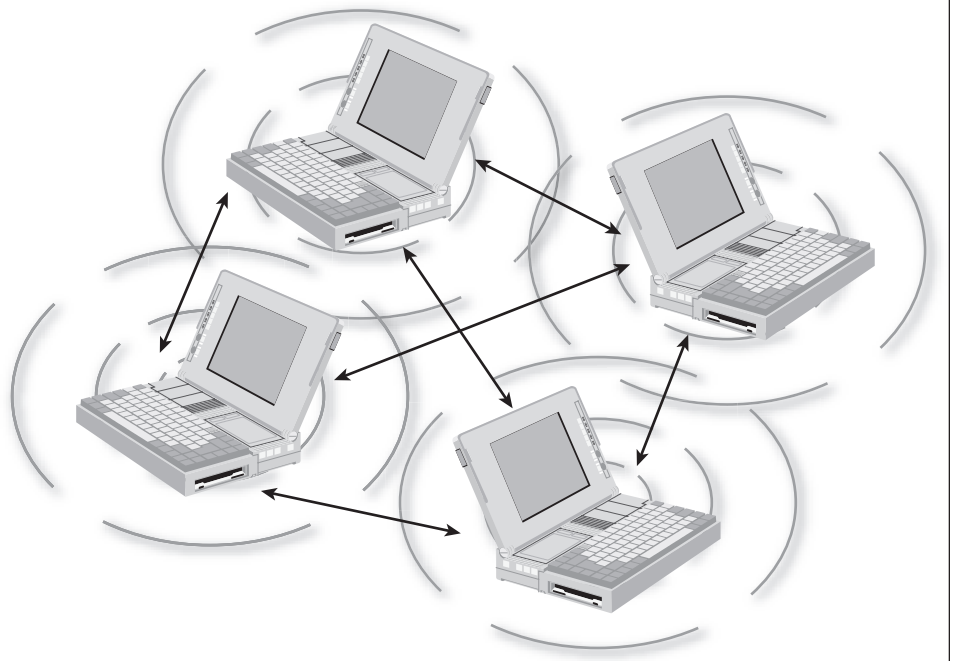
Figure 1: Example of a Wireless Infrastructure Mode Network



Sources: GAO analysis, Microsoft Visio, and Art Explosion.

- **Ad hoc mode**—This type of wireless topology allows wireless devices that are near one another to easily interconnect. In ad hoc mode laptops, desktops, and other 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

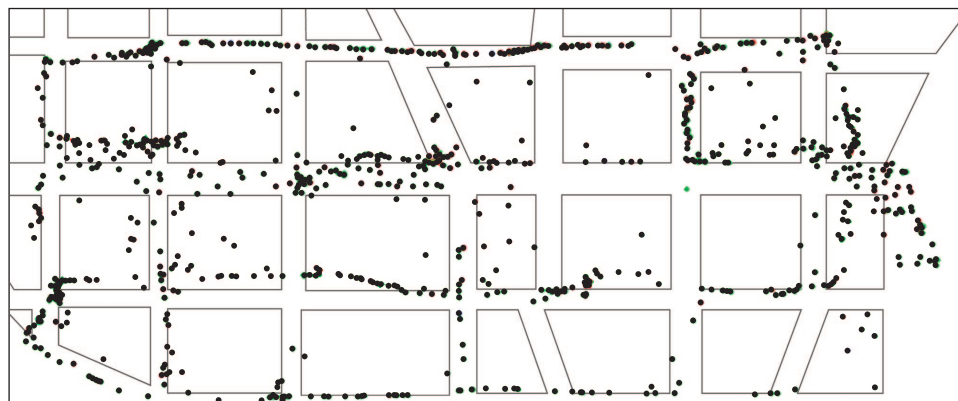


Sources: GAO analysis, Microsoft Visio, and Art Explosion.

Increased Speed Fueled the Growth of Wireless Networks

The increased speed of wireless networks has helped to fuel their growth and popularity. The growing popularity of wireless networks can be easily witnessed in urban environments. For example, during a recent test in Washington, D.C., we drove around 15 square blocks and, using a commonly available wireless network scanner, we detected over a thousand wireless networks. Figure 3 depicts a sample of the saturation of wireless networks we detected during our brief test.

Figure 3: Wireless Networks Detected in a Section of Downtown D.C.



Source: GAO.

Wireless networks offer connectivity without the physical restrictions associated with building wired networks. Though generally developed as an extension to an existing wired infrastructure, a wireless network may be stand-alone as well. The key reason for the growth in the use of wireless networks is the increased bandwidth made possible by the 802.11 standard and its successors. The implementation of the 802.11 family of standards increased the data transfer rates offered by wireless networks, making them comparable to those available in the wired environment.

The 802.11 standard was first approved by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. IEEE's goal was to develop and establish a technology standard that insured global interoperability among wireless products, regardless of their manufacturers. This initial wireless standard was useful for certain applications, but the data transfer rate it specified was far slower than that of wired networks. Responding to the data transfer rate limitations set by the initial standard, the IEEE released several additional standards with the intent of increasing the transfer rates and making wireless functionality comparable to that of wired networks. The significant increases in data transfer rates of the new standards, coupled with the availability of affordable wireless-enabled devices, contributed to the rapid adoption of wireless networks.

Federal Laws and Guidance Provide a Framework for Wireless Security Policies

The Federal Information Security Management Act (FISMA)² 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. FISMA gives OMB many responsibilities for overseeing the agency information security policies, including developing and overseeing the implementation of policies and standards for information security; requiring agencies to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, modification, or destruction of federal information and information systems; and coordinating the development of standards and guidance. OMB annually reports to Congress on the progress of agencies' compliance with FISMA.³ Accordingly, agencies need to evaluate the risks and develop policies for emerging technologies such as wireless networks.

The National Institute of Standards and Technology (NIST) develops standards that agencies are required to follow and guidelines recommending steps that agencies can take to protect their information and information systems. In November 2002, NIST released *Wireless Network Security: 802.11, Bluetooth and Handheld Devices (Special Publication 800-48)*, which is intended to provide agencies with guidance for establishing secure wireless networks. The guidance recognizes that maintaining a secure wireless network is a continuous process requiring additional effort beyond that required to maintain other networks and systems. Accordingly, NIST has recommended that federal agencies

- perform risk assessments and develop security policies before purchasing wireless technologies and anticipate that their unique security requirements will determine which products should be considered for purchase;
- wait to deploy wireless networks for essential operations until after agencies have fully assessed the risks to their information and system operations and have determined that they can manage and mitigate those risks;

²44 U.S.C. §3544(b).

³44 U.S.C. §3543(a)(8).

-
- assess risks, test and evaluate security controls more frequently than they would on a wired network.

Currently, NIST is in the process of developing a follow-up to this publication, which will reflect the recent updates to the 802.11 network standards.

Wireless Networks Provide Benefits and Present Challenges to Agencies

Wireless networks offer federal agencies two primary benefits: increased flexibility and easier installation. Because wireless networks rely on radio transmissions, federal employees can work in a variety of ways. For example, users can take laptops to meetings, create ad hoc networks, and collaboratively develop products or work on projects. In addition, if a federal agency has installed a wireless infrastructure, users with wireless-enabled devices can work throughout the agency's facilities without having to be in a particular office. Finally, an agency employee traveling with a wireless-enabled device may be able to connect to an agency network via any one of the many public Internet access points or hotspots found in hotels or in commercial, retail, or transportation centers. This ability to connect to the agency's systems via wireless networks can increase employee productivity.

Ease of installation is commonly cited as a key attribute of wireless networks. Generally, deployments of wireless networks do not require the complicated undertakings that are associated with wired networks. For example, the ability to "connect" the network without having to add or pull wires through walls or ceilings or modify the physical network infrastructure can greatly expedite the installation process. As a result, a wireless network can offer a cost-effective alternative to a wired network. In addition to their increased ease of installation, wireless networks can be easily scaled from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area. 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.

Wireless Networks Present Additional Challenges for Federal Information Security

Wireless networks face all of the information security risks that are associated with conventional wired networks, such as worms and viruses, malicious attacks, and software vulnerabilities, but there are significant challenges that are unique to the wireless network environment. In implementing wireless networks, federal agencies face three overarching

Protecting Against Wireless Network Security Exploits is Challenging

challenges to maintaining the confidentiality, integrity, and availability of their information:

- protecting against attacks that exploit wireless transmissions,
- establishing physical control of wireless-enabled devices, and
- preventing unauthorized wireless deployments.

Protecting against wireless network security attacks is challenging because information is broadcast over radio waves and can be accessed more easily by attackers than can data in a conventional wired network. For example, wireless communications that are not appropriately secured are vulnerable to eavesdropping and other attacks. Poorly controlled wireless networks can allow sensitive data, passwords, and other information about an organization’s operations to be easily read by unauthorized users. In addition, wireless networks can experience attacks from unauthorized parties that attempt to modify information or transmissions. Table 1 provides examples of the different types of attacks that can threaten wireless networks and the information that they are transmitting.

Table 1: Examples of Wireless Network Security Threats

Eavesdropping	The attacker monitors transmissions for message content. For example, a person listens to the transmissions on a network between two workstations or tunes in to transmissions between a wireless handset and a base station.
Traffic analysis	The attacker, in a more subtle way, gains intelligence by monitoring transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages among communicating parties.
Masquerading	The attacker impersonates an authorized user and exploits the user’s privileges to gain unauthorized access in order to modify data.
Replay	The attacker places himself between communicating parties, intercepting their communications, and retransmitting them; this is commonly referred to as “Man-in-the-Middle.”

(Continued From Previous Page)

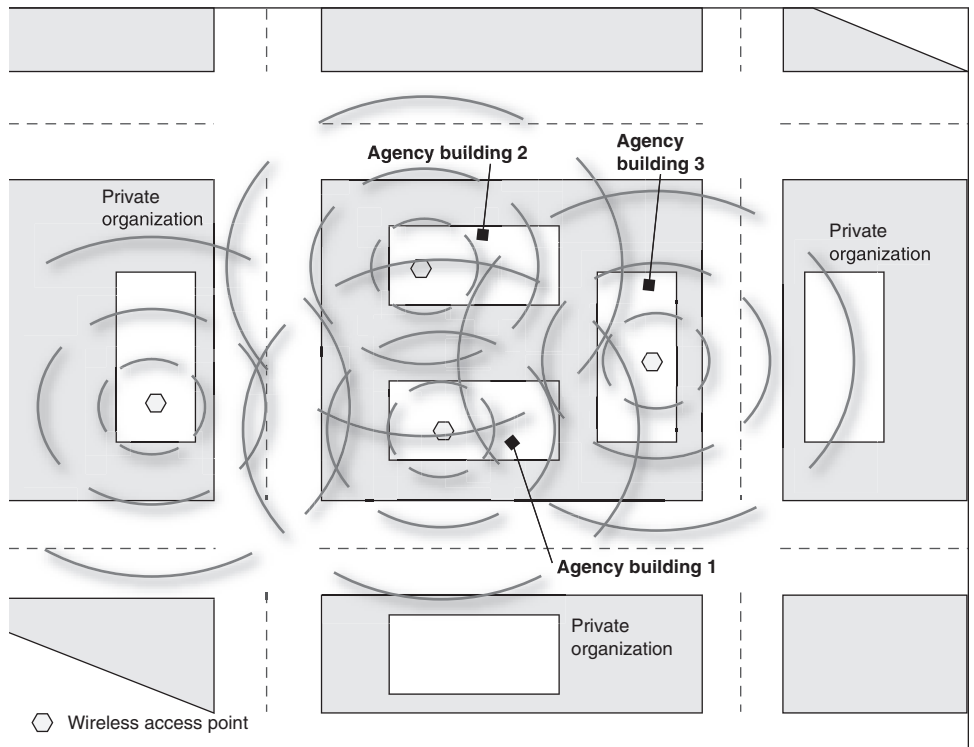
Message modification	The attacker alters a legitimate message by deleting or modifying it.
Jamming	Attackers flood a wireless network with excess radio signals to prevent authorized users from accessing it. Other devices that emit radio signals, such as cordless phones and microwaves, can also disrupt or degrade wireless network performance.

Source: NIST.

Physical Control of Wireless-Enabled Devices Takes on New Importance in Maintaining Security

Physical control of wireless-enabled devices takes on new importance in maintaining information security. Areas of physical risk include the placement and configuration of wireless access points and control of the wireless-enabled device that connects to the agency's network. For example, it can be difficult to control the distance of wireless network transmissions, because wireless access points can broadcast signals from 150 feet to as far as 1,500 feet, depending on how they are configured. As a result, wireless access points can and do broadcast signals outside building perimeters. Figure 4 illustrates how poorly positioned or improperly configured wireless access points may radiate signals beyond the physical boundaries of the agency's facility or the range within which the agency desires to send its signal. Wireless signals broadcast from within an agency's facility that extend through physical walls, windows, and beyond a building's perimeter—commonly known as “signal leakage”—can increase an agency's susceptibility to the various attacks described in table 1 above.

Figure 4: Example of Signal Leakage at Federal and Private Facilities



Source: GAO.

In addition to the challenge of signal leakage, it can be difficult for wireless network administrators to track the physical location of wireless-enabled devices. For example, in conventional wired networks, users are required to physically plug in to the agency's networks via cable. This allows administrators to determine where each device is connected. However, with a wireless network, pinpointing a wireless-enabled device's location can be difficult because the device is mobile. As a result, it can be harder for information security officials to locate unauthorized devices and eliminate the risks they pose.

Unauthorized Wireless Deployments Create New Challenges for Agencies' Information Security

Unauthorized wireless networks create two main challenges for agencies' information security. The first challenge comes from legitimate agency organizations, employees, or contractors seeking to benefit from the flexibility of wireless networks. Because of the affordability and availability of wireless network equipment, well-meaning individuals might

install unauthorized wireless-enabled devices or wireless access points into an agency's traditional wired network environment without the approval of the agency's chief information officer. As a result, agency information security officials might be unaware that wireless networks are being used and would therefore be unable to take the appropriate mitigating actions—such as protecting against potential wireless attacks or preventing signal leakage.

The second challenge stems from the increasing availability and integration of wireless technology into products such as laptops. For example, agencies that are not seeking to install a wireless network may find that as they purchase new equipment they are buying wireless-enabled devices. In some instances, these devices are not available without wireless technology. As a result, an agency may inadvertently procure wireless network components that could pose risks to its enterprise. It is critical that agencies understand whether or not the equipment they are procuring is wireless-enabled and determine how they will mitigate the risks it can pose to their information and systems.

Controls Can Mitigate Wireless Network Security Challenges

Controls such as policies, practices, and tools can help to mitigate wireless network security challenges that federal agencies face. These controls include

- developing comprehensive policies that govern the implementation and use of wireless networks,
- defining configuration requirements that provide guidance on the deployment of available security tools,
- establishing comprehensive monitoring programs that help to ensure that wireless networks are operating securely, and
- training employees and contractors effectively in an agency's wireless policies.

Developing Comprehensive Policies Can Mitigate Security Risks to Wireless Networks

Developing comprehensive information security policies that address the security of wireless networks can help agencies mitigate risks. FISMA recognizes that development of policies and procedures is essential to cost-effectively reducing the risks associated with information technology to an

acceptable level. NIST specifies 13 elements⁴ that should be addressed in a policy for securing wireless networks. These elements can be broadly organized into the following three categories: (1) authorized use, (2) identification of requirements, and (3) security controls.

Table 2: Policies for Managing Wireless Network Risks

Authorize use of wireless networks:	identify who may use WLAN technology in an agency
	describe the type of information that may be sent over wireless links
	describe who can install access points and other wireless equipment
	describe conditions under which wireless devices are allowed
	describe limitations on how the wireless device may be used, such as location
	provide guidelines on reporting losses of wireless devices and security incidents
Identify requirements:	describe the hardware and software configuration of all wireless devices
	provide guidelines for the protection of wireless clients to minimize/reduce theft
	identify whether Internet access is required
Establish security controls:	define standard security settings for access points
	provide limitations on the location of and physical security for access points
	define the frequency and scope of security assessments including access point discovery
	provide guidelines on the use of encryption and key management

Source: NIST.

By establishing policies that address the issues in table 2 above, agencies can create a framework for applying practices, tools, and training to help support wireless network security.

⁴National Institute of Standards and Technology, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, Special Publication 800-48 (Gaithersburg, Md.: November 2002).

Defining Configuration Requirements Can Improve the Security of Wireless Networks

Defining requirements for how specific wireless security tools or wireless-enabled devices should be used or configured can help to improve network security in accordance with agency policy. For example, configuration requirements can guide agency employees in identifying and setting up wireless security tools such as encryption, authentication, virtual private networks, and firewalls (see table 3).

Table 3: Examples of Wireless Security Tools That Can Be Configured to Meet Agency Policies

Encryption	Encryption protects the confidentiality of information traversing wireless networks by transforming data into code form (ciphertext).
Authentication	Authentication technologies such as smart cards or time synchronized tokens help to establish the validity of a user's claimed identity and prevent unauthorized access to data and systems.
Virtual private networks	Virtual private networks allow users in two separate physical locations to establish network connections over a shared public infrastructure, such as the Internet, with functionality that is similar to that of a private encrypted network.
Firewalls	Firewalls are network devices or systems that run special software to control the flow of network traffic among networks or between a host and a network. Firewalls on wireless networks can be used to protect a wireless network from unauthorized access and to prevent some types of behaviors.

Source: NIST.

In addition to helping promote the effective and efficient use of security tools, establishing settings or configuration requirements for devices such as wireless access points can help agencies manage the risks of wireless networks. It is important to secure wireless access points to ensure that they are not tampered with or modified. Configuration requirements can guide the placement and signal strength of wireless access points to minimize signal leakage and exposure to attacks.

Comprehensive Wireless Network Monitoring Is a Key Security Practice

Comprehensive wireless network monitoring programs are important security for protecting wireless networks and their information. Comprehensive wireless monitoring programs usually focus on

- detecting signal leakage,

-
- determining compliance with configuration requirements, and
 - identifying authorized and unauthorized wireless-enabled devices.

Effective monitoring programs typically employ site surveys and wireless intrusion detection systems to accomplish these goals. Site surveys involve using wireless monitoring tools that identify wireless-enabled devices such as wireless access points, laptops, and personal digital assistants. Site surveys can include exterior scans of a building to detect signal leakage. Such scans can inform agency personnel about the strength of wireless signals and the effectiveness of wireless access point configuration. In addition, site surveys can assist agencies in detecting unauthorized wireless-enabled devices.

A wireless network intrusion detection system can be used to automatically detect inappropriate activity, ensure that configuration requirements are followed, and ensure that only authorized wireless-enabled devices are functioning. Such a detection system scans radio signals to obtain information on a wireless network, analyzes the information based on set security policy, and then responds to the analysis accordingly. An intrusion detection system for wireless networks includes positioning sensors, similar to access points, near authorized access points or in other areas that require monitoring. A wireless detection system can be combined with a system designed for wired networks to provide comprehensive network monitoring, but neither type alone provides adequate security for both wired and wireless networks.

Training Staff is a Fundamental Element of Successful Wireless Security

Training employees and contractors in an agency'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 them. 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.⁵ It is important to provide training on technology to ensure that users comply with current policies. NIST also strongly recommends specific

⁵44 U.S.C. §3544(b)(4).

training on wireless security and asserts that trained and aware users are the most important protection against wireless risks.

Federal Agencies Lack Key Controls for Securing Wireless Networks

Agencies often lack key controls for securing wireless networks, such as

- comprehensive policies that govern the implementation and use of wireless networks,
- configuration requirements that provide guidance on the settings and deployment of available security tools,
- comprehensive monitoring programs that help to ensure that wireless networks are operating securely, and
- training in an agency's wireless policies for both employees and contractors.

If agencies do not establish effective controls for securing federal wireless networks, federal information and operations can be placed at risk.

Agencies Have Not Developed Comprehensive Policies for Wireless Networks

Many agencies have not developed policies addressing wireless networks, and those that have often omitted key elements. Nine of the 24 major agencies reported having no specific policies and procedures related to wireless networks. Thirteen agencies stated that they had established policies that authorize the operation and use of wireless networks. Twelve of these 13 agencies also reported that their policies extended to the use of wireless networks by contractors. Two federal agencies reported having policies that forbid the use of wireless networks or devices.

Policies for many of the agencies did not address acceptable use of wireless networks. For example, 7 of the 13 agencies with policies had not established an acceptable use policy or provided specific guidance on the type of information agency personnel were allowed to transmit using wireless networks. NIST guidance recommends that acceptable use policies delineate the type of information that may be sent over wireless networks, in order to reduce the risk that sensitive information will be exposed. Without establishing acceptable use policies, agencies will not be able to determine whether wireless networks are being used appropriately.

The lack of such a policy could result in unauthorized disclosure of agency information or could increase the agency’s risk of a security breach.

Most Agencies Have Not Set Configuration Requirements for Wireless Networks

Thirteen of 24 agencies reported not having configuration requirements for wireless networks. Further, the configuration requirements submitted by the remaining 11 agencies were often incomplete, omitting key elements that NIST guidance identifies—such as the use of and settings for security tools, including encryption, authentication, virtual private networks, and firewalls; the placement and strength of wireless access points to minimize signal leakage; and the physical protection of wireless-enabled devices. Two of the 11 agencies with policies had established configuration requirements that addressed all of these elements. However, the configuration requirements of the other 9 agencies did not cover key areas of wireless security. For example,

- Three agencies did not have policies explaining how to configure wireless access points and other wireless-enabled devices.
- Five agencies have not developed detailed guidance describing how to physically secure wireless-enabled devices.

Most Agencies Lack Comprehensive Wireless Network Monitoring Programs

Most of the major agencies have not established comprehensive wireless network monitoring programs for detecting signal leakage or ensuring compliance with security policies. For example, 14 agencies, including 4 agencies that permit wireless networks, do not monitor for signal leakage. Additionally, 19 agencies report not monitoring the data flowing through their systems to ensure that users of wireless networks are complying with acceptable use policies. Further, 14 agencies have not established programs to monitor wireless networks to ensure compliance with configuration requirements.

Fifteen agencies reported monitoring for the existence of unauthorized or “rogue” wireless networks. Of these 15 agencies, only 6 continuously monitored their facilities 24 hours a day. The remaining 9 agencies monitored only periodically, sometimes as rarely as twice a year. The lack of continuous monitoring, combined with the ease of setting up wireless networks, creates a situation in which wireless networks can be operating in agencies with neither authorization nor the required security configurations. Consequently, agencies may not be able to determine whether security policies are being implemented in an appropriate manner,

whether employees are conforming to policy, and—more importantly—they may not have a full understanding of the existing risks to agency information and information systems. Even if an agency does not allow wireless networks, monitoring is one of the most effective ways to ensure compliance with agency policy.

The Majority of Agencies Have Not Established Wireless Security Training Efforts

Eighteen of the 24 agencies have not established any training programs for their employees and contractors on wireless security or the policies surrounding wireless networks. FISMA requires that agencies provide information security awareness training to all personnel, including contractors. 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. For example, employees may use wireless-enabled devices—configured to attach to wireless networks automatically—to access the agency's private wired network. An attacker might connect to such a device, accessing the agency's network under a legitimate user's authority.

Selected Agencies Did Not Implement Wireless Networks Securely

We tested the wireless network security at the headquarters of six federal agencies in Washington, D.C., and identified significant weaknesses related to signal leakage, configuration, and unauthorized devices.

- **Signal leakage**—We were able to detect signal leakage outside the headquarters buildings at all six agencies. In one case, we were able to detect an agency's network while we were testing at another agency several blocks away. By not managing signal leakage, agencies increase their susceptibility to attack. In addition, the confidentiality of agency data may be diminished because an unauthorized user could be eavesdropping or monitoring wireless traffic.
- **Insecure configurations**—We also found wireless-enabled devices operating with insecure configurations at all six agencies. For example, at one agency over 90 wireless laptops were attempting to associate with wireless networks while they were connected to the agency's wired networks. This configuration could provide unauthorized access to an agency's internal networks. In all six agencies we found wireless devices operating in ad hoc mode. In over half of these cases the ad hoc networks could be detected outside of the building and could have

provided access to the agency's networks. We found these situations at agencies without monitoring programs as well as at agencies with extensive monitoring programs.

- **Unauthorized wireless-enabled devices**—We detected unauthorized wireless-enabled devices at all six agencies. These devices included both unauthorized wireless access points and ad hoc wireless networks. None of the six agencies we tested maintained continuous wireless monitoring. Three had programs that would periodically test portions of their facilities; however, periodic monitoring was not sufficient to prevent unauthorized wireless activity.

Signal leakage, insecure configuration, and unauthorized wireless devices pose serious risks to the confidentiality, integrity, and availability of the information of the six agencies we tested. Because attackers in a wireless environment can focus on an easily discernable location, such as a headquarters building, federal agencies need to be especially concerned about signal leakage, insecure configurations, and unauthorized devices. If wireless signals emanate from a building, they could make the agency a target of attack.

Conclusions

Wireless networks can offer a wide range of benefits to federal agencies, including increased productivity, decreased costs, and additional flexibility for the federal workforce. However, wireless networks also present significant security challenges to agency management. The affordability of wireless technology, along with the increasing integration of wireless capabilities into equipment procured by the federal government, increases the importance of developing appropriate policies, procedures, and practices. Such actions could help ensure that wireless devices and networks do not place federal information and information systems at increased risk.

Currently, the lack of key controls in federal agencies means that unauthorized or poorly configured wireless networks could be creating new vulnerabilities. In some instances, the lack of policies and procedures for assessing and protecting wireless networks is impeding agency efforts to effectively address wireless security. In other cases, agencies' ineffective compliance monitoring hinders their ability to detect unauthorized wireless devices, ensure compliance with agency policies, and supervise behavior on wireless networks. Finally, the majority of agencies have not trained

their employees and contractors in the challenges of wireless networking and in agency policies concerning this technology.

Our testing at six major federal agencies found significant security weaknesses: signal leakage, insecure configurations of wireless equipment, and unauthorized devices. Wireless network security is a serious, pervasive, and crosscutting challenge to federal agencies, warranting increased attention from OMB. If these challenges are not addressed, federal agency information and operations will be at increased risk.

Recommendation for Executive Action

Because of the governmentwide challenges of wireless network security, we recommend that the Director of OMB instruct the federal agencies to ensure that wireless network security is incorporated into their agencywide information security programs, in accordance with FISMA. In particular, agencywide security programs should include

- robust policies for authorizing the use of the wireless networks, identifying requirements, and establishing security controls for wireless-enabled devices in accordance with NIST guidance;
- security configuration requirements for wireless devices that include
 - available security tools, such as encryption, authentication, virtual private networks, 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; and

-
- wireless security training for employees and contractors.

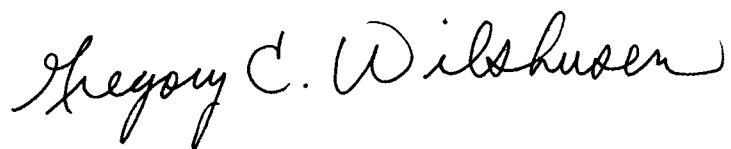
Agency Comments

In providing oral comments on a draft of this report, representatives of OMB's Office of Information and Regulatory Affairs and Office of General Counsel told us that they generally agreed with the contents of the report. OMB officials told us that NIST is developing updated wireless guidance for the federal agencies, which is scheduled to be issued for comment in August 2005. Further, OMB stressed that the agencies have the primary responsibility for complying with FISMA's information security management program requirements. OMB told us that as part of its annual review of agency information security programs, it would consider whether agencies' programs adequately addressed emerging technology issues such as wireless security before approving them.

We are sending copies of this report to the Director of OMB and to interested congressional committees. We will provide copies to other interested parties upon request. The report will also be available on GAO's Web site at <http://www.gao.gov>.

If you have any questions or wish to discuss this report, please contact either Gregory Wilshusen at (202) 512-6244 or Keith Rhodes at (202) 512-6412. We can also be reached at wilshuseng@gao.gov or rhodesk@gao.gov. Key contributors to this report are listed in appendix II.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues



Keith A. Rhodes
Chief Technologist

Objectives, Scope, and Methodology

The objectives of our review were to

- describe the benefits and challenges associated with securing wireless networks,
- identify the controls (policies, practices, and tools) available to assist federal agencies in securing wireless networks,
- analyze the wireless policies and practices reported by each of the 24 agencies covered by the Chief Financial Officers (CFO) Act of 1990,¹ and
- test the security of wireless networks at the headquarters of six major federal agencies in Washington, D.C.

For the first three objectives, the scope of our review included (1) the 24 agencies under the CFO Act and focused on wireless networks conforming to the 802.11x standard. For the fourth objective, we tested the wireless network security at 6 major federal agencies. Our review did not evaluate the risks that remote wireless users, such as teleworkers, might pose to agency systems.

To determine the benefits and challenges of using 802.11x wireless networks securely, we reviewed federal and private-sector technical documents, including National Institute of Standards and Technology (NIST) guidance and leading private sector practices. Additionally, we documented the various benefits and challenges of wireless networks with representatives from private-sector wireless security providers, federal experts and agency officials, and financial institutions.

To determine what controls were available to agencies for securing their 802.11x wireless networks, we reviewed federal and private-sector technical documents, including NIST guidance and leading private-sector practices. Additionally, we documented various controls for securing wireless networks—such as policies, practices, and tools—with representatives of private-sector wireless security providers, federal experts and agency officials, and financial institutions.

To determine the wireless security practices and policies used at federal agencies, we conducted a survey of the 24 CFO agencies. We developed a

¹31 U.S.C. 901(b).

series of questions that were incorporated into a Web-based survey instrument. We tested this instrument with one federal agency and internally at GAO through our Chief Information Officer's office. The survey included questions on the agencies' use of wireless networks and their policies and procedures for securing them. For each agency to be surveyed, we identified the office of the chief information officer, notified each office of our work, and, distributed a link to each office via e-mail to allow them to access the Web-based survey. In addition, we discussed the purpose and content of the survey with agency officials when they requested it. All 24 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that the agencies provided to validate their responses. We contacted agency officials when necessary for follow-up.

Although this was not a sample survey and, therefore, there were no sampling errors, conducting any survey may introduce errors—commonly referred to as nonsampling errors. For example, difficulties in how a particular question is interpreted, in the sources of information that are available to respondents, or in how the data are entered into a database or analyzed can introduce unwanted variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize these nonsampling errors. For example, a survey specialist designed the survey instrument in collaboration with GAO staff with subject-matter expertise. Then, as stated earlier, it was pretested to ensure that the questions were relevant, clearly stated, and easy to comprehend. When the data were analyzed, a second, independent analyst checked all computer programs. Because this was a Web-based survey, respondents entered their answers directly into the electronic questionnaire. This eliminated the need to have the data keyed into a database, thus removing an additional potential source of error.

To assess the state of wireless security at a selected group of federal agencies, we conducted onsite network surveys at 6 of the 24 CFO agencies. We selected 6 agencies in various stages of wireless implementation: 2 had established wireless networks, 1 had a pilot system, 2 did not have any authorized wireless networks, and 1 forbade the use of wireless. At each agency's Washington, D.C., headquarters, we scanned for signal leakage and wireless activity, using wireless monitoring tools both inside and outside the agency's facility. For security purposes, we do not identify the 6 agencies in the report.

Appendix I
Objectives, Scope, and Methodology

We performed our work in the Washington, D.C., metropolitan area from September 2004 to March 2005, in accordance with generally accepted government auditing standards.

Contacts and Staff Acknowledgments

GAO Contact

J. Paul Nicholas, (202) 512-4457
Assistant Director

Staff Acknowledgments

In addition to the person mentioned above, Mark Canter, Lon Chin, West Coile, Derrick Dicoi, Neil Doherty, Joanne Fiorino, Suzanne Lightman, Kush Malhotra, and Christopher Warweg made key contributions to this report.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548