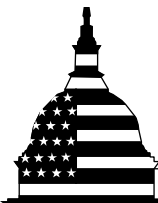


September 2012

INFORMATION  
SECURITY

Better Implementation  
of Controls for Mobile  
Devices Should Be  
Encouraged



G A O

Accountability \* Integrity \* Reliability

## Why GAO Did This Study

Millions of Americans currently use mobile devices—e.g., cellphones, smartphones, and tablet computers—on a daily basis to communicate, obtain Internet-based information, and share their own information, photographs, and videos. Given the extent of consumer reliance on mobile interactions, it is increasingly important that these devices be secured from expanding threats to the confidentiality, integrity, and availability of the information they maintain and share.

Accordingly, GAO was asked to determine (1) what common security threats and vulnerabilities affect mobile devices, (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities, and (3) the extent to which government and private entities have been addressing the security vulnerabilities of mobile devices. To do so, GAO analyzed publicly available mobile security reports, surveys related to consumer cybersecurity practices, as well as statutes, regulations, and agency policies; GAO also interviewed representatives from federal agencies and private companies with responsibilities in telecommunications and cybersecurity.

## What GAO Recommends

GAO recommends that FCC encourage the private sector to implement a broad, industry-defined baseline of mobile security safeguards. GAO also recommends that DHS and NIST take steps to better measure progress in raising national cybersecurity awareness. The FCC, DHS, and NIST generally concurred with GAO's recommendations.

View [GAO-12-757](#). For more information, contact Gregory C. Wilshusen at 202-512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) or Dr. Nabajyoti Barkakati at (202) 512-4499 or [barkakatin@gao.gov](mailto:barkakatin@gao.gov).

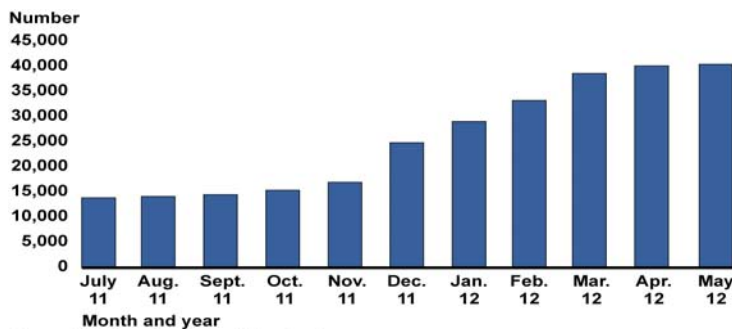
## Information Security

### Better Implementation of Controls for Mobile Devices Should Be Encouraged

## What GAO Found

Threats to the security of mobile devices and the information they store and process have been increasing significantly. For example, the number of variants of malicious software, known as "malware," aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185 percent in less than a year (see figure). Cyber criminals may use a variety of attack methods, including intercepting data as they are transmitted to and from mobile devices and inserting malicious code into software applications to gain access to users' sensitive information. These threats and attacks are facilitated by vulnerabilities in the design and configuration of mobile devices, as well as the ways consumers use them. Common vulnerabilities include a failure to enable password protection and operating systems that are not kept up to date with the latest security patches.

Figure: Number of Malware Variants Identified Globally between July 2011 and May 2012



Source: GAO based on Juniper Networks, Inc.

Mobile device manufacturers and wireless carriers can implement technical features, such as enabling passwords and encryption to limit or prevent attacks. In addition, consumers can adopt key practices, such as setting passwords and limiting the use of public wireless connections for sensitive transactions, which can significantly mitigate the risk that their devices will be compromised.

Federal agencies and private companies have promoted secure technologies and practices through standards and public private partnerships. Despite these efforts, safeguards have not been consistently implemented. Although the Federal Communications Commission (FCC) has facilitated public-private coordination to address specific challenges such as cellphone theft, it has not yet taken similar steps to encourage device manufacturers and wireless carriers to implement a more complete industry baseline of mobile security safeguards. In addition, many consumers still do not know how to protect themselves from mobile security vulnerabilities, raising questions about the effectiveness of public awareness efforts. The Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST) have not yet developed performance measures or a baseline understanding of the current state of national cybersecurity awareness that would help them determine whether public awareness efforts are achieving stated goals and objectives.

---

# Contents

---

Letter		1
	Background	2
	Mobile Devices Face a Broad Range of Security Threats and Vulnerabilities	11
	Security Controls and Practices Identified by Experts Can Reduce Vulnerabilities	22
	Public and Private-Sector Entities Have Taken Initial Steps to Address Security of Mobile Devices, but Consumers Remain Vulnerable to Threats	27
	Efforts Have Been Made to Address Security Vulnerabilities, but Controls Are Not Always Implemented	27
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	39
Appendix II	Comments from the Federal Communications Commission	41
Appendix III	Comments from the Department of Homeland Security	42
Appendix IV	Comments from the Department of Commerce	44
Appendix V	Federal Websites for Information Related to Mobile Security	46
Appendix VI	GAO Contacts and Staff Acknowledgments	48
Tables		
	Table 1: Sources of Mobile Threats	14
	Table 2: Common Mobile Attacks	15

---

Table 3: Key Security Controls to Combat Common Threats and Vulnerabilities	23
Table 4: Additional Security Controls Specific to Organizations to Combat Common Threats and Vulnerabilities	24
Table 5: Key Security Practices to Combat Common Threats and Vulnerabilities	25
Table 6: Additional Security Practices Specific to Organizations to Combat Common Threats and Vulnerabilities	26
Table 7: Federal Websites and Links to Information Related to Mobile Security	46

---

## Figures

Figure 1: Key Components of a Cellular Network	6
Figure 2: Number of Malware Variants Identified Globally between July 2011 and May 2012	13
Figure 3: Repackaging Applications with Malware	19
Figure 4: Man-in-the-Middle Attack Using an Unsecured WiFi Network	22

---

---

### Abbreviations

Commerce	Department of Commerce
CSRIC	Communications, Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
DOD	Department of Defense
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
FTC	Federal Trade Commission
http	hypertext transfer protocol
NCSA	National Cyber Security Alliance
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
PIN	personal identification number
PKI	public key infrastructure
US-CERT	US-Computer Emergency Readiness Team
VPN	virtual private network

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



**G A O**

Accountability \* Integrity \* Reliability

United States Government Accountability Office  
Washington, DC 20548

---

September 18, 2012

The Honorable Fred Upton  
Chairman  
The Honorable Henry Waxman  
Ranking Member  
Committee on Energy and Commerce  
House of Representatives

The Honorable Greg Walden  
Chairman  
The Honorable Anna Eshoo  
Ranking Member  
Committee on Energy and Commerce  
Subcommittee on Communications and Technology  
House of Representatives

The Honorable Cliff Stearns  
Chairman  
The Honorable Diana DeGette  
Ranking Member  
Committee on Energy and Commerce  
Subcommittee on Oversight and Investigations  
House of Representatives

Millions of Americans currently use mobile devices—cellphones, smartphones, and tablet computers—on a daily basis to communicate, obtain Internet-based information, and share information, photographs, and videos. Dramatic recent advances in the technical capabilities of mobile devices have paved the way for increased connectivity. As a result, consumers can now carry out a broad range of interactions, including sensitive transactions, which previously required the use of a desktop or laptop computer. Given the extent of consumer reliance on mobile interactions, it is increasingly important that these devices be secured from threats to the confidentiality, integrity, and availability of the information they maintain and share.

Accordingly, our objectives were to determine: (1) what common security threats and vulnerabilities affect mobile devices, (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities, and (3) the extent to which government and private entities have been addressing the security

---

vulnerabilities of mobile devices. To assess common security threats and vulnerabilities as well as security controls and practices to address them, we obtained and reviewed published analyses and guidance, including databases of mobile security vulnerabilities. We also interviewed representatives from federal agencies and private companies with responsibilities in the telecommunications and cybersecurity fields to obtain current information about threats and vulnerabilities. To determine the extent to which the government and private entities are addressing vulnerabilities, we analyzed statutes, regulations, agency policies, and technical standards. We also interviewed officials from federal agencies and private companies to identify actions taken to address mobile security, such as developing guidance and sharing information.

We conducted this performance audit from November 2011 to September 2012 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

Consumer adoption of mobile devices is growing rapidly, enabled by affordable prices, increasingly reliable connections, and faster transmission speeds. According to a recent analysis, mobile devices are the fastest growing consumer technology, with worldwide sales increasing from 300 million in 2010 to an estimated 650 million in 2012.<sup>1</sup> Advances in computing technology have resulted in increased speed and storage capacity for mobile devices. The advances have enhanced consumers' abilities to perform a wide range of online tasks. While these devices provide many productivity benefits to consumers and organizations, they also pose security risks if not properly protected.

---

<sup>1</sup>Lookout Mobile Security, *Lookout Mobile Threat Report* (San Francisco, Calif.: August 2011).

---

## A Variety of Entities Provide Products and Services to Consumers

Several different types of private sector entities provide products and services that are used by consumers as part of a seamless mobile telecommunications system. These entities include mobile device manufacturers, operating system developers, application developers, and wireless carriers.

### Mobile Device Manufacturers

Manufacturers of mobile equipment include both hardware and software developers. Components of the hardware or software on any given device may come from multiple manufacturers. Major device manufacturers with the largest total market shares in the United States include Apple Inc., HTC Corporation, Research In Motion, Corp., Motorola Mobility Inc., Samsung, and LG Electronics. The products they develop include cellphones, smartphones, and tablet computers.

- A cellphone is a device that can make and receive telephone calls over a radio network while moving around a wide geographic area. According to a recent report,<sup>2</sup> 88 percent of American adults owned cellphones as of February 2012.
- A smartphone has more capabilities than a cellphone. Consumers can use smartphones to run a wide variety of general and special-purpose software applications. Smartphones typically have a larger graphical display with greater resolution than cellphones and have either a keyboard or touch-sensitive screen for alphanumeric input. Smartphones also offer expansion capabilities and other built-in wireless communications (such as WiFi and Bluetooth services).<sup>3</sup> According to a recent report,<sup>4</sup> 46 percent of American adults owned smartphones as of February 2012.
- A tablet personal computer is a portable personal computer with a touch-sensitive screen. The tablet form is typically smaller than a notebook computer but larger than a smartphone. According to a

---

<sup>2</sup>Pew Research Center, *46% of American Adults Are Smartphone Owners* (Washington, D.C.: March 2012).

<sup>3</sup>WiFi and Bluetooth are commonly used technologies that allow an electronic device to exchange data wirelessly (using radio waves) with other devices and computer networks.

<sup>4</sup>Pew Research Center, *46% of American Adults Are Smartphone Owners* (Washington, D.C.: March 2012).



---

recent report,<sup>5</sup> 19 percent of American adults owned a tablet as of January 2012.

### **Mobile Operating System Developers**

Operating system developers build the software that provides basic computing functions and controls for mobile devices. The operating system is the software platform used by other programs, called applications, to interact with the mobile device. Major operating system developers for mobile devices with the largest total market shares in the United States include Apple Inc., Google Inc., and Research In Motion, Corp.

- **Apple Inc.** The mobile operating system developed and distributed by Apple is known as iOS. It is a proprietary system; all updates and other changes to the software are administered by Apple. In addition, all software applications that run on iOS devices (e.g., iPhones and iPads) are required to conform to specifications established by Apple and be digitally signed by approved developers. Apple distributes these applications through its online “store,” called App Store.
- **Google Inc.** As a member of the Open Handset Alliance,<sup>6</sup> Google Inc. led the development of Android, an operating system for mobile devices, based on the Linux operating system. Android, like Linux, is an “open” operating system, meaning that its software code is publicly available and can be tailored to the needs of individual devices and telecommunications carriers. Thus, many different tailored versions of the software are in use. To run on Android devices, software applications need to be digitally signed by the developer, who is responsible for the application’s behavior. Android applications are made available on third-party application marketplaces, websites, and on the online official Android application store called Google Play.
- **Research In Motion, Corp.** Research In Motion developed a proprietary operating system for its BlackBerry mobile devices. Although a proprietary system, it can run any third-party applications that are written in Java.<sup>7</sup> Applications are tested by Research In

---

<sup>5</sup>Pew Research Center, *Tablet and E-book Reader Ownership Nearly Double Over the Holiday Gift-Giving Period* (Washington, D.C.: January 2012).

<sup>6</sup>The Open Handset Alliance is a consortium of 84 hardware, software, and telecommunications companies devoted to advancing open standards for mobile devices.

<sup>7</sup>Java is a programming language and computing platform that powers programs including utilities, games, and business applications.

---

Motion before users can download them. In addition, any application given access to sensitive data or features when installed is required by Research In Motion to be digitally signed by the developer. BlackBerry applications are available for download on the online store called BlackBerry App World.

### **Mobile Application Developers**

Mobile application developers develop the software applications that consumers interact with directly. In many cases, these applications provide the same services that are available through traditional websites, such as news and information services, online banking, shopping, and electronic games. Other applications are designed to take into account a user's physical location to provide tailored information or services, such as information about nearby shops, restaurants, or other elements of the physical environment.

### **Wireless Carriers**

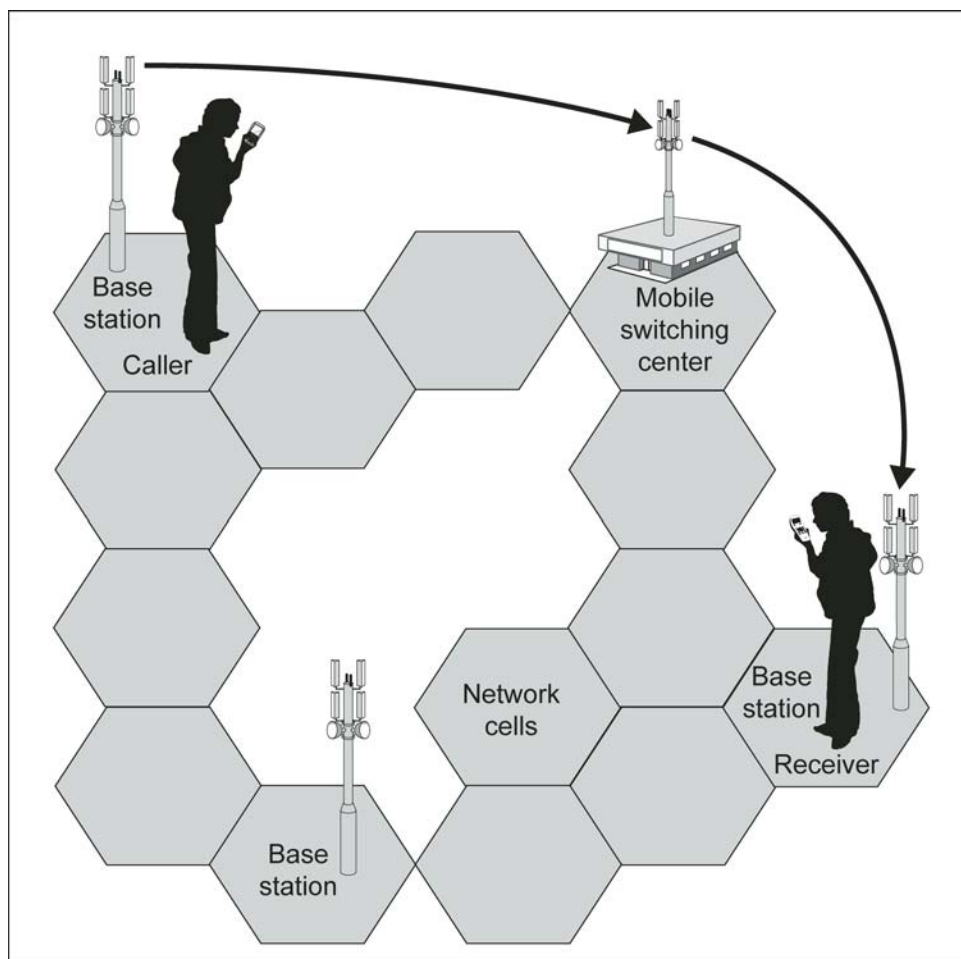
Wireless carriers manage telecommunications networks and provide phone services, including mobile devices, directly to consumers. While carriers do not design or manufacture their own mobile devices, in some cases they can influence the design and the features of other manufacturers' products because they control sales and interactions with large numbers of consumers. Major wireless carriers with the largest total market shares in the United States include Verizon Wireless, AT&T Inc., Sprint, and T-Mobile USA Inc.

Carriers provide basic telephone service through wireless cellular networks which cover large distances. However, other types of shorter-range wireless networks may also be used with mobile devices. These shorter-range networks may be supported by the same carriers or by different providers. Major types of wireless networks include cellular networks, WiFi networks, and wireless personal area networks.

- **Cellular networks.** Cellular networks are managed by carriers and provide coverage based on dividing a large geographical service area into smaller areas of coverage called "cells." The cellular network is a radio network distributed over the cells and each cell has a base station equipped with an antenna to receive and transmit radio signals to mobile phones within its coverage area. A mobile device's communications are generally associated with the base station of the cell in which it is located. Each base station is linked to a mobile telephone switching office, which is also connected to the local

wireline telephone network. The mobile phone switching office directs calls to the desired locations, whether to another mobile phone or a traditional wireline telephone. This office is responsible for switching calls from one cell to another in a smooth and seamless manner as consumers change locations during a call. Figure 1 depicts the key components of this cellular network.

**Figure 1: Key Components of a Cellular Network**



Source: GAO.

- **WiFi networks.** WiFi networking nodes may be established by businesses or consumers to provide networking service within a limited geographic area, such as within a home, office, or place of business. They are generally composed of two basic elements:

---

access points and wireless-enabled devices, such as smart phones and tablet computers. These devices use 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. WiFi networks conform to the Institute of Electrical and Electronics Engineers 802.11 standards.<sup>8</sup>

- **Other wireless personal area networks.** Other wireless personal area networks may be used that do not conform to the WiFi standard. For example, the Bluetooth standard<sup>9</sup> is often used to establish connectivity with nearby components, such as headsets or computer keyboards.

---

## Federal Agencies Have Roles in Addressing Mobile Security

While federal agencies are not responsible for ensuring the security of individual mobile devices, several are involved in activities designed to address and promote cybersecurity and mobile security in general.

- The Department of Commerce (Commerce) is responsible under Homeland Security Presidential Directive 7<sup>10</sup> in coordination with other federal and nonfederal entities, for improving technology for cyber systems and promoting efforts to protect critical infrastructure. Within Commerce, the National Institute of Standards and Technology (NIST) is responsible for developing information security standards and guidelines, including minimum requirements for unclassified federal information systems, as part of its statutory responsibilities

---

<sup>8</sup>The Institute of Electrical and Electronics Engineers is a professional association focused on electrical and computer sciences, engineering, and related disciplines. It is responsible for developing technical standards through its Standards Association, which follows consensus-based standards development processes.

<sup>9</sup>Bluetooth is an open standard for short-range radio frequency communication. Bluetooth technology is used primarily to establish wireless personal area networks, commonly referred to as ad hoc or peer-to-peer networks. The standard allows mobile devices to be placed in different modes: discoverable, which allows the device to be detected and receive connections from other Bluetooth-enabled devices; connectable, which allows the device to respond to other devices and establish a network connection with them; or completely off.

<sup>10</sup>Homeland Security Presidential Directive 7 establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state, and local agencies will play in carrying it out.

---

under the Federal Information Security Management Act (FISMA).<sup>11</sup> For example, NIST has developed guidelines on cellphone and Bluetooth security.<sup>12</sup> These standards and guidelines are generally made available to the public and can be used by both the public and private sectors. NIST also serves as the lead federal agency for coordinating the National Initiative for Cybersecurity Education (NICE) with other agencies. According to NIST, NICE seeks to establish an operational, sustainable, and continually improving cybersecurity education program for the nation. NICE includes an awareness initiative, which is led by the Department of Homeland Security (DHS), which focuses on boosting national cybersecurity awareness through public service campaigns to promote cybersecurity and responsible use of the Internet, and making cybersecurity a popular educational and career pursuit for older students. As we previously reported,<sup>13</sup> NIST developed a draft strategic plan for the NICE initiative. This plan includes strategic goals, supporting objectives, and related activities for the awareness component. Specifically, the draft strategic plan calls for (1) improving citizens' knowledge to allow them to make smart choices as they manage online risk, (2) improving knowledge of cybersecurity within organizations so that resources are well applied to meet the most obvious and serious threats, and (3) enabling access to cybersecurity resources. The plan also identifies supporting activities and products designed to support the overarching goal, such as the "Stop. Think. Connect." awareness campaign.

According to Commerce's National Telecommunications and Information Administration (NTIA), it serves as the President's principal adviser on telecommunications policies pertaining to economic and technological advancement and to the regulation of the telecommunications industry, including mobile telecommunications. NTIA is responsible for coordinating telecommunications activities of the executive branch and assisting in the formulation of policies and standards for those activities, including considerations of

---

<sup>11</sup>15 U.S.C. 278g-3, as amended by FISMA, Title III, Pub. L. No. 107-347 (Dec. 17, 2002).

<sup>12</sup>NIST, *Guidelines on Cell Phone and PDA Security*, SP 800-124 (Gaithersburg, Md.: October 2008) and *Guide to Bluetooth Security*, SP 800-121, Revision 1 (Gaithersburg, Md.: June 2012).

<sup>13</sup>GAO, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination*, [GAO-12-8](#) (Washington, D.C.: Nov. 29, 2011).

---

interoperability, privacy, security, spectrum use, and emergency readiness.

- Federal law and policy tasks DHS with critical infrastructure protection responsibilities that include creating a safe, secure, and resilient cyber environment in conjunction with other federal agencies, other levels of government, international organizations, and industry. The National Strategy to Secure Cyberspace tasked DHS as the lead agency in promoting a comprehensive national awareness program to empower Americans to secure their own parts of cyberspace.<sup>14</sup> Consistent with that tasking, DHS is currently leading the awareness component of NICE.
- The Federal Communications Commission's (FCC) role in mobile security stems from its broad authority to regulate interstate and international communications, including for the purpose of "promoting safety of life and property."<sup>15</sup> In addition, FCC has established the Communications, Security, Reliability, and Interoperability Council (CSRIC). CSRIC is a federal advisory committee whose mission is to provide recommendations to FCC to help ensure, among other things, secure and reliable communications systems, including telecommunications, media, and public safety. A previous CSRIC<sup>16</sup> included a working group that was focused on identifying cybersecurity best practices (including mobile security practices), and had representation from segments of the communications industry and public safety communities. The current CSRIC has focused on the development and implementation of best practices related to several specific cybersecurity topics. FCC has also established a Technological Advisory Council, which includes various working groups, one of which has been working since March 2012 to identify, prioritize, and analyze mobile security and privacy issues.
- The Federal Trade Commission (FTC) promotes competition and protects the public by, among other things, bringing enforcement actions against entities that engage in unfair or deceptive acts or

---

<sup>14</sup>The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

<sup>15</sup>See for example, 47 U.S.C. 151 and 332; Communications Act of 1934, as amended, including by the Telecommunications Act of 1996, Pub. L. No. 104-104 (Feb. 8, 1996).

<sup>16</sup>The CSRIC has operated under 2-year charters that have regularly been renewed.

---

practices.<sup>17</sup> An unfair act is an act or practice that causes or is likely to cause substantial injury to consumers that is not reasonably avoidable by consumers and is not outweighed by countervailing benefits to consumers or to competition. A deceptive act or practice occurs if there is a representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment. According to FTC, its authority to bring enforcement actions covers many of the entities that provide mobile products and services to consumers, including mobile device manufacturers, operating system developers, and application developers. FTC's jurisdiction also extends to wireless carriers when they are not engaged in common carrier activities. For example, mobile phone operators engaging in mobile payments functions such as direct-to-carrier billing are under FTC's jurisdiction.

- The Department of Defense (DOD) is responsible for security systems, including mobile devices that use its networks or contain DOD data. While it has no responsibility with regards to consumer mobile devices, its guidance can be useful for consumers. For example, the DOD Security Technical Implementation Guides are available to the public. These guides contain technical guidance to secure information systems or software that might otherwise be vulnerable to a malicious computer attack. In addition, certain guides address aspects of mobile device security.
- The Office of Management and Budget (OMB) is responsible for overseeing and providing guidance to federal agencies on the use of information technology, which can include mobile devices. One OMB memorandum to federal agencies, for example, instructs agencies to properly safeguard information stored on federal systems (including mobile devices) by requiring the use of encryption and a "time-out" function for re-authentication after 30 minutes of inactivity.<sup>18</sup>

---

<sup>17</sup>15 U.S.C. 45.

<sup>18</sup>OMB, *Memorandum for the Heads of Departments and Agencies: Protection of Sensitive Agency Information M-06-16* (Washington, D.C.: June 23, 2006).

---

## Mobile Devices Face a Broad Range of Security Threats and Vulnerabilities

Threats<sup>19</sup> to the security of mobile devices and the information they store and process have been increasing significantly.<sup>20</sup> Many of these threats are similar to those that have long plagued traditional computing devices connected to the Internet. For example, cyber criminals and hackers have a variety of attack methods readily available to them, including using software tools to intercept data as they are transmitted to and from a mobile device, inserting malicious software code into the operating systems of mobile devices by including it in seemingly harmless software applications, and using e-mail phishing techniques to gain access to mobile-device users' sensitive information. The significance of these threats, which are growing in number and kind, is magnified by the vulnerabilities associated with mobile devices. Common vulnerabilities<sup>21</sup> in mobile devices include a failure to enable password protection, the lack of the capability to intercept malware, and operating systems that are not kept up to date with the latest security patches.

---

## Attacks on Mobile Devices Are Increasing

Cyber-based attacks against mobile devices are evolving and increasing. Examples of recent incidents include:

- In May 2012, a regulatory agency in the United Kingdom fined a company for distributing malware versions of popular gaming applications that triggered mobile devices to send costly text messages to a premium-rate telephone number.
- In February 2012, a cybersecurity firm, Symantec Corporation, reported that a large number of Android devices in China were

---

<sup>19</sup>Threats are any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

<sup>20</sup>Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997. See, most recently, GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011).

<sup>21</sup>Vulnerabilities are weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.



---

infected with malware that connected them to a botnet.<sup>22</sup> The botnet's operator was able to remotely control the devices and incur charges on user accounts for premium services such as sending text messages to premium numbers, contacting premium telephony services, and connecting to pay-per-view video services. The number of infected devices able to generate revenue on any given day ranged from 10,000 to 30,000, enough to potentially net the botnet's operator millions of dollars annually if infection rates were sustained.

- In January 2012, an antivirus company reported that hackers had subverted the search results for certain popular mobile applications so that they would redirect users to a web page where they were encouraged to download a fake antivirus program containing malware.
- In October 2011, FTC reached a settlement of an unfair practice case with a company after alleging that its mobile application was likely to cause consumers to unwittingly disclose personal files, such as pictures and videos, stored on their smartphones and tablet computers. The company had configured the application's default settings so that upon installation and set-up it would publicly share users' photos, videos, documents, and other files stored on those devices.

These incidents reflect a trend of increasing global attacks against mobile devices. Specifically, recent studies have found that

- mobile malware grew by 155 percent in 2011;<sup>23</sup>
- new mobile vulnerabilities have been increasing, from 163 in 2010 to 315 in 2011, an increase of over 93 percent;<sup>24</sup>

---

<sup>22</sup>A botnet is a collection of compromised systems, each of which is known as a 'bot,' connected to the Internet. When a mobile device is compromised by an attacker, there is often code within the malware that commands it to become part of a botnet. The botnet's operator remotely controls these compromised mobile devices.

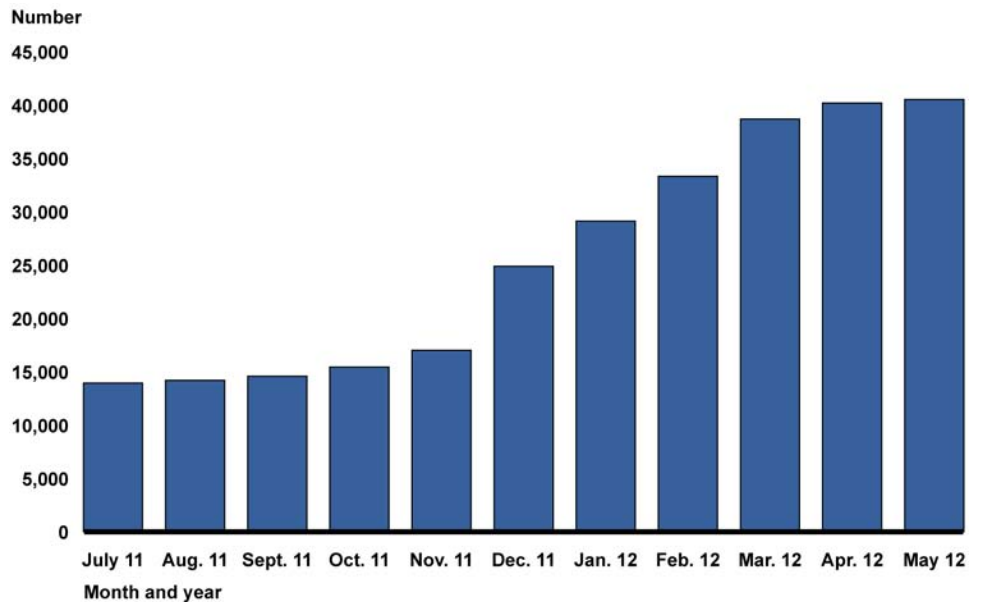
<sup>23</sup>Juniper Networks, Inc., *2011 Mobile Threats Report* (Sunnyvale, Calif.: February 2012).

<sup>24</sup>Symantec Corporation, *Internet Security Threat Report, 2011 Trends Vol.17* (Mountain View, Calif.: April 2012).

- an estimated half million to one million people had malware on their Android devices in the first half of 2011; and<sup>25</sup>
- 3 out of 10 Android owners are likely to encounter a threat on their device each year as of 2011.<sup>26</sup>

According to a networking technology company, Juniper Networks, malware aimed at mobile devices is increasing. For example, the number of variants of malicious software, known as “malware,” aimed at mobile devices has reportedly risen from about 14,000 to 40,000, a 185 percent increase in less than a year. Figure 2 shows the increase in malware variants between July 2011 and May 2012.

**Figure 2: Number of Malware Variants Identified Globally between July 2011 and May 2012**



Source: GAO based on Juniper Networks, Inc.

<sup>25</sup>Lookout Mobile Security, *Lookout Mobile Threat Report* (San Francisco, Calif.: August 2011).

<sup>26</sup>Lookout Mobile Security, *Lookout Mobile Threat Report* (San Francisco, Calif.: August 2011).

The increasing prevalence of attacks against mobile devices makes it important to assess and understand the nature of the threats they face and the vulnerabilities these attacks exploit.

## Sources of Threats and Attack Methods Vary

Mobile devices face a range of cybersecurity threats. These threats can be unintentional or intentional. Unintentional threats can be caused by software upgrades or defective equipment that inadvertently disrupt systems. Intentional threats include both targeted and untargeted attacks from a variety of sources, including botnet operators, cyber criminals, hackers, foreign nations engaged in espionage, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. For example, cyber criminals are using various attack methods to access sensitive information stored and transmitted by mobile devices.

Table 1 summarizes those groups or individuals that are key sources of threats for mobile devices.

**Table 1: Sources of Mobile Threats**

Threat source	Description
Botnet operators	Botnet operators use malware distributed to large numbers of mobile devices and other electronic systems to coordinate remotely controlled attacks on websites and to distribute phishing schemes, spam, and further malware attacks on individual mobile devices.
Cyber criminals	Cyber criminals generally attack mobile devices for monetary gain. They may use spam, phishing, and spyware/malware to gain access to the information stored on a device, which they then use to commit identity theft, online fraud, and computer extortion. In addition, international criminal organizations pose a threat to corporations, government agencies, and other institutions by attacking mobile devices to conduct industrial espionage and large-scale monetary and intellectual property theft.
Foreign governments	Foreign intelligence services may attack mobile devices as part of their information-gathering and espionage activities. Foreign governments may develop information warfare doctrine, programs, and capabilities that could disrupt the supply chain, mobile communications, and economic infrastructures that support homeland security and national defense.
Hackers	Hackers may attack mobile devices to demonstrate their skill or gain prestige in the hacker community. While hacking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and easily launch them against mobile devices.
Terrorists	Terrorists may seek to destroy, incapacitate, or exploit critical infrastructures such as mobile networks, to threaten national security, weaken the U.S. economy, or damage public morale and confidence. Terrorists may also use phishing schemes or spyware/malware to generate funds or gather sensitive information from mobile devices.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, the Software Engineering Institute's CERT® Coordination Center, and security reports.

These threat sources may use a variety of techniques, or exploits, to gain control of mobile devices or to access sensitive information on them. Common mobile attacks are presented in table 2.

**Table 2: Common Mobile Attacks**

Attacks	Description
Browser exploits	These exploits are designed to take advantage of vulnerabilities in software used to access websites. Visiting certain web pages and/or clicking on certain hyperlinks can trigger browser exploits that install malware or perform other adverse actions on a mobile device.
Data interception	Data interception can occur when an attacker is eavesdropping on communications originating from or being sent to a mobile device. Electronic eavesdropping is possible through various techniques, such as (1) man-in-the-middle attacks, which occur when a mobile device connects to an unsecured WiFi network and an attacker intercepts and alters the communication; and (2) WiFi sniffing, which occurs when data are sent to or from a device over an unsecured (i.e., not encrypted) network connection, allowing an eavesdropper to “listen to” and record the information that is exchanged.
Keystroke logging	This is a type of malware that records keystrokes on mobile devices in order to capture sensitive information, such as credit card numbers. Generally keystroke loggers transmit the information they capture to a cyber criminal’s website or e-mail address.
Malware	Malware is often disguised as a game, patch, utility, or other useful third-party software application. Malware can include spyware (software that is secretly installed to gather information on individuals or organizations without their knowledge), viruses (a program that can copy itself and infect the mobile system without permission or knowledge of the user), and Trojans (a type of malware that disguises itself as or hides itself within a legitimate file). Once installed, malware can initiate a wide range of attacks and spread itself onto other devices. The malicious application can perform a variety of functions, including accessing location information and other sensitive information, gaining read/write access to the user’s browsing history, as well as initiating telephone calls, activating the device’s microphone or camera to surreptitiously record information, and downloading other malicious applications. Repackaging—the process of modifying a legitimate application to insert malicious code—is one technique that an attacker can use.
Unauthorized location tracking	Location tracking allows the whereabouts of registered mobile devices to be known and monitored. While it can be done openly for legitimate purposes, it may also take place surreptitiously. Location data may be obtained through legitimate software applications as well as malware loaded on the user’s mobile device.
Network exploits	Network exploits take advantage of software flaws in the system that operates on local (e.g., Bluetooth, WiFi) or cellular networks. Network exploits often can succeed without any user interaction, making them especially dangerous when used to automatically propagate malware. With special tools, attackers can find users on a WiFi network, hijack the users’ credentials, and use those credentials to impersonate a user online. Another possible attack, known as bluesnarfing, enables attackers to gain access to contact data by exploiting a software flaw in a Bluetooth-enabled device.
Phishing	Phishing is a scam that frequently uses e-mail or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to “phish” for passwords and financial information from mobile users and other Internet users.
Spamming	Spam is unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malicious software. Spam can appear in text messages as well as electronic mail. Besides the inconvenience of deleting spam, users may face charges for unwanted text messages. Spam can also be used for phishing attempts.

Attacks	Description
Spoofing	Attackers may create fraudulent websites to mimic or “spoof” legitimate sites and in some cases may use the fraudulent sites to distribute malware to mobile devices. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message. Spoofed e-mails may contain malware.
Theft/loss	Because of their small size and use outside the office, mobile devices can be easier to misplace or steal than a laptop or notebook computer. If mobile devices are lost or stolen, it may be relatively easy to gain access to the information they store.
Zero-day exploit	A zero-day exploit takes advantage of a security vulnerability before an update for the vulnerability is available. By writing an exploit for an unknown vulnerability, the attacker creates a potential threat because mobile devices generally will not have software patches to prevent the exploit from succeeding.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports.

Attacks against mobile devices generally occur through four different channels of activities:

- **Software downloads.** Malicious applications may be disguised as a game, device patch, or utility, which is available for download by unsuspecting users and provides the means for unauthorized users to gain unauthorized use of mobile devices and access to private information or system resources on mobile devices.
- **Visiting a malicious website.** Malicious websites may automatically download malware to a mobile device when a user visits. In some cases, the user must take action (such as clicking on a hyperlink) to download the application, while in other cases the application may download automatically.
- **Direct attack through the communication network.** Rather than targeting the mobile device itself, some attacks try to intercept communications to and from the device in order to gain unauthorized use of mobile devices and access to sensitive information.
- **Physical attacks.** Unauthorized individuals may gain possession of lost or stolen devices and have unauthorized use of mobile devices and access sensitive information stored on the device.

---

## A Range of Vulnerabilities Facilitate Attacks

Mobile devices are subject to numerous security vulnerabilities, including a failure to enable password protection, the inability to intercept malware, and operating systems that are not kept up to date with the latest security patches. While not a comprehensive list of all possible vulnerabilities, the following 10 vulnerabilities can be found on all mobile platforms.

- **Mobile devices often do not have passwords enabled.** Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.
- **Two-factor authentication is not always used when conducting sensitive transactions on mobile devices.** According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors"—something you know, something you have, or something you are—before being granted access. Mobile devices themselves can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.
- **Wireless transmissions are not always encrypted.** Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to

---

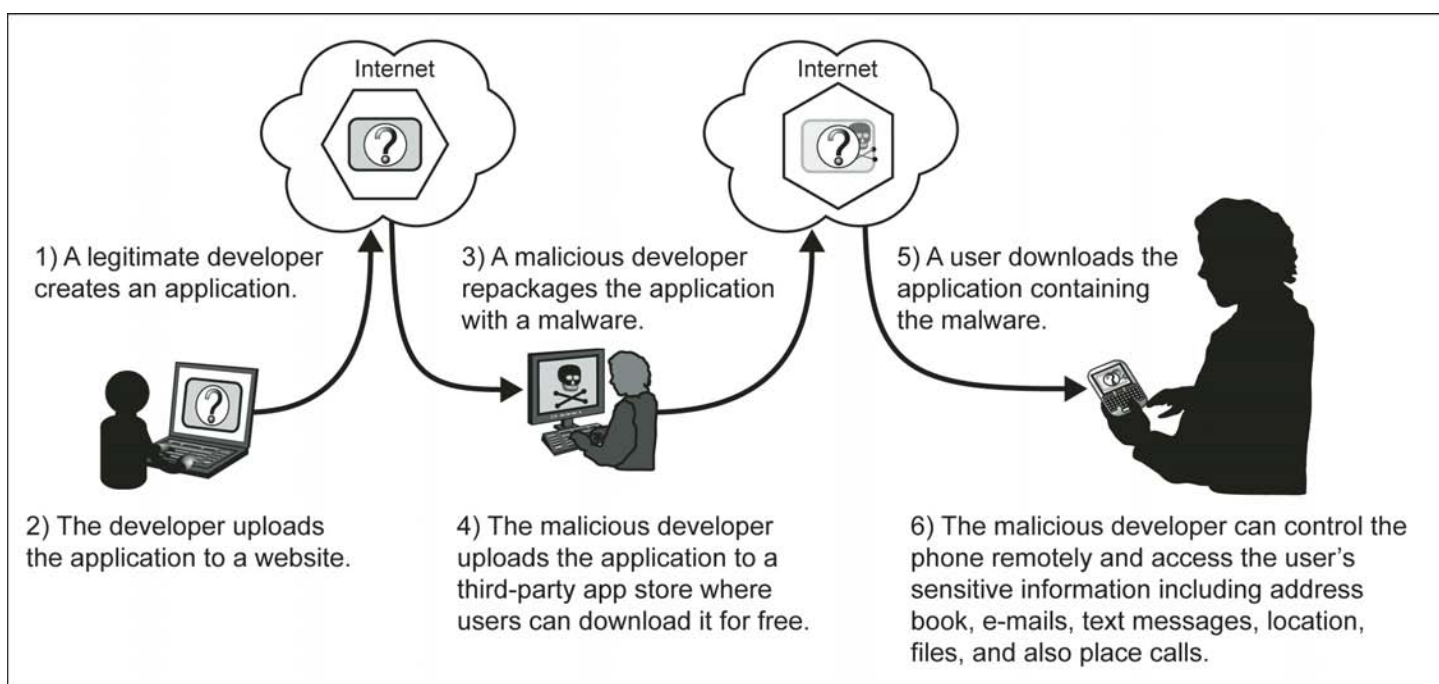
be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using hypertext transfer protocol (http) (rather than secure http),<sup>27</sup> the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.

- **Mobile devices may contain malware.** Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, figure 3 shows how an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device.

---

<sup>27</sup> Http is an application protocol that allows the transmitting and receiving of information across the Internet. While http allows for the quick transmission of information it is not secure and it is possible for a third party to intercept the communication. The secure http protocol encrypts http and was developed to allow the authorization of users and secure transactions.

Figure 3: Repackaging Applications with Malware



Source: GAO analysis of studies and security reports.

- **Mobile devices often do not use security software.** Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam, to lure users into revealing passwords or other confidential information.
- **Operating systems may be out-of-date.** Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update



---

incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.

In addition, mobile devices that are older than 2 years may not receive security updates because manufacturers may no longer support these devices. Many manufacturers stop supporting smartphones as soon as 12 to 18 months after their release. Such devices may face increased risk if manufacturers do not develop patches for newly discovered vulnerabilities.

- **Software on mobile devices may be out-of-date.** Security patches for third-party applications are not always developed and released in a timely manner. In addition, mobile third-party applications, including web browsers, do not always notify consumers when updates are available. Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.
- **Mobile devices often do not limit Internet connections.** Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network it uses communications ports to connect with other devices and the Internet. These ports are similar to doorways to the device. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he or she wants to allow into the mobile device. The firewall intercepts both incoming and outgoing connection attempts and blocks or permits them based on a list of rules. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.
- **Mobile devices may have unauthorized modifications.** The process of modifying a mobile device to remove its limitations so consumers can add additional features (known as "jailbreaking" or "rooting") changes how security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root

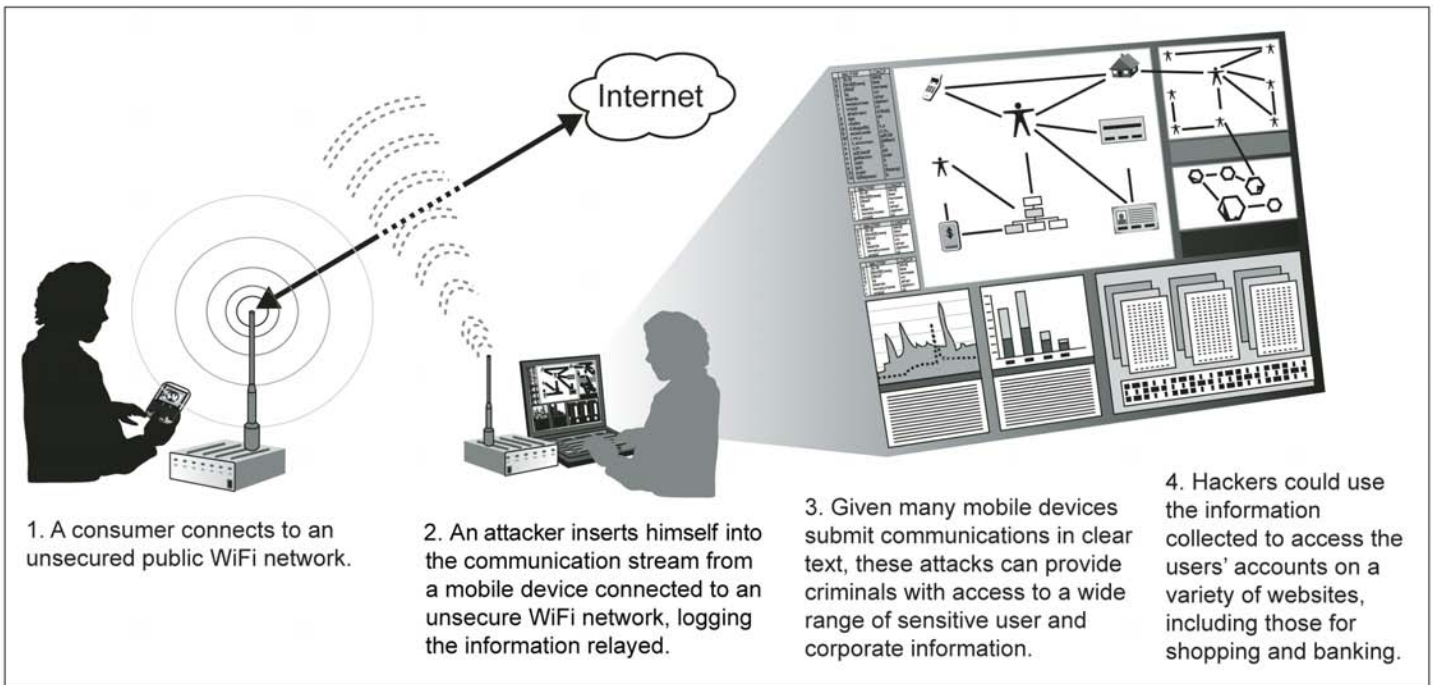
---

their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.

- **Communication channels may be poorly secured.** Having communication channels, such as Bluetooth communications, “open” or in “discovery” mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

In addition, connecting to an unsecured WiFi network could allow an attacker to access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information. For example, figure 4 depicts a man-in-the-middle attack using an unsecured WiFi network. As a result, an attacker within range could connect to a user’s mobile device and access sensitive information.

Figure 4: Man-in-the-Middle Attack Using an Unsecured WiFi Network



Source: GAO analysis of studies and security reports.

The number and variety of threats aimed at mobile devices combined with the vulnerabilities in the way the devices are configured and used by consumers means that consumers face significant risks that the proper functioning of their devices as well as the sensitive information contained on them could be compromised.

## Security Controls and Practices Identified by Experts Can Reduce Vulnerabilities

Mobile device manufacturers and wireless carriers can implement a number of technical features, such as enabling passwords and encryption, to limit or prevent attacks. In addition, consumers can adopt key practices, such as setting passwords, installing software to combat malware, and limiting the use of public wireless connections for sensitive transactions, which also can significantly mitigate the risk that their devices will be compromised.

## Security Controls for Mobile Devices

Table 3 outlines security controls that can be enabled on mobile devices to help protect against common security threats and vulnerabilities. The security controls and practices described are not a comprehensive list, but are consistent with recent studies<sup>28</sup> and guidance from NIST and DHS, as well as recommended practices identified by the FCC CSRIC advisory committee. In addition, security experts, device manufacturers, and wireless carriers agreed that the security controls and practices identified are comprehensive and are in agreement with the lists. Appendix III provides links to federal websites that provide information on mobile security.

**Table 3: Key Security Controls to Combat Common Threats and Vulnerabilities**

Security control	Description
Enable user authentication	Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.
Enable two-factor authentication for sensitive transactions	Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Two-factor authentication provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different “factors”—something you know, something you have, or something you are—before being granted access. Mobile devices themselves can be used as a second factor in some two-factor authentication schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Two-factor authentication may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.
Verify the authenticity of downloaded applications	Procedures can be implemented for assessing the digital signatures <sup>a</sup> of downloaded applications to ensure that they have not been tampered with.
Install antimalware capability	Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards, <sup>p</sup> and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments.
Install a firewall	A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
Receive prompt security updates	Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.

<sup>28</sup>Juniper Networks, Inc., *2011 Mobile Threats Report* (Sunnyvale, Calif.: February 2012), Symantec Corporation, *Internet Security Threat Report, 2011 Trends Vol. 17* (Mountain View, Calif.: April 2012), Lookout Mobile Security, *Lookout Mobile Threat Report* (San Francisco, Calif.: August 2011), McAfee, *Securing Mobile Devices: Present and Future* (Santa Clara, Calif.: 2011).

Security control	Description
Remotely disable lost or stolen devices	Remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the user if they are recovered.
Enable encryption for data stored on device or memory card	File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
Enable whitelisting	Whitelisting is a software control that permits only known safe applications to execute commands.

Source: GAO analysis of guidance from NIST and DHS as well as recommended practices identified by the FCC CSRIC advisory committee.

<sup>a</sup>Digital signatures, or e-signature, are a way to communicate electronically and indicate that the person who claims to have written a message is the one who wrote it.

<sup>b</sup>A secure digital card is a memory card for use in portable devices.

Organizations may face different issues than individual consumers and thus may need to have more extensive security controls in place. For example, organizations may need additional security controls to protect proprietary and other confidential business data that could be stolen from mobile devices and need to ensure that mobile devices connected to the organization's network do not threaten the security of the network itself. Table 4 outlines controls that may be appropriate for organizations to implement to protect their networks, users, and mobile devices.

**Table 4: Additional Security Controls Specific to Organizations to Combat Common Threats and Vulnerabilities**

Security control	Description
Adopt centralized security management	Centralized security management can ensure an organization's mobile devices are compliant with its security policies. Centralized security management includes (1) configuration control, such as installing remote disabling on all devices; and (2) management practices, such as setting policy for individual users or a class of users on specific devices.
Use mobile device integrity validation	Software tools can be used to scan devices for key compromising events (e.g., an unexpected change in the file structure) and then report the results of the scans, including a risk rating and recommended mitigation.
Implement a virtual private network (VPN)	A VPN can provide a secure communications channel for sensitive data transferred across multiple, public networks during remote access. VPNs are useful for wireless technologies because they provide a way to secure wireless local area networks, such as those at public WiFi spot, in homes, or other locations.
Use public key infrastructure (PKI) support	PKI-issued <sup>a</sup> digital certificates can be used to digitally sign and encrypt e-mails.
Require conformance to government specifications	Organizations can require that devices meet government specifications before they are deployed. For example, NIST recommends that mobile devices used in government enterprises adhere to a minimum set of security requirements for cryptographic modules that include both hardware and software components. The Defense Information Systems Agency has certified a secure Android-based mobile system for use by DOD agencies. The system allows DOD personnel to sign, encrypt and decrypt e-mail, and securely access data from a smart phone or tablet computer.

Security control	Description
Install an enterprise firewall	An enterprise firewall can be configured to isolate all unapproved traffic to and from wireless devices.
Monitor incoming traffic	Enterprise information technology network operators can use intrusion prevention software to examine traffic entering the network from mobile devices.
Monitor and control devices	Devices can be monitored and controlled for messaging, data leakage, inappropriate use, and to prevent applications from being installed.
Enable, obtain, and analyze device log files for compliance	Log files can be reviewed to detect suspicious activity and ensure compliance.

Source: GAO analysis of guidance from NIST and DHS as well as recommended practices identified by the FCC CSRIC advisory committee.

<sup>a</sup>PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

## Security Practices for Mobile Devices

In addition to using mobile devices with security controls enabled, consumers can also adopt recommended security practices to mitigate threats and vulnerabilities. Table 5 outlines security practices consumers can adopt to protect the information on their devices. The practices are consistent with guidance from NIST and DHS, as well as recommended practices identified by FCC’s CSRIC advisory committee.

**Table 5: Key Security Practices to Combat Common Threats and Vulnerabilities**

Security practice	Description
Turn off or set Bluetooth connection capabilities to nondiscoverable	When in discoverable mode, Bluetooth-enabled devices are “visible” to other nearby devices, which may alert an attacker to target them. When Bluetooth is turned off or in nondiscoverable mode, the Bluetooth-enabled devices are invisible to other unauthenticated devices.
Limit use of public WiFi networks when conducting sensitive transactions	Attackers may patrol public WiFi networks for unsecured devices or even create malicious WiFi spots designed to attack mobile phones. Public WiFi spots represent an easy channel for hackers to exploit. Users can limit their use of public WiFi networks by not conducting sensitive transactions when connected to them or if connecting to them, using secure, encrypted connections. This can help reduce the risk of attackers obtaining sensitive information such as passwords, bank account numbers, and credit card numbers.
Minimize installation of unnecessary applications	Once installed, applications may be able to access user content and device programming interfaces, and they may also contain vulnerabilities. Users can reduce risk by limiting unnecessary applications.
Configure web accounts to use secure connections	Accounts for many websites can be configured to use secure, encrypted connections. Enabling this feature limits eavesdropping on web sessions.
Do not follow links sent in suspicious e-mail or text messages	Users should not follow links in suspicious e-mail or text messages, because such links may lead to malicious websites.

<b>Security practice</b>	<b>Description</b>
Limit clicking on suspicious advertisements within an application	Suspicious advertisements may include links to malicious websites, prompting the users to download malware, or violate their privacy. Users can limit this risk by not clicking on suspicious advertisements within applications.
Limit exposure of mobile phone numbers	By not posting mobile phone numbers to public websites, users may be able to limit the extent to which attackers can obtain known mobile numbers to attack.
Limit storage of sensitive information on mobile devices	Users can limit storing of sensitive information on mobile devices.
Maintain physical control	Users can take steps to safeguard their mobile devices, such as by keeping their devices secured in a bag to reduce the risk that their mobile devices will be lost or stolen.
Delete all information stored in a device prior to discarding it	By using software tools that thoroughly delete (or “wipe”) information stored in a device before discarding it, users can protect their information from unauthorized access.
Avoid modifying mobile devices	Modifying or “jailbreaking” mobile devices can expose them to security vulnerabilities or can prevent them from receiving security updates.

Source: GAO analysis of guidance from NIST and DHS, as well as recommended practices identified by the FCC CSRIC advisory committee.

Organizations also benefit from establishing security practices for mobile device users. Table 6 outlines additional security practices organizations can take to safeguard mobile devices.

**Table 6: Additional Security Practices Specific to Organizations to Combat Common Threats and Vulnerabilities**

<b>Security practice</b>	<b>Description</b>
Establish a mobile device security policy	Security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, 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.
Provide mobile device security training	Training employees in an organization’s mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
Establish a deployment plan	Following a well-designed deployment plan helps to ensure that security objectives are met.
Perform risk assessments	Risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks on mobile devices.
Perform configuration control and management	Configuration management ensures that mobile devices are protected against the introduction of improper modifications before, during, and after deployment.

Source: GAO analysis of guidance from NIST and DHS, as well as recommended practices identified by the FCC CSRIC advisory committee.

---

## Public and Private-Sector Entities Have Taken Initial Steps to Address Security of Mobile Devices, but Consumers Remain Vulnerable to Threats

Federal agencies and mobile industry companies have taken steps to develop standards for mobile device security and have participated in initiatives to develop and implement certain types of security controls. However, these efforts have been limited in scope, and mobile device manufacturers and carriers do not consistently implement security safeguards on mobile devices. Although FCC has facilitated public-private coordination to address specific challenges, such as cellphone theft, and developed cybersecurity best practices, it has not yet taken similar steps to encourage device manufacturers and wireless carriers to implement a more complete industry baseline of mobile security safeguards. Furthermore, DHS, FTC, NIST, and the private sector have taken steps to raise public awareness about mobile security threats. However, security experts agree that many consumers still do not know how to protect themselves from mobile security vulnerabilities. DHS and NIST have not yet developed performance measures that would allow them to determine whether they are making progress in improving awareness of mobile security issues.

---

## Efforts Have Been Made to Address Security Vulnerabilities, but Controls Are Not Always Implemented

Federal agencies and mobile industry companies have worked to develop best practices and taken steps to address certain aspects of mobile security.

FCC has worked with mobile companies on several initiatives. For example, FCC tasked its advisory committee, CSRIC, with developing cybersecurity best practices, including recommended practices for wireless and mobile security. In March 2011, CSRIC released its report recommending that wireless carriers and device manufacturers consider adopting practices such as:<sup>29</sup>

- working closely and regularly with customers to provide recommendations concerning existing default settings and to identify future default settings that may introduce vulnerabilities;

---

<sup>29</sup>CSRIC, *Working Group 2A Cyber Security Best Practices, Final Report* (Washington, D.C.: March 2011). The CSRIC Working Group's security best practices are mostly technical in nature and the examples provided are high-level examples of wireless and mobile security practices. A copy of the best practices can be obtained from the CSRIC website, date accessed March 13, 2012, <http://transition.fcc.gov/pshs/advisory/csric/>.



- 
- employing fraud detection systems to detect customer calling anomalies (e.g., system access from a single user from widely dispersed geographic areas);
  - having processes in place to ensure that all third-party software has been properly patched with the latest security patches and that the system works correctly with those patches installed;
  - establishing application support for cryptography that is based on open and widely reviewed and implemented encryption algorithms and protocols; and
  - enforcing strong passwords for mobile device access and network access.

In addition, in March 2012 FCC tasked CSRIC with examining three major cybersecurity threats to networks that allow cyber criminals to access Internet traffic for theft of personal information and intellectual property. In response, CSRIC recommended that wireless carriers (1) use key practices when mitigating botnet threats, (2) use best practices for deploying and managing Domain Name System Security Extensions,<sup>30</sup> and (3) develop an industry framework to prevent Internet route hijacking via security weaknesses in the Border Gateway Protocol.<sup>31</sup> CSRIC is working with the wireless carriers to implement these recommendations and is tasked with developing ways to measure the effectiveness of the recommendations.

FCC also tasked the Technological Advisory Council's Wireless Security and Privacy working group to examine mobile security issues, such as vulnerabilities of WiFi networks, security of older generation cellular networks, malicious applications, and text messaging security. The

---

<sup>30</sup>The Domain Name System converts domain names to numerical IP addresses. Security shortcomings in the Domain Name System have enabled spoofing, allowing Internet criminals to steal credit card numbers and personal data from users who do not realize they have been sent to an illegitimate website. Domain Name System Security Extensions have been developed to prevent such fraudulent activity.

<sup>31</sup>The Border Gateway Protocol is the protocol that allows seamless connectivity among the networks that make up the Internet. It does not have built-in security measures. Thus, Internet traffic can be misdirected through potentially untrustworthy networks such as those operated by cyber criminals or by foreign governments.

---

working group is scheduled to issue its recommendations in December 2012.

Moreover, in April 2012, FCC announced that it had reached agreement with the CTIA-the Wireless Association,<sup>32</sup> and multiple wireless carriers to establish processes to deter theft of mobile devices. Under the antitheft agreement, participating wireless carriers are to take several specific actions and submit quarterly progress reports to FCC. For example, the antitheft agreement calls for wireless carriers to initiate, implement, and deploy database solutions by October 31, 2012, to prevent reportedly lost or stolen smartphones from being used on another wireless network. The FCC plans to monitor progress in developing these databases and CTIA agreed to report progress quarterly, beginning June 30, 2012. The agreement also will result in the launch of a public education campaign by July 1, 2012, to inform consumers about the ability to lock or locate and erase data from a smartphone.

In addition, wireless carriers and device manufacturers reported that they participate in private-sector standards-setting organizations, which have addressed aspects of mobile security. For example, the Open Mobile Alliance, an industry standards group, has developed a specification to provide a common means for mobile developers to implement standards for secure and reliable data transport between two communicating parties. Furthermore, a consortium of wireless carriers and mobile device manufacturers known as the Messaging, Malware and Mobile Anti-Abuse Working Group<sup>33</sup> has an initiative underway to address text-message-based spam. Under this initiative, wireless carriers encourage customers to forward spam text messages back to the carriers, who can use the messages to identify the source of spam and take corrective action to block its content from their networks. According to FCC officials, the current chairman of the Messaging, Malware and Mobile Anti-Abuse

---

<sup>32</sup>CTIA is an international nonprofit membership organization that has represented the wireless communications industry since 1984. Membership in the association includes wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products.

<sup>33</sup>The Messaging, Malware and Mobile Anti-Abuse Working Group, whose members include wireless carriers and handset manufacturers, among others, is a private organization that collaborates to address online challenges such as web messaging abuse and botnets.

---

Despite Efforts, Mobile Security Safeguards Are Not Always Implemented

---

Working Group is a member of CSRIC and the chair of the working group that developed recommended solutions for the botnet threats.

While private and public sector entities have initiated activities to identify mobile security safeguards, these safeguards are not always available on mobile devices or activated by users. According to a 2012 study by NQ Mobile and the National Cyber Security Alliance (NCSA),<sup>34</sup> approximately 30 percent of respondents<sup>35</sup> said they did not have mobile security features on their smartphones.<sup>36</sup> In addition, approximately 66 percent of respondents did not report that they activated password protection on their devices to prevent unauthorized access and that at least 67 percent did not report activating a remote-wipe or remote-locate security feature. Security company representatives told us that these results were generally consistent with their experiences and observations.

In addition, mobile device manufacturers and wireless carriers do not consistently implement or activate security safeguards on their mobile devices. According to most of the device manufacturers and several wireless carriers we spoke with, safeguards such as passwords, encryption, and remote wipe/lock/locate can be made available on their mobile devices, although one wireless carrier noted that encryption might be inappropriate for certain types of devices. Several of these companies also acknowledged that it is possible to preconfigure mobile devices to prompt the user to implement safeguards when the phone is first set up. However, with the exception of password protection for online voicemail accounts, none of the device manufacturers or wireless carriers stated that they generally configure their devices to prompt the user to implement these controls. We also observed that general cybersecurity instructions were not directly accessible from either carriers or device manufacturers, although instructions for implementing controls could be

---

<sup>34</sup>The NCSA is a nonprofit organization whose mission is to promote secure and safe use of the Internet. NCSA leadership includes several private companies, including two major wireless carriers.

<sup>35</sup>NQ Mobile and National Cyber Security Alliance, *Report on Consumer Behaviors and Perceptions of Mobile Security* (Jan. 25, 2012), date accessed April 10, 2012, [http://docs.nq.com/NQ\\_Mobile\\_Security\\_Survey\\_Jan2012.pdf](http://docs.nq.com/NQ_Mobile_Security_Survey_Jan2012.pdf).

<sup>36</sup>Participants in this web survey had Internet access and were recruited from visitors to selected websites and other sources. The survey is not based on a random probability sample and is not necessarily representative of the larger population of cellphone users in the United States. See app. I for additional information about this survey.

---

---

**FCC Has Facilitated Industry Best Practice Efforts but Has Not Yet Encouraged Broad Implementation of Mobile Security Safeguards**

found by searching the company's website for information about individual models of smartphones.

FCC has the ability to encourage broad implementation of mobile security safeguards among mobile industry companies. While it has taken steps to encourage implementation of safeguards in certain areas, it has not yet taken similar steps to encourage industry implementation of a broad baseline of mobile security safeguards. For example, in its recent antitheft agreement with CTIA, and participating wireless carriers, FCC took an active role in encouraging major wireless carriers to adopt specific procedures to discourage the theft of mobile devices. This effort demonstrates that FCC can facilitate private sector efforts to establish an industry baseline and milestones for addressing mobile security challenges. Moreover, representatives from multiple companies agreed that FCC could play a role in coordinating private sector efforts to improve mobile security.

FCC has also facilitated private sector efforts to establish cybersecurity best practices in areas not specific to mobile security. As mentioned previously, FCC tasked CSRIC to review best practices for botnet threats, Domain Name System attacks, and Internet route hijacking. CSRIC developed voluntary recommendations in these areas and has been working with wireless carriers to implement them. According to FCC officials, wireless carriers representing 90 percent of the domestic customer base have committed to adopting and using these practices. Although these recommendations are not specific to mobile devices, FCC officials stated that the process of seeking voluntary compliance from carriers had been successful and demonstrated the willingness of carriers to adopt best practices.

FCC officials stated that they hope to have the same cooperation from wireless carriers when the Technological Advisory Council's Wireless Security and Privacy working group releases its recommendations on mobile security issues, scheduled for December 2012. While it is not clear that the working group will develop a baseline of recommended practices for implementation by mobile industry companies, the council's recommendations nevertheless could be part of such a baseline.

Another candidate for a set of baseline mobile security standards that mobile industry companies could be encouraged to implement is the collection of cybersecurity best practices developed by CSRIC in 2011. Those practices have not yet been adopted as a baseline within the mobile industry. FCC officials from the Public Safety and Homeland

---

Security Bureau stated that they had not yet taken action to promote this specific set of recommended practices, although they had held informal meetings with industry to discuss the implementation of cybersecurity practices. Whether mobile industry companies adopt the CSRIC-recommended practices or choose other baseline practices and controls, it will be important for FCC to encourage industry to adopt recommended practices. If such practices are not implemented, vulnerabilities in mobile devices are likely to continue to pose risks for consumers.

---

### The Effectiveness of Public and Private Sector Efforts to Raise Awareness about Mobile Security Is Unclear

Many of the key practices that have been identified as effective in mitigating mobile security risks depend on the active participation of users. Thus it is important that an appropriate level of awareness is achieved among consumers who use mobile devices on a regular basis. To address this need, federal agencies have developed and distributed a variety of educational materials. For example:

- DHS's US-Computer Emergency Readiness Team (US-CERT) has developed cybersecurity tip sheets and technical papers related to mobile security. These materials, which are published on the US-CERT website, provide lists of suggestions, such as the use of passwords and encryption, to help consumers to protect their devices and sensitive data from network attacks and theft.<sup>37</sup>
- DHS coordinates domestic and international engagements and cybersecurity outreach endeavors. For example, as the lead agency for the awareness component of the NICE initiative, DHS coordinates the National Cyber Security Awareness Month and a national cybersecurity public awareness campaign called "Stop. Think. Connect." As part of these efforts, DHS has developed educational materials that, although not specifically related to mobile security, encourage users to adopt safe practices when using the Internet. The DHS website related to this effort also provides links to educational materials hosted on third-party websites, such as StaySafeOnline.org.

---

<sup>37</sup>Examples of US-CERT tip sheets include *Protecting Portable Devices: Data Security*, date accessed March 19, 2012, <http://www.us-cert.gov/cas/tips/ST04-020.html>; and *Protecting Portable Devices: Physical Security*, date accessed July 3, 2012, <http://www.us-cert.gov/cas/tips/ST04-017.html>.

- 
- FTC manages the OnGuardOnline website,<sup>38</sup> which provides individuals with information about how to use the Internet in a safe, secure, and responsible manner. As part of this effort, FTC has developed educational materials specifically related to mobile security, such as avoiding malicious mobile applications and protecting children who use mobile devices.<sup>39</sup> In addition, FTC and DHS have developed and distributed printed cybersecurity guides to schools, business, and other entities, according to an FTC staff member.
  - NIST published guidelines on the security of cellphones and personal digital assistants in 2008.<sup>40</sup> Among other things, this guidance provides users with information about how to secure their devices. For example, the guidance discusses the value of implementing authentication (e.g., password protection) and remotely erasing or locking devices that are lost or stolen.

DHS and nonprofit organizations also have developed and distributed cybersecurity educational materials in collaboration with NCSA. In addition to funding from the private sector, DHS officials stated that DHS has contributed a grant to NCSA to conduct surveys and other activities. NCSA has produced educational materials that specifically relate to mobile security. For example, NCSA's website provides tips that individuals can follow to protect their mobile devices such as avoiding malware, using trusted internet connections, and securing personal information through the use of strong passwords.

Other private sector organizations have also developed educational materials related to securing mobile devices. For example, the Global System for Mobile Communications Association has published articles targeted towards mobile phone users on topics, such as (1) preventing

---

<sup>38</sup>The OnGuardOnline website can be accessed at <http://onguardonline.gov/>, date accessed August 9, 2012.

<sup>39</sup>*Understanding Mobile Apps* (September 2011), date accessed June 14, 2012, <http://onguardonline.gov/articles/0018-understanding-mobile-apps>; *Kids and Mobile Phones* (September 2011), date accessed June 14, 2012, <http://onguardonline.gov/articles/0025-kids-and-mobile-phones>.

<sup>40</sup>NIST, *Special Publication 800-124, Guidelines on Cell Phone and PDA Security* (October 2008). According to NIST officials, they are revising this publication and will release a draft update in fiscal year 2012.

---

mobile phone theft, (2) spam and mobile phones, and (3) computer viruses and mobile phones.<sup>41</sup> Similarly, CTIA maintains a blog with information on topics such as establishing passwords and using applications that can track, locate, lock, and/or wipe wireless devices that are lost or stolen. In addition, as part of the antitheft initiative discussed above, CTIA agreed that its members would implement a system to inform users about security safeguards on mobile devices as well as launch an education campaign regarding the safe use of smartphones.

Despite the efforts underway by the federal government and the private sector to develop and distribute educational materials, it is unclear whether consumer awareness has improved as a result. Representatives from companies that specialize in information security told us that many consumers do not understand the importance of implementing mobile security safeguards or do not know how to implement them. Their views are consistent with the results of the 2012 NCSA study, which suggested that many mobile users do not know how to implement mobile security safeguards. The survey reported that more than half of respondents felt that they required additional information in order to select and/or implement security solutions for their mobile devices. Further, the study reported that approximately three-quarters of respondents reported that they did not receive information about the need for security solutions at the time they purchased their phone. The survey did not include data that would indicate whether consumer awareness had improved or worsened over time.

#### DHS and NIST Have Not Determined Whether Efforts Are Improving Consumer Awareness

While DHS and NIST have conducted or supported several consumer cybersecurity awareness efforts, neither has developed outcome-oriented performance measures to assess the effectiveness of government efforts to enhance consumer awareness of mobile security. An outcome-oriented performance measure is an assessment of the result, effect, or consequence that will occur from carrying out a program or activity compared to its intended purpose. NIST officials stated that they do not currently measure progress related to awareness activities associated with NICE. Furthermore, although DHS officials stated that the department assesses the effectiveness of several of the awareness activities, these assessments are not based on outcome-oriented measures. For example, DHS officials stated that they assess the “Stop.

---

<sup>41</sup>GSMA, *Security Advice for Mobile Phone Users*, date accessed June 14, 2012, <http://www.gsma.com/security-advice-for-mobile-phone-users>.

---

Think. Connect.” events by (1) the number of individuals who join the campaign and agree to receive additional information, such as newsletters, concerning cybersecurity; (2) the total number of events held; (3) the number of agencies and states that join the campaign; and (4) the number of times the campaign website is visited. However, these measures are not outcome-oriented because they do not indicate how, if at all, these activities have (1) improved citizens’ knowledge about managing online risk, (2) improved knowledge of cybersecurity within organizations, or (3) enabled access to cybersecurity resources.

To develop measures of the impact of government efforts on consumer awareness of mobile security issues, a baseline measure of consumer awareness would be needed from which to mark progress. However, neither DHS nor NIST has developed a baseline measure of the state of national cybersecurity awareness. Establishing a baseline measure and regularly assessing consumer awareness and behavior regarding a particular issue can enable organizations to document where problems exist, identify causes, prioritize efforts, and monitor progress. DHS officials stated that the department has considered conducting a study on consumer behavior and awareness related to general cybersecurity but has not yet done so.

Without a baseline measure of consumer awareness, it will remain difficult for NIST and DHS to measure any correlation between the government’s activities and enhanced consumer awareness. Further, without outcome-oriented performance measures, the government will be limited in its ability to determine whether it is achieving its identified goals and objectives, including whether cybersecurity awareness efforts are effective at increasing adoption of recommended security practices.

---

## Conclusions

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers.

Private sector entities and relevant federal agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices. However, security controls are not always consistently implemented on mobile devices, and it is unclear whether consumers are aware of the importance of enabling security controls on their devices and adopting recommended practices.



---

Although FCC has taken steps to work with industry to develop cybersecurity best practices, it has not yet taken steps to encourage wireless carriers and device manufacturers to implement a more complete industry baseline of mobile security safeguards, and NIST and DHS have not determined whether consumer awareness of mobile security issues has improved since the government's efforts have been initiated.

---

## Recommendations for Executive Action

To help mitigate vulnerabilities in mobile devices, we recommend that the Chairman of the Federal Communications Commission

- continue to work with wireless carriers and device manufacturers on implementing cybersecurity best practices by encouraging them to implement a complete industry baseline of mobile security safeguards based on commonly accepted security features and practices; and
- monitor progress of wireless carriers and device manufacturers in achieving their milestones and time frames once an industry baseline of mobile security safeguards has been implemented.

To determine whether the NICE initiative is having a beneficial effect in enhancing consumer awareness of mobile security issues, we recommend that the Secretary of Homeland Security in collaboration with the Secretary of Commerce

- establish a baseline measure of consumer awareness and behavior related to mobile security and
- develop performance measures that use the awareness baseline to assess the effectiveness of the awareness component of the NICE initiative.

---

## Agency Comments and Our Evaluation

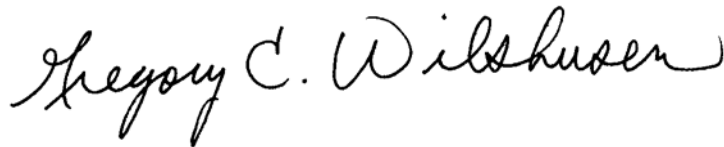
We received written comments on a draft of this report from the Chief of FCC's Public Safety and Homeland Security Bureau, the Director of DHS's Departmental GAO-OIG Liaison Office, and the Acting Secretary of Commerce. These officials generally concurred with our recommendations and provided technical comments, which we have considered and incorporated as appropriate into the final report. FTC did not provide written comments on the draft report, but an attorney in FTC's Office of the General Counsel did provide technical comments in an e-mail that we addressed as appropriate. DOD did not provide comments on the draft report. The comments we received are summarized below.

- 
- In addition to FCC's written comments, the Chief of FCC's Public Safety and Homeland Security Bureau stated in e-mail comments that the commission generally concurred with our recommendations that it encourage wireless carriers and device manufacturers to implement a complete industry baseline of mobile security safeguards; and to monitor progress of wireless carriers and device manufacturers in achieving their milestones and time frames once a baseline has been implemented. In the written comments, the Chief added that FCC has facilitated private sector efforts, for example, through advisory committees such as CSRIC to establish and promote the implementation of cybersecurity best practices that secure the underlying Internet infrastructure. FCC officials also provided preliminary oral and written technical comments, which we addressed as appropriate (FCC's written comments are reprinted in app. II).
  - The Director of DHS's Departmental GAO-OIG Liaison Office provided written comments in which the department concurred with our recommendations that it work with Commerce to establish a baseline measure of consumer awareness and behavior related to mobile security and develop performance measures that use the baseline to assess the effectiveness of the awareness component of the NICE initiative. He stated that the department will coordinate with its counterparts at Commerce to assess the feasibility of different methods to create a baseline measure of consumer awareness and continue to promote initiatives to educate the public about cybersecurity. He also stated that the department will coordinate with its NIST counterparts on the development of performance measures using the awareness campaign and other methods. He also provided technical comments, which we have incorporated as appropriate (DHS's comments are reprinted in app. III).
  - The Acting Secretary of Commerce provided written comments in which the department concurred in principle with our recommendations that NIST work with DHS to establish a baseline measure of consumer awareness and behavior related to mobile security and that it develop performance measures that use the baseline to assess the effectiveness of the awareness component of the NICE initiative. The Acting Secretary provided technical comments and asked that we consider replacing "baseline understanding" with "baseline measure," which we have incorporated into the final report. She also provided suggested revised text. However, we believe that the information in the draft is correct and communicates appropriately as written. Therefore, we have not added the suggested text (Commerce's comments are reprinted in app. IV).

---

We are sending copies of this report to the appropriate congressional committees; the Chairmen of the Federal Communications Commission and Federal Trade Commission; the Secretaries of Commerce, Defense, and Homeland Security; and other interested congressional parties. The report also is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact: Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499, or by e-mail at [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov) or [barkakatin@gao.gov](mailto: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 VI.



Gregory C. Wilshusen  
Director  
Information Security Issues



Dr. Nabajyoti Barkakati  
Chief Technologist

---

# Appendix I: Objectives, Scope, and Methodology

---

The objectives of our review were to determine: (1) what common security threats and vulnerabilities currently exist in mobile devices, (2) what security features are currently available and what practices have been identified to mitigate the risks associated with these vulnerabilities, and (3) the extent to which government and private entities are addressing security vulnerabilities of mobile devices.

To determine the common security threats and vulnerabilities that currently exist in mobile devices (cellphones, smartphones, and tablets), as well as security features and practices to mitigate them, we identified agencies and private companies with responsibilities in the telecommunication and cybersecurity arena, and reviewed and analyzed information security-related websites, white papers, and mobile security studies. We interviewed officials, and obtained and analyzed documentation from the Federal Communications Commission (FCC), Department of Homeland Security (DHS), Department of Defense (DOD), Department of Commerce (Commerce), and Federal Trade Commission (FTC) to determine the extent to which they have identified mobile security vulnerabilities and developed standards and guidance on the security of mobile devices. We interviewed and obtained documents from an industry group and an advisory council, both of which have representation from the telecommunication industry; these included the CTIA-The Wireless Association and the Communications Security, Reliability, and Interoperability Council (CSRIC). We also analyzed information from the US-Computer Emergency Readiness Team (US-CERT) and the National Vulnerability Database on mobile security vulnerabilities.

Further, we obtained input from the private companies who make up the largest market share for mobile devices in the United States to determine what steps they are taking to provide security for their mobile devices. These included mobile device manufacturers—HTC Corporation, Research In Motion, Corp, Motorola Mobility Inc., Samsung, and LG Electronics—as well as wireless carriers—Verizon Wireless, AT&T Inc., T-Mobile USA Inc., and Sprint. We also met with representatives of information security companies, including Symantec Corporation and Juniper Networks. We approached Apple Inc. and Google Inc.; however, Apple officials did not agree to meet with us and Google officials did not provide responses to our questions. We developed draft lists of common vulnerabilities and security practices based on our analysis of government security guidance as well as private sector studies and reports. We provided copies of these lists to each of the companies listed above and addressed their comments as appropriate.

To determine the extent to which government and private entities are addressing security vulnerabilities of mobile devices, we analyzed statutes and regulations to determine federal roles related to mobile security. In order to identify initiatives related to improving mobile security or raising consumer awareness, we interviewed the federal and private sector officials mentioned above, and members of a private sector working group devoted to mobile security issues, known as the Messaging, Malware, and Mobile Anti-Abuse Working Group. In addition, we analyzed multiple studies related to consumer attitudes and practices related to mobile devices. Specifically, we assessed available methodological information against general criteria for survey quality and relevant principles derived from the Office of Management and Budget (OMB) Standards and Guidelines for Statistical Surveys. Because the available methodological documentation did not allow us to fully assess the quality of the survey data, the risk of error in the surveys makes it possible that reported results may not be very accurate or precise. Although we corroborated the study's general findings with information security experts, readers should be cautious in drawing conclusions based on these results.

We conducted this performance audit from November 2011 to September 2012 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 Federal Communications Commission



Federal Communications Commission  
Washington, D.C. 20554

August 17, 2012

Mr. John de Ferrari  
U.S. Government Accountability Office  
441 G St., N.W.  
Washington, D.C. 20548

Re: FCC Response to GAO Revisions

Dear Mr. De Ferrari:

Thank you for the opportunity to review the United States Government Accountability Office's draft (GAO) Report to Congressional Requesters entitled "Better Implementation of Controls for Mobile Devices Should Be Encouraged."

The Federal Communications Commission (FCC) takes the security of our Nation's communications networks – both wired and wireless – seriously. The FCC has facilitated private-sector efforts, for example, through advisory committees such as the Communications Security, Reliability and Interoperability Council (CSRIC) to establish and promote the implementation of cybersecurity best practices that secure the underlying Internet infrastructure. The best practices have resulted in improved security for all communications technologies, including mobile. As discussed previously, the Commission is committed to continuing these efforts with respect to mobile security vulnerabilities.

The FCC appreciates GAO's willingness to consider our comments regarding the draft report and to discuss them with us on Monday, August 13. We submitted initial comments to you on August 15, 2012. In response, on August 16, 2012, you sent proposed revisions to the draft. We have reviewed those revisions and believe they capture the essence of our discussions earlier this week. We do, however, have a few suggested changes for your consideration. These are included in the attached document and are highlighted in yellow. We believe these changes will improve the accuracy of the report.

Again, thank you for the opportunity to review the draft report.

Sincerely,

A handwritten signature in black ink that reads "David Turetsky".

David Turetsky  
Chief  
Public Safety and Homeland Security Bureau

# Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

August 17, 2012

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

Re: Draft Report GAO 12-757, "INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be Encouraged"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the National Protection & Programs Directorate's (NPPD's) Office of Cybersecurity and Communications' (CS&C) current awareness initiatives regarding mobile security awareness. DHS views mobile security as an important area for current and future public concern; however, it remains only one part of the Department's broader efforts to raise public awareness about safe practices in cyberspace.

The National Strategy to Secure Cyberspace tasks DHS with promoting a comprehensive national awareness program to empower Americans to secure their own parts of cyberspace. As the lead for the awareness component of the National Initiative for Cybersecurity Education (NICE), DHS has fulfilled this mission by promoting cybersecurity and responsible use of the Internet through public service campaigns and collaboration with the private sector. As the report states, mobile security is currently part of the collaboration taking place between DHS and private-sector partners and will remain integrated into awareness operations within DHS/NPPD.

The draft report contained two recommendations directly involving DHS, with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security, in collaboration with the Secretary of Commerce:

**Recommendation 1:** Establish a baseline measure of consumer awareness and behavior related to mobile security.

**Response:** Concur. DHS, led by NPPD/CS&C personnel, will work with its Department of Commerce counterparts to assess the feasibility of different methods to create a baseline measure of consumer awareness. DHS already uses measures, such as the number of individuals who join

the Stop.Think.Connect.™ Campaign, to determine the scope and reach of the general awareness campaign. To reiterate, the Campaign is a national public awareness effort to guide the Nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing safe online habits. It seeks to have Americans view Internet safety as a shared responsibility—at home, in the workplace, and in our communities—and demonstrate that responsibility by bringing together a coalition of federal, state and local government entities, as well as private-sector and nonprofit partners.

DHS will continue to promote initiatives to educate the public about cybersecurity. While it is difficult to measure the extent to which individuals have changed their Internet and mobile security habits, the Department believes it has produced, and will continue to produce, demonstrable benefits for the American people to help them understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior. More specifically, the Campaign aims to:

- Elevate the Nation's awareness of cybersecurity and its association with national security and the safety of our personal lives,
- Engage the American public, the private sector, and state and local governments in our Nation's effort to improve cybersecurity, and
- Communicate approaches and strategies for the public to keep themselves, their families and their communities safer online.

**Recommendation 2:** Develop performance measures that use the awareness baseline to assess the effectiveness of the awareness component of the NICE initiative.

**Response:** Concur. NPPD/CS&C personnel are currently engaging with their National Institute of Standards and Technology (NIST) counterparts, on the development of performance measures using the awareness campaign and other methods. NPPD and NIST have developed draft indicators which will assist with the development of one or more measures best suited for consumer awareness. Currently, we envision beginning to collect metrics by the end of FY2013.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker  
Director  
Departmental GAO-OIG Liaison Office



# Appendix IV: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE  
The Secretary of Commerce  
Washington, D.C. 20230

August 13, 2012

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: Better Implementation of Controls for Mobile Devices Should be Encouraged (GAO-12-757)*.

Staff members from the Information Technology Laboratory at the National Institute of Standards and Technology (NIST) have reviewed the draft report and concur in principle with the draft report and recommendations. The following are comments regarding GAO's conclusions:

1. Page 39, last paragraph. The GAO Draft uses the terms "baseline measure" and "baseline understanding" in a way that implies that they are interchangeable. The actual paragraph is shown below:

"To develop measures of the impact of government efforts on consumer awareness of mobile security issues, a baseline measure of consumer awareness would be needed from which to mark progress. However, neither DHS nor NIST have developed a baseline understanding of the state of national cybersecurity awareness. Establishing a baseline understanding and regularly assessing consumer awareness and behavior of the status of a particular issue can enable organizations to document where problems exist, identify causes, prioritize efforts, and monitor progress."

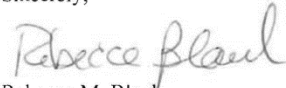
Please consider replacing "baseline understanding" with "baseline measure" throughout this paragraph as the measure will be a mechanism to enable greater understanding. A suggested replacement paragraph is shown below:

"To understand the impact of government efforts on consumer awareness of mobile security issues, a baseline measure of consumer awareness would be needed from which to mark progress. However, neither DHS nor NIST have developed a baseline measure of the state of national cybersecurity awareness. Establishing a baseline measure and regularly assessing it can enable organizations to understand where consumer awareness deficiencies exist and to prioritize efforts to eliminate those deficiencies."

Mr. Gregory C. Wilshusen  
Page 2

We welcome further communications with GAO regarding its conclusion and look forward to receiving the final report. If you have any questions regarding this response, please contact Dan Cipra of NIST at (301) 975-3649.

Sincerely,



Rebecca M. Blank  
Acting Secretary of Commerce

# Appendix V: Federal Websites for Information Related to Mobile Security

The table below provides information and website links to federal sites that include information related to mobile security. Website links are current as of July 10, 2012.

**Table 7: Federal Websites and Links to Information Related to Mobile Security**

Agency	Information related to mobile security	Links
DOD	DOD maintains a website on Security Technical Implementation Guides, which contain technical guidance to secure information systems or software that might otherwise be vulnerable to a malicious computer attack. In addition, the guides address aspects of mobile device security.	<a href="http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html">http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html</a>
DHS	DHS maintains a website called Cybersecurity Tips that provides general cybersecurity tips as well as a section specific to mobile devices. DHS also launched a website to promote the “Stop.Think.Connect.” initiative. This website provides information to visitors on the initiative itself, top security issues, cybersecurity tips, and links to additional resources. US-CERT also maintains a website with cybersecurity tips. Information on threats to the security of mobile devices is available in addition to more general cybersecurity information.	<a href="http://www.dhs.gov/files/events/cybersecurity-tips.shtm">http://www.dhs.gov/files/events/cybersecurity-tips.shtm</a> <a href="http://www.dhs.gov/files/events/stop-think-connect.shtm">http://www.dhs.gov/files/events/stop-think-connect.shtm</a> <a href="http://www.us-cert.gov/cas/tips">http://www.us-cert.gov/cas/tips</a> <a href="http://www.us-cert.gov/cas/tips/ST04-017.html">http://www.us-cert.gov/cas/tips/ST04-017.html</a> <a href="http://www.us-cert.gov/cas/tips/ST04-020.html">http://www.us-cert.gov/cas/tips/ST04-020.html</a>
FCC	FCC maintains a website with public safety tech topics that provides detailed information on the threats and vulnerabilities associated with the use of various communication technologies, including mobile devices.	<a href="http://www.fcc.gov/guides/stolen-and-lost-wireless-devices">http://www.fcc.gov/guides/stolen-and-lost-wireless-devices</a> <a href="http://www.fcc.gov/help/topic/106">http://www.fcc.gov/help/topic/106</a> <a href="http://www.fcc.gov/help/public-safety-tech-topic-23-femtocells">http://www.fcc.gov/help/public-safety-tech-topic-23-femtocells</a> <a href="http://transition.fcc.gov/pshs/techtopics/">http://transition.fcc.gov/pshs/techtopics/</a>
FTC	FTC maintains a list of consumer publications as well as links to information on information security. The website “OnGuard Online” provides information for consumers to protect their devices while on the Internet. In addition, the FTC website has tips on how to properly dispose of mobile devices.	<a href="http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/consumer-publications.html">http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/consumer-publications.html</a> <a href="http://www.ftc.gov/bcp/menus/consumer/data/privacy.shtm">http://www.ftc.gov/bcp/menus/consumer/data/privacy.shtm</a> <a href="http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm">http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm</a>

---

**Appendix V: Federal Websites for Information  
Related to Mobile Security**

---

<b>Agency</b>	<b>Information related to mobile security</b>	<b>Links</b>
NIST	NIST's homepage has a publications link that directs customers to a web page containing a publications search engine. This search engine enables customers to search through a database of publications, related to cybersecurity, maintained by NIST. One of the publications located within this database details information about the threats and technology risks associated with the use of mobile devices and available safeguards to mitigate them (Guidelines on Cell Phone and PDA Security Special Publication 800-124).	<a href="http://csrc.nist.gov/groups/SNS/mobile_security/publications.html">http://csrc.nist.gov/groups/SNS/mobile_security/publications.html</a> <a href="http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf">http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf</a>

---

Source: GAO analysis of federal websites related to mobile security.

---

# Appendix VI: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Gregory C. Wilshusen, (202) 512-6244, or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov)

Dr. Nabajyoti Barkakati, (202) 512-4499, or [barkakatin@gao.gov](mailto:barkakatin@gao.gov)

---

## Staff Acknowledgments

In addition to the individuals named above, key contributions to this report were made by John de Ferrari (Assistant Director), West E. Coile, Neil J. Doherty, Rebecca E. Eyler, Richard J. Hagerman, Tammi N. Kalugdan, David F. Plocher, Carl M. Ramirez, Meredith R. Raymond, and Brandon C. Sanders.

---

## 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 website ([www.gao.gov](http://www.gao.gov)). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to [www.gao.gov](http://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 website, <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.

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@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](mailto:youngc1@gao.gov), (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

