THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

WIRELESS TASK FORCE REPORT

Wireless Security

January 2003

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Numerous wireless technologies are being used to transmit voice, data, and video in support of national security and emergency preparedness (NS/EP) operations. As a result, the NS/EP community needs to identify its security requirements and understand potential wireless vulnerabilities to that security.

The President's National Security Telecommunications Advisory Committee (NSTAC) Wireless Task Force (WTF) was tasked to determine how the NS/EP user can operate in a secure environment and to provide conclusions and recommendations to the President regarding wireless security. To adequately discuss these subjects and formulate actionable recommendations designed to help offset wireless threats and vulnerabilities, the WTF agreed to—

- Define the terms "wireless" and "wireless security"
- Identify NS/EP wireless users' unique requirements
- Compile a list of wireless vulnerabilities and threats
- Where known, identify mitigation approaches to address wireless vulnerabilities and threats.

Using subject matter experts from NSTAC member companies, other information technology companies, industry associations, and Government participants, the WTF studied the issue of wireless security. The WTF noted that wireless security challenges exist at many levels, including product design, wireless standards, and wireless/Internet convergence. Based on its analysis of issues related to wireless security, the NSTAC offers the following recommendations.

The NSTAC recommends that the President—

- Direct Federal departments and agencies to construct mitigation and alleviation policies regarding wireless vulnerabilities and further consider the applicability of the recent National Institute of Standards and Technology and Department of Defense's wireless security policies to all Federal departments and agencies.[1]
- Direct Government chief information officers to immediately emphasize enterprise management controls, with respect to wireless devices, to ensure that appropriate security controls are implemented, given that the banning of wireless devices is counterproductive and ignores the efficiency that such devices bring to users.

[1] Recent wireless security policies include: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-46, "Security for Telecommuting and Broadband Communications," September 2002; NIST SP 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices," (November 2002); and Draft Department of Defense (DoD) Directive 8100.bb, "Use of Commercial Devices, Services, and Technologies in the DoD Global Information Grid (GIG)," July 15, 2002.

- Direct Federal departments and agencies to work in concert with industry to develop security principles and to resolve security-related deficiencies in wireless devices when employed by NS/EP users.
- Direct Federal departments and agencies using wireless communications to address wireless security threats and vulnerabilities. In addition, consider the end-to-end security of their respective communications and information system capabilities.
- Direct Federal departments and agencies using wireless communications to purchase and implement fully tested and compliant secure wireless products and services.
- Direct appropriate staff to advocate funding initiatives for replacing nonsecure analog with secure digital NS/EP equipment and systems.
- Direct Federal departments and agencies using microwave communications facilities to address unprotected link security vulnerabilities. In addition, advise State and local governments and other critical infrastructure providers of the vulnerability of unprotected microwave communications as part of the Homeland Security initiative.
- Establish policies regarding the public availability and dissemination of Federal critical infrastructure information (such as the policies on Internet availability of Federal Communications Commission and the Federal Aviation Administration databases of tower locations).

1.0 INTRODUCTION AND CHARGE

Numerous wireless technologies are being used with greater regularity to transmit voice, data, and video in support of national security and emergency preparedness (NS/EP) operations. However, there are increasing concerns that wireless communications could expose NS/EP users to new security threats and vulnerabilities. As such, the NS/EP community needs to understand its security requirements and identify potential wireless vulnerabilities.

Challenges exist at many levels, including product design, wireless standards, and wireless/Internet convergence. First, the wide use of commercial off-the-shelf (COTS) products and legacy equipment by the NS/EP community is an important consideration because these devices and equipment were not designed with NS/EP security requirements in mind and sometimes without security features at all. Second, interoperability issues arise from the implementation of different security models and standards — for instance, there are several conflicting policies, either established or in development, designed to inhibit or prohibit the use of particular wireless capabilities and connectivity to classified networks and computers. Third, the extension of the Internet into the wireless domain adds new security challenges.

The purpose of this report by the President's National Security Telecommunications Advisory Committee (NSTAC) Wireless Task Force (WTF) is to determine how the NS/EP user can operate in a secure environment and to provide conclusions and recommendations to the President regarding wireless security. To adequately discuss these subjects and formulate actionable recommendations designed to help offset wireless threats and vulnerabilities, the WTF agreed to—

- Define the terms "wireless" and "wireless security"
- Identify NS/EP wireless users' unique requirements
- Compile a list of wireless vulnerabilities and threats
- Where known, identify mitigation approaches to address wireless vulnerabilities and threats.

1.1 Background

During past cycles, the NSTAC investigated secure wireless communications and produced various reports with recommendations, including the *Network Security/Vulnerability Assessments Task Force (NS/VATF) Report,* March 2002. In that report, the NS/VATF determined the need for policies that help ensure wireless networks and capabilities supporting NS/EP communications meet the highest level of security standards available. The task force also concluded that a better understanding of NS/EP communications functional requirements was needed to address the security of the interoperability between wireless and wireline networks.

During the NSTAC XXV Business Session, meeting participants addressed the topic of security vulnerabilities in wireless communications devices and networks. Because wireless technologies

are being used to transmit voice, data, and video in support of NS/EP operations, meeting participants agreed that the NS/EP community needed to identify its security requirements and understand potential wireless vulnerabilities. The NSTAC noted that wireless security challenges existed at many levels, including product design, wireless standards, wireless/Internet convergence, and implementation of existing security features.

Following the NSTAC XXV Meeting, the NSTAC's Industry Executive Subcommittee (IES) established the Wireless Security Scoping Group (WSSG) to consider how NSTAC should address the issue of wireless security. The WSSG recommended to the IES that the WTF be created to study wireless security as it pertained to NS/EP users.

1.2 Scope of Study

The WTF was directed to research wireless security issues for NS/EP users, to gain a better understanding of unique NS/EP security requirements, and to determine where wireless vulnerabilities exist (e.g., customer devices, network interfaces, and facilities). The WTF was tasked to provide policy recommendations on how to ensure standards bodies and individual companies consider NS/EP requirements when developing wireless connectivity solutions. The task force was also expected to provide policy recommendations to the President addressing how Government agencies should assess their vulnerabilities based on wireless technologies being deployed and specific agency requirements.

1.3 Approach

WTF members, subject matter experts from their respective companies and associations, and Government participants contributed to this effort. Appendix A provides a list of task force members, other participants, and briefers.

2.0 ISSUES RELATED TO WIRELESS SECURITY

The WTF considered a range of issues in its analysis of wireless security and how the NS/EP user operates in a wireless environment.

2.1 Definition of the Terms "Wireless" and "Wireless Security"

For the purposes of this report, the WTF agreed on the following definitions:

- *Wireless*: Descriptive of a network or terminal that uses electromagnetic waves (including radio frequency [RF], infrared, laser, visible light, and acoustic energy) rather than wire conductors for telecommunications.[1]
- *Wireless Security*: The protection afforded to a wireless network or terminal to attain the applicable objectives of preserving the integrity, availability, and confidentiality of wireless network resources (e.g., hardware, software, and firmware) and information contained within it.[2]

To address the issue of wireless security and develop focused conclusions and policy recommendations, the WTF used three classifications of various wireless network platforms—Public, Private, and Commercial—to reflect the user's accessibility to these networks (see Table 1). Through these three platform categories, the WTF considered any related risk and vulnerability issues that merited specific attention for NS/EP wireless users. This effort will be discussed in greater detail in Section 2.4.

Table 1. Wireless Network Platforms

Network	Types of Communications	Security Implications
Public	Unlicensed spectrum, such as 802.11 networks or 900 Megahertz (MHz) cordless telephones.	Platform is publicly accessible and security is generally nominal.
Private	Includes unlicensed 802.11 virtual private networks (VPN), spectrum licensed for use by commercial entities (i.e., delivery services, taxis, and trucking), microwave systems or licensed spectrum used by public safety missions (i.e., fire and police), or governmental agencies (i.e., Department of Defense [DoD] and Department of Energy).[3]	Platform is user class accessible and security is assigned by the network manager.
Commercial	Wireless common carrier networks, including cellular, Personal Communications System (PCS), paging, and satellite networks.	Network is discreetly available for subscribers; security is considered good.

[1] American National Standard for Telecommunications–Telecom Glossary 2000, Alliance for Telecommunications Industry Solutions.

[2] This definition is adapted from the National Institute of Standards and Technology (NIST) definition of the term "computer security," provided in Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook.*

[3] Public safety and/or Federal department and agency user requirements may be more stringent than other Private network users because of the critical nature of such communications.

2.2 NS/EP Users' Unique Requirements[4]

- *Service availability*: ability to obtain access to the service. For the NS/EP user, availability of communications is the primary concern.
- *Interoperability:* direct compatibility between user and service infrastructure, including the extension of features across the service provider and local network domains
- *Confidentiality*: protection of user data, signaling, identification, and location
- *Integrity*: protection from insertion, deletion, modification, or replay of data
- *Authentication*: assured identification of the user, terminal, and carrier
- *Accountability*: ability to verify transactions
- *Nonrepudiation*: ability to verify the origin of a specific message by a third party.

2.3 Wireless Advantages, Vulnerabilities, and Threats

There are distinct advantages to using wireless communication technologies, particularly in support of NS/EP missions. These advantages are as follows:

- *Portability*: NS/EP missions require availability of data for end-users often beyond the reach of wired connectivity (e.g., landlines, Ethernet) and via a number of end-user devices (e.g., portable computers, personal digital assistants [PDA], pagers, wireless telephones). Portability gives end-users the ability to send and receive critical data and connect with a Private local area network (LAN), the public switched network, or the Internet, at any given location.
- *Flexibility*: No fixed communications infrastructure is necessary to establish wireless communications capabilities. NS/EP wireless communications capabilities can be modified as required by specific missions, terrain, transmission conditions, or other factors.
- *Low installation costs*: Communications installation in difficult-to-wire and/or remote areas is made easier via wireless networking. Wireless technology enables reduced carrier costs and lower installation expenses than standard wireline infrastructures; recurring costs associated with wireline installation and network upgrades are dramatically reduced.
- *Short installation time*: Wireless communications offers an effective alternative in buildings or remote locales where installing a wired Ethernet or a copper telephone line is simply not feasible given the time constraints of NS/EP missions.

[4] Definitions drawn primarily from Federal Wireless Policy Committee, "Federal Functional Requirements for Commercial Wireless Services," May 21, 1999.

- *Location services*: Location services facilitated by wireless devices are enabling technologies offering NS/EP personnel valuable data, including navigation instructions, and tracking capabilities of people and NS/EP assets.
- *Diversity*: To ensure the continuity of NS/EP communications, diverse communications paths that do not rely on a single capability are necessary. Wireless communications offer the NS/EP user an additional layer of communications redundancy and in itself possesses an infrastructure with route diversity to avoid service disruptions and single points of failure.

The WTF determined that although there are many advantages to using wireless devices and services, there are corresponding vulnerabilities and threats that must be addressed before using wireless capabilities for mission-critical NS/EP communications. In studying this issue, the WTF concurred with other prevalent studies, which determined that any vulnerabilities that exist in conventional wired and computer communications and networks are applicable to wireless technologies. These vulnerabilities and related threats are as follows:

- *Inadequate or no encryption*: Wireless communications not employing strong encryption (i.e., Advanced Encryption Standard [AES] and triple-Data Encryption Standard [DES]) are vulnerable to compromised network resources, eavesdropping, foreign government espionage, and hijacked sessions.
- *Improperly configured devices*: Many organizations implement wireless technologies in a nonsecure manner, default security settings are not enabled, network resources are poorly managed, and/or the wireless signal is inadequately shaped via the layout of access points or antennae. Keeping the door open to the network not only exposes the devices attached to the wireless network and the wired network to malicious code (e.g., viruses and worms) but also threatens the confidentiality of information and integrity of the networks.
- *Inadequate physical security*: Physical security threats such as theft and hardware tampering can pose more substantial risks for wireless, mobile devices and extend to other portable devices, such as PDAs. Theft of wireless devices is an example of a threat faced by NS/EP users when using mobile devices outside a typical office environment. Proper physical security also includes mitigating possible risks to the network by disgruntled employees. Consequences include misuse, unauthorized access to the network, and loss of information stored on the device.
- *Known wireless protocol vulnerabilities*: Some wireless protocols (such as 802.11b) have well-publicized vulnerabilities, leaving some wireless communications vulnerable to eavesdropping, unauthorized access, password sniffing, masquerading, replay, message modification, and distributed denial of service (DDoS). These vulnerabilities potentially threaten system availability, confidentiality, and integrity of the network.
- *Inadequate management of passwords and keys*: Using shared keys that are often too short and not updated regularly can leave a wireless LAN (WLAN) vulnerable to attack. For example, when wired equivalent privacy (WEP) is enabled in a WLAN, all network

devices use the same key for data encryption and decryption. Other security flaws allow unauthorized persons to access user names and passwords.

- *Convergence of wireless and data communications*: As discussed in previous NSTAC reports,[5] the convergence of wireless data networks (e.g., WLANs) with the public switched telephone network (PSTN) and traditional wireless networks introduces new vulnerabilities. For example, end-to-end security for wireless networks and electronic transmissions involving wireless application protocol (WAP)-enabled applications lags behind the levels of security found in more robust Internet standards.

In the following section, the WTF addresses not only many of these vulnerabilities and threats in the context of Public, Private and Commercial platforms (as defined in Table 1), but also general wireless end-user and policy issues that are not specific to a single platform.

2.4 Wireless Security Issues and Conclusions

The range of wireless security varies from effective, practical security on the Commercial wireless networks, to significantly less security on the Public wireless networks. As such, an NS/EP agency must ensure that its NS/EP communications are secured appropriately for its mission. Again, the extent to which these vulnerabilities have been or can be addressed will be a function of the degree to which the network is managed by organizations with experience in security issues.

The specific issues associated with the three categories of wireless network platforms are discussed below.

2.4.1 Public Wireless Networks

- **Wireless security is improving, yet at a much slower pace than developments in wireless technology and deployments of WLAN capabilities. Many security problems associated with wireless devices are attributed to a lack of management control over incorporated assets by network/LAN administrators. The problem seems exacerbated within Government networks as a result of inadequate implementation of security doctrine.**

At a minimum, Government and NS/EP personnel must configure wireless access points to take advantage of the out-of-the-box security features. Even if WLANs are deployed with their built-in, basic security measures enabled, such as WEP and media access control (MAC) address lists, they are still vulnerable to attack. WEP encryption, for example, leaves WLANs open to passive hacking attacks that can allow a malicious party to uncover WLAN's encryption keys by sniffing a given amount of WEP-encrypted wireless traffic.

[5] See, for example, the NSTAC Network Security/Vulnerability Assessments Task Force Report, March 2002.

Additional security features can be added at the network and application layers and new Federal Communications Commission (FCC) requirements may also enhance WLAN security. In its proceedings to allocate additional spectrum for unlicensed applications (e.g., WLANs), the FCC may require equipment operating in that spectrum to implement a credible, secure transmission protocol. Wireless networks should provide protection to minimize the impacts of DDoS and eavesdropping.

- **WLANs were initially deployed with inadequate security to prevent fraud and abuse; however, security concerns are being addressed in standards bodies and new product releases. Government-specific wireless security needs have not been adequately identified or proffered to the standards bodies for review and incorporation into the process.**

The appropriate Federal departments and agencies must continue working with standards bodies and industry groups to ensure that NS/EP wireless security needs are addressed by standards bodies and incorporated in new products.

2.4.2 Private Wireless Networks

- **Although some measures of security are available in nondigital radio systems, digital networks enable a multitude of advanced security options. These security options are necessary for NS/EP communications, depending on the nature of the public safety service and the sensitivity of the transmitted information. Currently, fewer than 10 percent of public safety radio communications (e.g., police and fire) are on digital networks. Transitioning from analog to digital can facilitate widespread implementation of secure communications.**

Analog networks pose a significant security risk because of their vulnerability to interception. Voice calls on digital networks are less vulnerable because the digital interface is very complex and the required intercept equipment is very expensive and sophisticated. Ideally, wireless communications in support of NS/EP missions should be transmitted over digital networks.

- **Many Federal and State agencies are supporting systems capable of using high-level encryption (e.g., Project 25 and future Project MESA technology) to protect the confidentiality of sensitive but unclassified information involving Private radio systems. However, even where available, some NS/EP personnel often use no encryption because of complexity and interoperability concerns, and then communicate sensitive information in the clear during emergencies as a result of availability concerns.**

State and local public safety agencies often base communications decisions on cost and interoperability instead of security because of limited funds being provided for upgrading State and local public safety communications networks. As a result, State and local NS/EP personnel often have no alternative but to send transmissions in the clear. They may also carry several communications devices to increase their chances of communicating with other personnel in emergency situations. Ideally, public safety wireless communications should transpire via digital

networks, be compatible across NS/EP user sets and with Public networks, and provide better levels of security because the sensitive nature of NS/EP transmissions.

Educating users through existing partnerships with State and local public safety organizations (e.g., Association of Public-Safety Communications Officials) on the importance of security and establishing guidelines for transmitting sensitive information during emergencies may partially alleviate the problem of NS/EP communications transmissions in the clear. However, the larger issue is the need for funding to field widespread compatible and secure communications networks. Unfortunately, Federal monies to help States field interoperable, secure radio communications were not included in the homeland security legislation, and a systemic push to give cities, counties, and States a fundamental baseline for security is lacking. Ways to achieve that goal, in addition to reinstating funding through the Office/Department of Homeland Security, are via legislative endorsements or Federal guidance.

- **Unprotected microwave and other line-of-sight telecommunications links are vulnerable to undetected monitoring without physical break-in.**

Microwave telecommunications links have been operating for many years, and, unless encrypted, are vulnerable to monitoring. Microwave telecommunications links are unique because they may be monitored without detection and without physical break-in. Such monitoring can yield access to telecommunications management data, critical infrastructure network data, and targeted customer traffic. Today, the majority of telecommunications traffic is computer communications rather than voice traffic; successful surveillance can extract significant intelligence from wireless link data streams with low-cost, readily available equipment, such as standard laptop computers and commercially available radio equipment. These microwave links are particularly vulnerable to malicious attack, given their increase in "critical" data traffic and their publicly available geographic locations. Roughly 10,000 of these links are used in State and local government applications, along with approximately 10,000 used by "critical infrastructure" providers. In addition, about 10 percent of new microwave deployments are used in common carrier networks. Protection mechanisms—such as "link encryption" at the microwave layer or at a higher level, up to and including the message and control traffic layer, where microwave communication systems carry sensitive information—can mitigate this risk.

2.4.3 Commercial Wireless Networks

- **Additional encryption of voice transmissions over code division multiple access (CDMA) or time division multiple access (TDMA) networks is available; however, it is expensive and is provided only over-the-air interface. End-to-end protection requires not only compatible capabilities at both end devices but also suitable transmission media.**

Commercial digital networks provide effective, practical security on the air interface and physical transport layer through a combination of cryptographic authentication, air interface

complexity, encryption, and scrambling. Even so, some NS/EP missions may require a higher level of security. These NS/EP agencies should determine which missions require end-to-end security and should contract for that level of security with the commercial carrier, while recognizing limitations associated with employed end-to-end solutions, such as Secure Telephone Unit–Third Generation (STU-III) devices.

- **It is difficult to eliminate the threat of jamming in commercial mobile radio service (CMRS) networks in small, localized areas.**

Jamming of CMRS networks in small, localized areas remains a potential threat, but to jam transmissions in more than a very small geographic area would require a substantial and sophisticated attack. Unlike Government networks, information regarding commercial frequencies and cell sites is readily available on the Internet, making threat reduction difficult. Nonetheless, although the programming and configuration of site control channels is standards based (to ensure scalability and interoperable roaming), the high density of sites within any given area, and the diversity of carriers distributed over a range of bands from 800 Megahertz (MHz) to 1.9 Gigahertz (GHz), provides a highly diverse and robust wireless infrastructure that mitigates this threat. Methods of reducing the threat to NS/EP users include diversifying service providers and using providers that are spectrally distant when possible.

2.4.4 Wireless User Issues

- **For the NS/EP user, availability of communications is the first concern; security concerns do not figure as prominently.**

In an emergency situation, NS/EP personnel will use whatever wireless communications capabilities are at their disposal. Thus, availability significantly affects security during an emergency. It is crucial that entities with NS/EP missions formulate effective communications and contingency plans ensuring secure wireless communications are in place before an emergency.

- **Many users do not implement available security features on their wireless networks and most communications devices (e.g., devices have a default setting of security disabled or users do not change the default factory settings).**

The first steps for securing wireless devices are activating available device features and purchasing equipment with built-in encryption mechanisms; at a minimum, devices and other network components (e.g., access points) must be configured to use the out-of-the-box security features of wireless gear. However, wireless devices and networks remain vulnerable to attack with basic security features enabled.

- **There are unique considerations for the use of wireless computer devices in a secure manner.**

These unique considerations are as follows:

- Portable devices should be considered part of the networks to which they are connected.
- Strong authentication (e.g., smart card and biometrics) and personal identification should be employed.
- In regard to protected storage and use, encryption should use an approved algorithm (e.g., AES or triple-DES) and a key length sufficient to withstand an attack.
- Devices must be compliant with the appropriate certification and accreditation processes of Federal Information Processing Standards (FIPS) and National Information Assurance Partnership (NIAP).
- Wireless devices should not be used for storing, processing, or transmitting classified information unless used on an assured channel with National Security Agency (NSA) approved Type 1 encryption.
- Encryption of unclassified information for transmission to and from wireless devices is required. At a minimum, data encryption must be employed end-to-end using an approved algorithm (e.g., AES or triple-DES) and a key length sufficient to withstand an attack.

- **Security concerns are associated with the use of cryptographic keys, particularly issues related to effective key management.**

The immediate challenges for NS/EP entities implementing any wireless capabilities include choosing products that are standards-based, have robust key management functionality, and can grow to meet organizational requirements while maintaining a secure environment. Strong cryptography, robust key management, and proper authentication features are needed to alleviate some of the risks associated with wireless communications. Cryptographic keys are often too short, shared among the user set, and/or cannot be updated automatically and frequently. Effective wireless security demands more robust and reliable cryptographic keys that, if exposed, are dynamic and can be quickly replaced by new ones. Effective key management also entails a secure means of adding new users to the existing network without compromising security.

2.4.5 Other Policy Issues

- **Emergency 911 (E911) access does not extend to all wireless communications systems and devices.**

According to the FCC, more than 100,000 emergency calls are made each day from cell phones within the United States. As the volume and ubiquity of newer public wireless networks and their associated devices (e.g., PDAs, telematics, and wireless modems) increase, access to the

E911 networks must be anticipated and planned. In a recent report prepared for the FCC, a recommendation was made to create a "National 911 Program Office" within the newly established Department of Homeland Security.[6] It is likely that these newer evolutions could be addressed through the adoption of this recommendation.

- **The widespread availability of critical wireless network infrastructure information (e.g., cell towers, transmission sites) on the Internet and other public sources presents a threat to network security.**

For many years, databases detailing U.S. commercial transmission facilities have been widely disseminated (including availability on the Internet from sources such as the FCC), to support the technical coordination requirements between radio transmission facilities. These databases include highly detailed information on the location, ownership, and operating parameters of television broadcast facilities, satellite uplinks, and microwave point-to-point links, along with the locations of all antenna towers in the United States, including cellular towers. Many owners and users consist of Government agencies and critical infrastructure providers, including not only State and county governments, but also gas and electric companies.

Such widespread dissemination of information regarding critical infrastructure telecommunications facilities poses a physical and content security risk. This risk is further exacerbated by the increasing numbers of new requests for more extensive information from NS/EP and Federal, State, and local agencies, as they initiate their own planning activities. Further study on this issue is necessary to determine the extent to which Federal agencies can and should place controls over the availability of such information in order to strike an appropriate balance between security of the networks and the practical requirements for access to the data for legitimate commercial use or NS/EP planning.

3.0 RECOMMENDATIONS TO THE PRESIDENT

Based on its analysis of issues related to wireless security, and the conclusions outlined above, the National Security Telecommunications Advisory Committee (NSTAC) offers the following recommendations.

The NSTAC recommends that the President—

- Direct Federal departments and agencies to construct mitigation and alleviation policies regarding wireless vulnerabilities and further consider the applicability of the recent National Institute of Standards and Technology and Department of Defense's wireless security policies to all Federal agencies and departments.[7]

---

[6] "A Report on Technical and Operational Issues Impacting The Provision of Wireless Enhanced 911 Services" Prepared for the Federal Communications Commission by Dale N. Hatfield, filed on October 15, 2002.

[7] Recent wireless security policies include: NIST Special Publication (SP) 800-46, "Security for Telecommuting and Broadband Communications," September 2002; NIST SP 800-48, "Wireless Network Security: 802.11, Bluetooth and Handheld Devices,"

- Direct Government chief information officers to immediately emphasize enterprise management controls, with respect to wireless devices, to ensure that appropriate security controls are implemented, given that the banning of wireless devices is counterproductive and ignores the efficiency that such devices bring to users.
- Direct Federal departments and agencies to work in concert with industry to develop security principles and to resolve security-related deficiencies in wireless devices when employed by NS/EP users.
- Direct Federal departments and agencies using wireless communications to address wireless security threats and vulnerabilities. In addition, consider the end-to-end security of their respective communications and information system capabilities.
- Direct Federal departments and agencies using wireless communications to purchase and implement fully tested and compliant secure wireless products and services.
- Direct appropriate staff to advocate funding initiatives for replacing nonsecure analog with secure digital national security and emergency preparedness (NS/EP) equipment and systems.
- Direct Federal departments and agencies using microwave communications facilities to address unprotected link security vulnerabilities. In addition, advise State and local governments and other critical infrastructure providers of the vulnerability of unprotected microwave communications as part of the Homeland Security initiative.
- Establish policies regarding the public availability and dissemination of critical infrastructure information (such as the policies on Internet availability of Federal Communications Commission and Federal Aviation Administration databases of tower locations).

(November 2002); and Draft Department of Defense (DoD) Directive 8100.bb, "Use of Commercial Devices, Services, and Technologies in the DoD Global Information Grid (GIG),"
July 15, 2002.

APPENDIX A

TASK FORCE MEMBERS AND OTHER PARTICIPANTS

TASK FORCE MEMBERS

Verizon Communications, Inc.	Mr. James Bean, Chair
Motorola, Inc.	Mr. Ben LaPointe, Co-Vice Chair
SBC Communications Inc.	Ms. Rosemary Leffler, Co-Vice Chair
Bank of America Corporation	Mr. Jenkins Ravenel
BellSouth Corporation	Mr. Shawn Cochran
The Boeing Company	Mr. Robert Steele
Computer Sciences Corporation	Mr. Guy Copeland
Electronic Data Systems	Mr. Dale Fincke
Lockheed Martin Corporation	Ms. Jennifer Warren
Lucent Technologies	Ms. Anne Frantzen
Nortel Networks	Dr. Jack Edwards
Northrop Grumman Corporation	Mr. Scott Freber
Qwest Communications	Mr. Jon Lofstedt
Raytheon Company	Mr. Tim Bashara
Science Applications International Corporation	Mr. Hank Kluepfel
Sprint Corporation	Mr. Jim Norris
TRW Inc.	Mr. Joe Yates
WorldCom, Inc.	Mr. Thomas Gann

OTHER PARTICIPANTS

Bank of America Corporation	Mr. Sam Phillips
Cingular Wireless	Mr. Jim Bugel
Cellular Telecommunications & Internet Association	Ms. Kathryn Condello
Cellular Telecommunications & Internet Association	Mr. Rick Kemper
The George Washington University	Dr. Jack Oslund
Lockheed Martin Corporation	Mr. John Bryfogle
Lucent Technologies	Mr. Stanley Jones
Motorola, Inc.	Mr. Bob Fairbairn
Nortel Networks	Mr. Roy McClellan
Sprint Corporation	Ms. Carol Ross
Telecommunications Industry Association	Mr. Dan Bart

BRIEFERS

BellSouth Corporation	Mr. Neale Hightower, Sr.
Booz Allen Hamilton Inc.	Mr. Les Owens
Federal Law Enforcement Wireless User Group	Mr. James Downes
Harris Corporation	Mr. Steven Warwick
Inmarsat Ltd.	Mr. Ruy Pinto
Kasten Chase	Mr. Bill Colvin
Kasten Chase	Mr. Paul Hyde
Lucent Technologies	Mr. Simon Mizikovsky
SBC Technology Resources, Inc.	Mr. David Wolter
Telcordia Technologies, Inc.	Dr. Joe Wilkes
Verizon Wireless Inc.	Mr. Chris Carroll

APPENDIX B

BRIEFER QUESTIONNAIRE ON WIRELESS SECURITY

BRIEFER QUESTIONNAIRE ON WIRELESS SECURITY

The following is a list of questions prepared by the task force to assist briefers in their preparation. In the final report, the task force did not fully address every question.

NS/EP Agencies and Users

- What wireless devices do you use now or plan to use in the future (e.g., cell phones, pagers, personal digital assistants, laptops, and wireless imagery devices)?
- What is your biggest security concern when using wireless devices?
- What security requirements do you believe are necessary for national security and emergency preparedness (NS/EP) users?
- What vulnerabilities do you see with wireless devices?
- What steps do you take to secure the provision and deployment of wireless devices (e.g., locks, passwords, transport encryption, media encryption, alarms, biometrics, and smart cards)?
- What security products are you aware of that are in use now that can secure your wireless devices?
- What are the obstacles to implementing security?
- How do you address security issues during the provisioning process?
- How do you envision end-to-end security in the wireless environment?
- What audit or testing procedures are in place to maintain security in your organization after implementing security products?
- How do you oversee personnel issues (e.g., operational and administrative procedures) regarding the use of wireless communications?
- What information-sharing procedures are in place in your organization to disseminate information on known security vulnerabilities?
- Does the new Department of Defense wireless policy affect your mission?
  - If so, what additional security features will you need to implement in order to satisfy this policy?
- How do you meet the requirements of your wireless NS/EP users abroad?
  - What additional audit and security issues surface from international usage?

Carriers

- Can you identify your NS/EP wireless customers?
  - If so, what security requirements have they placed on you during the provisioning process, if any?
  - Can you give them special treatment for additional security features?

- Do you support wireless devices in your operations, administration, maintenance, and provisioning (OAM&P) systems?
  - What security steps have you taken in this area?
  - How are you protecting your OAM&P systems?

- What is on the horizon for wireless devices and security?

- What support exists for legacy systems (e.g., time division multiple access [TDMA])?
  - If none, what are the security impacts?

- How does your company address the international aspects of security standards with regard to NS/EP users?