THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

WIRELESS TASK FORCE
Findings

Security of Internet-Enabled Wireless Devices

January 2003

NSTAC's Wireless Task Force (WTF) Findings on The Security of Internet–Enabled Wireless Communications Devices

The security of Internet-enabled wireless communications devices (e.g., third generation [3G] wireless devices) is an issue of obvious importance to the wireless industry, the private sector, and the Government. Recent exploitations of particular vulnerabilities in Internet-enabled wireless communications devices have resulted in increased public awareness of this problem. One publicized exploitation involved the launching of a denial of service attack on the Japanese equivalent of the U.S. emergency 911 system. In this instance, NTT DoCoMo users unknowingly dialed the emergency system when an appellate was executed on their wireless devices. These types of attacks could pose a serious threat to the availability and security of national security and emergency preparedness (NS/EP) communications networks.

At a December 2, 2002, Industry Executive Subcommittee (IES) task force briefing, Mr. Richard Clarke, Chair, the President's Critical Infrastructure Protection (CIP) Board, requested that the President's National Security Telecommunications Advisory Committee's (NSTAC) Wireless Task Force (WTF) consider examining the security of Internet-enabled wireless communications devices and the efficacy of installing anti-virus software for wireless telephones, since such devices are becoming increasingly more integrated with computing functions. In response to the Administration's request, the Task Force scoped the issue, receiving briefings regarding industry solutions for addressing this issue from Bank of America, and the Cellular Telecommunications & Internet Association.

In scoping the issue, the WTF made the following observations:

- **The security of Internet-enabled wireless communications devices is a serious issue, yet the problem is not limited exclusively to "wireless" or "3G" wireless devices; any device connected to the Internet can be attacked.** Any device connected to a distributed network is vulnerable to malicious code (e.g., Trojan horses, viruses, etc.). For example, there have been reported attacks on the emergency 911 system through WebTV devices that are connected to the Internet, but are not wireless.

- **The security of Internet-enabled communications devices is not a new issue.** While recent attacks have targeted advanced wireless devices, similar attacks have been executed on other user devices and network applications in the past. The Government and industry have been aware of network vulnerabilities related to the convergence of telecommunications networks and the Internet for years, and have worked together to develop solutions.

- **The problem currently affects the application layer, not the network layer; network safeguards are in place and attacks have been focused on weaknesses in the specific platforms being used (e.g., short messaging systems, I-mode, etc.).** The safeguards found in the network layer provide adequate security for the switching and routing of data being transmitted via a certain protocol (e.g, Internet Protocol, etc.). Vulnerabilities at the application layer, where an application file or particular program connect to a communications protocol, have been exploited in Internet-enabled wireless devices.

- **Solutions and responses to this problem have been reactionary; security is not sufficiently built-in for Internet-enabled devices.** Industry has not had a coordinated response to this problem to date, but has added on security solutions as problems have arisen. However, the commercial wireless sector is in the early stages of coordinating efforts to develop platform standards that address these issues.

- **This issue could affect the security and availability of the NS/EP communications infrastructure.** As was seen in the attacks against the emergency 911 system and the potential for other types of attacks through wireless devices, there exists a substantial risk to the security and availability of the NS/EP communications infrastructure.

- **Industry has been working this issue from a market-driven standpoint; application deployment is being deferred by carriers until they can ensure adequate security is in place.** As security of wireless networks has become a larger and more visible issue, the U.S. wireless industry has become more cautious and delayed the release of some 2.5G and 3G wireless products/applications until adequate security can be assured.

- **The problem is international in scope and needs to be addressed in cooperation with international groups.** The security of Internet-enabled wireless communications devices and convergence issues have impacts outside of the United States. Any efforts to develop mitigation strategies, standards or best practices must include regional standards organizations (e.g., The European Telecommunications Standards Institute) and international organizations (e.g., The International Telecommunication Union), as well as application developers and network operators.

- **The Government can take an increased role in helping focus solutions.** The Task Force advises Federal agencies and departments to become more involved in the standards development process and help focus solutions to ensure NS/EP requirements are considered.

- **The NSTAC may play a role to focus the issue; while that role is not currently clear, the IES should revisit this issue in the future.** After scoping the issue, the WTF has not identified any new issues warranting study from a wireless perspective.

The WTF reached the following conclusion:

- **Although the initial tasking references wireless specifically, the NSTAC has worked on this larger issue as it relates to the convergence of telecommunications networks and the Internet.** The NSTAC investigated and presented recommendations regarding the convergence of telecommunications networks and the Internet during past cycles. In 2001, for example, the NSTAC's Convergence Task Force examined the ability of the converged network to securely and reliably support NS/EP communications requirements. At the January 23, 2003, IES Meeting, members agreed to keep abreast of new developments on this issue, but to defer conducting any further study at this time.