# Wireless Security

## Issue Background

Wireless technologies are increasingly relied upon to transmit voice, data, and video in support of national security and emergency preparedness (NS/EP) operations.  It is therefore imperative for the Government to understand the vulnerabilities and risks associated with using wireless technology as an NS/EP communications tool.  Known vulnerabilities and related threats include:  inadequate encryption, improperly configured devices, inadequate physical security, protocol vulnerabilities, inadequate management of passwords and keys, and convergence of wireless and data communications.

## History of NSTAC Actions

The President's National Security Telecommunications Advisory Committee (NSTAC) first began studying network security issues in 1990.  In 2002, the NSTAC Network Security/Vulnerability Assessments Task Force (NS/VATF) concluded its assessment of policy and technical issues related to the evolving public network by highlighting wireless network vulnerabilities.  For the wireless section of its study, the NS/VATF limited its scope to the security of wireless application protocol, wireless local area networks, and personal area networks.  In its 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.

## Recent NSTAC Activities

The NSTAC recently performed a broad study of wireless security to understand NS/EP users' security requirements and identify potential wireless vulnerabilities.  To adequately discuss these subjects and formulate actionable recommendations designed to help offset wireless threats and vulnerabilities, the NSTAC Wireless Task Force (WTF) identified NS/EP wireless users' unique requirements, compiled a list of wireless vulnerabilities and threats, and, where known, identified mitigation approaches to address wireless vulnerabilities and threats.

In January 2003, the WTF concluded that challenges exist at many levels, including product design, wireless standards, and wireless/Internet convergence.  It recommended to the President that Federal departments and agencies address threats and vulnerabilities by:  constructing mitigation and alleviation policies, emphasizing enterprise management controls, considering end-to-end security capabilities, replacing non-secure analog equipment with secure digital NS/EP equipment, and addressing unprotected link security vulnerabilities of microwave communications facilities.  The WTF also evaluated the security of Internet-enabled wireless devices, concluding that threats to these devices are related to the convergence of telecommunications networks and the Internet and are not entirely unique to wireless.

In addition to staying apprised to developments in wireless security, the NSTAC will focus over the next year on issues related to commercial satellite security, including the Government's reliance on satellites for NS/EP missions and potential vulnerabilities to a range of intentional or unintentional threats.