



# INDUSTRY EXECUTIVES ADVISING THE PRESIDENT

Revised 12/1/06

## MEETING THE CHALLENGES OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS COMMUNICATIONS

*The President's National Security Telecommunications  
Advisory Committee*

### NSTAC MEMBERSHIP

#### NSTAC CHAIR

Mr. Gary D. Forsee  
Sprint Nextel

#### NSTAC VICE CHAIR

Mr. Randall Stephenson  
AT&T

Mr. F. Duane Ackerman  
BellSouth

Mr. James F. Albaugh  
Boeing

Mr. Lawrence T. Babbio, Jr.  
Verizon

Mr. Gregory Q. Brown  
Motorola

Mr. Daniel J. Carroll, Jr.  
Telcordia Technologies

Mr. Kenneth Dahlberg  
Science Applications International Corporation  
(SAIC)

Mr. Van B. Honeycutt  
Computer Sciences Corporation (CSC)

Mr. Arthur Johnson  
Lockheed Martin

Mr. Clayton M. Jones  
Rockwell Collins

Mr. Scott G. Kriens  
Juniper Networks

Mr. Howard L. Lance  
Harris Corporation

Mr. Craig O. McCaw  
Teledesic

Mr. Walter B. McCormick, Jr.  
United States Telecom Association (USTelecom)

Mr. Craig J. Mundie  
Microsoft

Mr. Richard C. Notebaert  
Qwest

Mr. Donald J. Obert  
Bank of America

Mr. Stratton Sclavos  
VeriSign

Mr. Stanley Sigman  
CTIA (Cingular Wireless)

Mr. William H. Swanson  
Raytheon Company

Mr. Lawrence Weinbach  
Unisys

Mr. Joseph R. Wright, Jr.  
Senior Executive Consultant for Satellites

### WHAT IS THE NSTAC?

The President created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982. Since then, the NSTAC has served four presidents. Composed of no more than 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues related to national security and emergency preparedness (NS/EP) communications policy. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.<sup>1</sup>

NS/EP communications enable the Government to make an immediate and coordinated response to all emergencies, whether caused by a natural or man-made disaster, an act of domestic terrorism, or a cyber attack. NS/EP communications also allow the President and other senior Administration officials to be continually accessible, even under stressed conditions such as the September 11, 2001, terrorist attacks.

The NSTAC collaborates on NS/EP issues with the Government and the Department of Homeland Security (DHS) through the National Communications System (NCS), a partnership with two unique features—direct industry involvement with both the defense and civil agencies comprising the NCS; and regular, sustained interaction between industry and NCS member departments and agencies through the Network Security Information Exchange (NSIE) process and the National Coordinating Center for Telecommunications Information Sharing and Analysis Center (NCC Telecom ISAC).

The NCS was integrated into DHS with the signing of the Homeland Security Act of 2002. The Manager, NCS, is the Designated Federal Official of the NSTAC.

### EVOLUTION OF THE NSTAC

New technologies in an increasingly competitive marketplace bring both new opportunities and new vulnerabilities to the information infrastructure. The NSTAC is strongly positioned to advise the President on how to: (1) leverage this dynamic environment to enrich NS/EP communications capabilities and ensure that new architectures fulfill NS/EP requirements; and (2) address vulnerabilities in the information infrastructure that could adversely affect NS/EP communications services.

At the NSTAC's genesis, NS/EP communications services were provided by an infrastructure based on a discrete, monolithic, domestic, terrestrial, circuit-switched voice network, supported primarily by mechanical controls. Today's communications infrastructure is composed of interdependent, diverse, circuit and packet switched networks using terrestrial, satellite, and wireless transmissions systems for voice, data, image, and video communications, supported primarily by software-based controls. Meanwhile, communications networks and information systems have converged into interdependent parts of a single information infrastructure, profoundly changing how

<sup>1</sup> More detailed information on the NSTAC is available on the NSTAC home page  
(<http://www.ncs.gov/nstac/nstac.html>).

both the public and private sectors conduct business and increasing their dependence on the technologies comprising the information infrastructure. As domestic companies enter partnerships or merge with foreign service providers, globalization introduces another element of complexity.

For two decades, industry chief executives from communications and information technology companies have offered their expertise to provide the NSTAC's independent, private sector, nonpartisan, provider-based perspective to the President. The NSTAC's viewpoint and its experiences with a broad range of Federal departments and agencies make it a key strategic resource for the President and his national security team in their efforts to protect our Nation's critical infrastructures. The NSTAC's current work plan includes initiatives that intersect with several programs set forth in DHS' National Response Plan, the National Infrastructure Protection Plan, and the National Strategy to Secure Cyberspace.

As the political and technological environments have changed, the NSTAC's work has kept pace and evolved from an initial emphasis on NS/EP communications policy to a broader scope that encompasses the entire information infrastructure. Today, the NSTAC offers advice to the President on a wide range of policy issues affecting the Government's ability to protect the information infrastructure from threats and vulnerabilities that might ultimately jeopardize the country's national and economic security, playing a critical role in the homeland security arena.

### **THE NSTAC: AN ESSENTIAL PUBLIC-PRIVATE PARTNERSHIP**

Although it is absolutely necessary for the operation of the Government in both day-to-day and emergency situations, the information infrastructure is owned and operated by the private sector. Consequently, Government is unable to fully address NS/EP communications issues associated with the information infrastructure without an industry/Government partnership such as that offered by the NSTAC. Two of the NSTAC's most important accomplishments are the industry/Government partnerships of the NCC Telecom ISAC and the NSIE. Both groups leverage the real-world experiences of telecommunications industry executives to improve the security and reliability of the nation's telecommunications infrastructure. These groups, as well as major issues recently addressed by the NSTAC, are described below.

**NCC Telecom ISAC:** The NCC was established in 1984 as a result of an NSTAC recommendation to develop a joint industry/Government national coordinating mechanism to respond to the Federal Government's NS/EP communications service requirements. Currently, nearly 75% of NSTAC member companies are represented in the NCC. The NSTAC was instrumental in expanding the NCC's responsibilities to include functioning as an ISAC for the telecommunications infrastructure. Established in January 2000, the Telecom ISAC was the second ISAC to be formed following the promulgation of Presidential Decision Directive 63 (PDD-63), and it was the first ISAC with both industry and Government membership. The NCC Telecom ISAC gathers information about vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, Government, and other sources, and then analyzes the data with the goal of averting or mitigating effects on the communications infrastructure. Results are sanitized and disseminated in accordance with sharing agreements established by the NCC Telecom ISAC participants.

**NSIE:** In 1991, the NSTAC, working with the NCS, recommended establishing an industry/Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. The NSIE process was established as a forum in which industry and Government could share information in a trusted and confidential environment. The NSIE continues to function well today, demonstrating that industry and Government will share sensitive security information if they find value in doing so. In 1998, PDD-63 called for the establishment of similar information exchange forums to reduce vulnerabilities in all critical infrastructures.

**Convergence:** The NSTAC has addressed numerous issues throughout its history, with recent initiatives involving the security of commercial satellite systems, cybercrime, Wireless Priority Service, and the resilience and reliability of the financial services industry's communications infrastructure. The NSTAC continues to look ahead in this era of convergence; as much of the telecommunications network moves to a packet-switched system from legacy circuit-switched networks, NS/EP mechanisms currently in place will need to be updated. In 2001, the NSTAC Convergence Task Force noted many vulnerability issues related to convergence and the Next Generation Networks (NGN) that could impact NS/EP communications, and the task force recommended further study. NSTAC's NGN Task Force is now working to provide a high-level description of the network itself and of the expected user environment, to identify which NS/EP user requirements will apply, including how they differ from traditional communications networks, and to explain what this means for network users.

**Other Current Issues:** Other NSTAC task forces and scoping groups are currently examining the interdependency between telecommunications and electric power, determining the long-term direction of the NCC, promoting research and development in associated NS/EP areas, and examining issues associated with open source infrastructure information published on the Internet. Recent accomplishments include addressing concerns related to industry and Government background checks.

The NSTAC's past accomplishments demonstrate the value it provides, advising the President on the protection and enhancement of the Nation's NS/EP communications infrastructure. The organization provides member companies with a robust opportunity to serve the Nation while providing leadership on Government actions that directly affect the telecommunications industry.