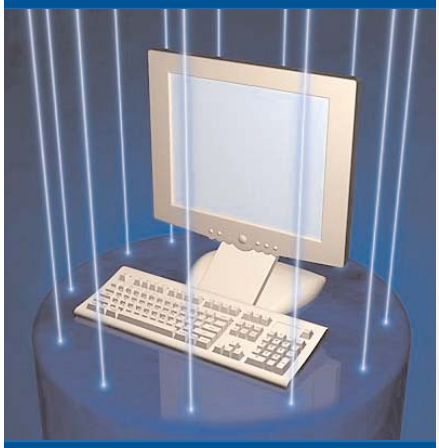
The President's National Security Telecommunications Advisory Committee



20 Years of Serving the President

THE WHITE HOUSE

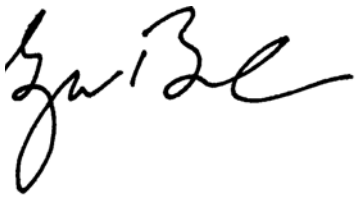
WASHINGTON

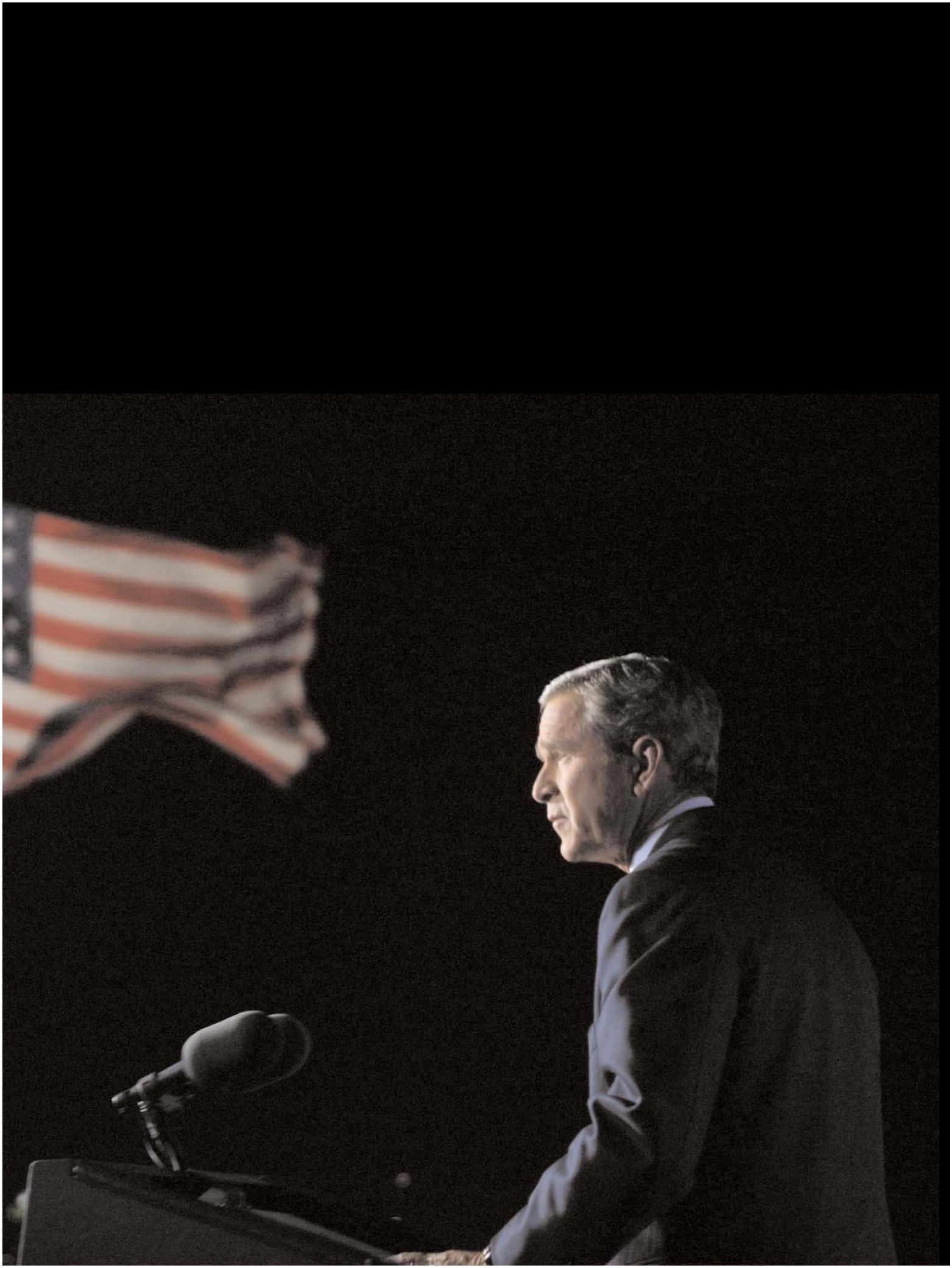
March 12, 2002

Congratulations to the members of the National Security Telecommunications Advisory Committee (NSTAC) as you celebrate 20 years of service to our country.

From finance networks to transportation systems and electronic commerce to utility operations, our society depends on complex interconnected technologies. By working to protect these systems, NSTAC plays an important role in the security of the American people.

I appreciate NSTAC's timely advice on communications issues, and I commend your members for your efforts to develop reliable, secure, and adaptable communications systems for our rapidly changing global environment. Best wishes for a memorable anniversary celebration.





Twenty Years of Partnership

For twenty years (1982-2002), the President's National Security Telecommunications Advisory Committee (NSTAC) has provided industry-based advice and expertise to the President of the United States on issues pertaining to the reliability and security of the communications and information infrastructure-issues that are critical to America's national security and commercial interests. The close partnership that has ensued between the 30 chief executives who compose the advisory committee —and Government officials— continually evolves to meet the new challenges related to changes in technology and national priorities. The NSTAC's partnership with Government is facilitated through the National Communications System (NCS), an interagency consortium of 23 Federal departments and agencies that serves as the focal point for industry/Government national security and emergency preparedness (NS/EP) communications planning and response.

Since its inception, the NSTAC has advised four Presidents and six Administrations and has proven itself adept at responding to challenges affecting our Nation. The NSTAC's unique public-private partnership has proven itself over the course of the past 20 years as a model for fostering cooperation and trust among the industry participants, and between industry and the Government. Its record of accomplishments includes substantive recommendations to the President, leading to enhancements of the Nation's NS/EP communications, critical infrastructure policies, and related information systems security posture. Enhancements in the form of operational programs and policy solutions benefit both industry and Government as the security requirements for the communications infrastructure evolve.

In this time of increased awareness of the criticality of and nexus between communications, technology, and national security, the NSTAC's work during the past 20 years highlights the importance of the NSTAC's advice to the Administration and response to incidents affecting national security. As the NCS transfers into the Department of Homeland Security (DHS), the NSTAC is well positioned to continue to serve the Nation's interests. The NSTAC, in keeping with its long, supportive history, will be a fundamental building block for public-private sector collaboration and will continue to provide essential guidance for the Government in the new national security environment.

Advising the President During a Time of Change

In 1982, when President Ronald Reagan established the NSTAC via Executive Order 12382—"President's National Security Telecommunications Advisory Committee," he sought advice on the implementation of the country's national security policy from the perspective of the telecommunications industry. This support included conducting feasibility studies on specific measures intended to improve the communications aspects of the country's national security posture and providing technical advice to identify and resolve issues that the NSTAC considered would negatively affect the Nation's secure communications capability. Twenty years later, the NSTAC continues to provide valuable advice to the President in the following five critical mission areas:

Infrastructure Protection

The well being of our Nation and its ability to sustain national security missions depends on secure and reliable infrastructures. The interruptions or manipulations of vital services, such as telecommunications, energy, transportation, and banking and finance, would be detrimental to the welfare of the United States. During the mid 1990s, the President acknowledged these interdependencies and encouraged the private sector to actively participate in the protection of critical infrastructures from both physical and cyber attacks. Since the September 11, 2001, terrorist attacks, the NSTAC, as advisor to the President on NS/EP communications, has played a leading role in helping the Government understand potential vulnerabilities and developing policy recommendations to mitigate associated risks. Building on previous infrastructure specific assessments, the NSTAC analyzed physical security threats and possible remedies to critical telecommunications infrastructure sites, focusing, in particular, on trusted access issues, the concentration of critical telecommunications assets in telecom hotels, and the resiliency of Internet peering points. The NSTAC is also fostering cooperation and information sharing initiatives across all critical infrastructures, including the electrical power, transportation, and financial services industries. The NSTAC recognizes that uninterrupted or minimally disrupted telecommunications services are indispensable to sustain other infrastructures' operational capabilities and is committed to continue supporting public-private partnerships, as well as information sharing efforts, with other sectors.

Information Assurance

The information revolution has transformed our Nation into a society that deeply relies on the information and communications infrastructure to function successfully. It is, therefore, imperative for both industry and Government to secure networks and information systems by ensuring information availability, integrity, authentication, confidentiality, and verifiability. The NSTAC is actively involved in efforts to address cyber-related vulnerabilities, network security issues, and wireless technologies vulnerabilities. The launch of several distributed denial of service attacks and the propagation of malicious worms in the last few years have demonstrated how easy it is to exploit cyber vulnerabilities. In addition, the growing reliance on mobile e-services and applications has rendered security of wireless protocols and systems an issue of concern, especially when related to NS/EP communications transiting over wireless networks and technologies.

Network Convergence

The late 1990s saw a fundamental shift in the overall architecture of the telecommunications network. To remain cost competitive and to enable the widespread delivery of advanced broadband services, telecommunications carriers increasingly began to implement packet-based networks. However, due to heavy investment in the public switched telephone network, many carriers chose to leverage components of both infrastructures resulting in a period of network convergence before the full transition to the security of the next generation network (NGN) is complete. Over the past several years, the NSTAC has focused much attention on the NS/EP consequences of the converged environment, especially as it relates to NS/EP communications programs, such as the Government Emergency Telecommunications Service (GETS) and Telecommunications Service Priority (TSP). The NSTAC recommended that Government promptly determine the precise functional NS/EP requirements for both the converged network and the NGN and ensure that those requirements are conveyed to standards bodies and service providers. Acting on the advice of the NSTAC, the NCS increased its participation in standards bodies and the Executive Office of the President formed an interagency Convergence Working Group to address issues associated with network convergence.

The NSTAC is actively involved in efforts to address cyber-related vulnerabilities, network security issues, and wireless technologies vulnerabilities.

The NSTAC provided technical analyses and developed risk assessments with other commercial industries to heighten the awareness of cross sector information assurance and infrastructure protection issues.

Information Sharing

One of the flagship missions of the NSTAC since its founding is the enhancement of communications and coordination between the private sector and Government. While the NSTAC has long recognized the value of information sharing—since it recommended the establishment of the National Coordinating Center for Telecommunications (NCC) in 1983—other public and private sectors only more recently recognized its true value. In the late 1990s, the NSTAC set out to better understand existing and proposed channels with which the telecommunications industry shares information. The NSTAC observed that information sharing is dependent on receiving a benefit when voluntarily shared, is based on trusted relationships, and may be affected by legal barriers. One of the NSTAC's lessons learned from industry's response to the September 11 terrorist attacks is the importance of sharing information with law enforcement and other Government agencies to protect the Nation's infrastructure and the need to remove barriers to information sharing to respond to attacks in a timely matter.

Outreach

Through outreach efforts such as symposia, published reports, and interaction with public and private sector leaders, the NSTAC fosters the exchange of information among NS/EP stakeholders. Following the terrorist attacks in 2001 and at the request of the White House, the NSTAC established an ad hoc group, in coordination with the Federal Government, to address lessons learned, share its views on the processes and procedures that worked well, and discuss how to further enhance communications processes. In addition, the NSTAC provided technical analyses and developed risk assessments with other commercial industries to heighten the awareness of cross sector information assurance and infrastructure protection issues. The NSTAC also actively encourages the exchange of ideas among representatives from industry, Government, and academia through research and development (R&D) exchanges. Over the past five years, the NSTAC has sponsored two R&D Exchanges. The first exchange, held in October 1998 at Purdue University in conjunction with the Office of Science and Technology Policy (OSTP), encouraged participants to discuss collaborative approaches to security technology R&D. The second exchange, held at the University of Tulsa in September 2000 in conjunction with OSTP and the National Institute of Standards and Technology, focused on the need to develop best practices, standards, and protection profiles to enhance the security of the NGN. These sessions are invaluable for the exchange of information between industry, Government, and academia alike, and recommendations raised during these exchanges help shape the NS/EP agenda.

Over the past twenty years, there were major advancements in information and communications technologies and changes in the geopolitical landscape. Throughout, the President's NSTAC has proactively advised the President on how to adapt national policies to these technological changes and new threats.

KEY

- NSTAC KEY EVENT
- THREAT
- TECHNOLOGY
- POLICY

"…We look around the world and see rampant conflict and aggression. There are many sources of this conflict -- expansionist ambitions, local rivalries, the striving to obtain justice and security. We must all work to resolve such discords by peaceful means and to prevent them from escalation..."

Reagan's Remarks to United Nations on Disarmament, June 17, 1982

AT&T and Justice Department sign consent decree signaling the intent to divest AT&T - 1982

1982

1981-1989

Industry and Government prepare for Y2K disruptions - 1999

Telecommunications industry mergers widespread - 1999 - 2000

Presidential Decision Directive 63 on critical infrastructure protection issued by President Clinton – 1998

NCC designated as Telecommunications Information Sharing and Analysis Center (per NSTAC recommendation) - 2000

Massive denial of service attacks launched against major commercial web sites - 2000

Companies worldwide pay billions in third generation (3G) wireless spectrum auctions - 2000

President Reagan signs Executive Order 12382 establishing NSTAC - September 1982

National Coordinating Center for Telecommunications (NCC) established following NSTAC's 1983 recommendation - 1984

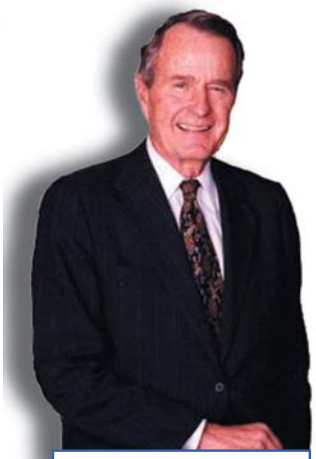
U.S. reaches 1 million cellular subscribers - 1987

"Internet worm" shuts down Internet for days - 1988

Computer Emergency Response Team (CERT) formed by DARPA - 1988

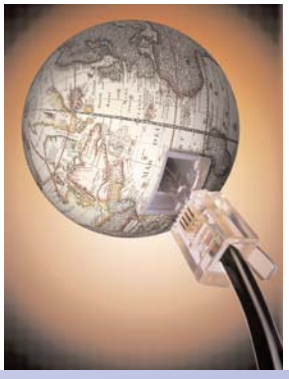
"…At this critical moment in history, at a time the cold war is fading into the past, we cannot fail. At stake is not simply some distant country called Kuwait. At stake is the kind of world we will inhabit…"

Bush's Radio Address to Nation on the Persian Gulf Crisis, January 5, 1991



1989 - 1993

Cable modem introduced in U.S. - 1996



Telecommunications Act of 1996

NSTAC recommends establishment of a cellular priority access service - 1995

30 million users on Internet worldwide - 1995

Terrorist attacks (e.g., World Trade Center and Oklahoma City bombings) - 1993 - 1995

"…Great harm has been done to us. We have suffered great loss. And in our grief and anger we have found our mission and our moment. Freedom and fear are at war. The advance of human freedom—the great achievement of our time, and the great hope of every time—now depends on us. Our nation—this generation—will lift a dark threat of violence from our people and our future."

Bush's Address to Joint Session of Congress and American People, September 20, 2001

White House Office of Cybersecurity established and the Administration develops National Plan for Information Systems Protection - 2001

2001 - Present

Cold War ends - 1989

Telecommunications Service Priority program begins operation (recommended by NSTAC in 1984) - 1990

NSTAC begins a continuing study of network security issues - 1990

NSTAC National Security and Information Exchange (NSIE) established - 1991

Internet hosts worldwide breaks one million - 1992

First digital cellular network - 1993

"…Information technology has helped to create the unprecedented prosperity we enjoy at the end of the 20th century…. It is important to recognize the role technology has played in this remarkable economic prosperity. But it is also important to recognize the challenges that we face out there in the security area."
Clinton's Remarks on National Plan for Information Systems Protection, January 7, 2000

1993 - 2001

September 11, 2001: Terrorist attacks interrupt and congest telecommunications networks around the affected areas

Wireless Priority Service with initial operating capability launched in select cities - 2002

President Bush signs bill creating The Department of Homeland Security - 2002

SEVERE
Severe risk of Terrorist Attack
HIGH
High Risk of Terrorist Attack
ELEVATED
Significant risk of Terrorist Attack
GUARDED
General risk of Terrorist Attack
LOW
Low risk of Terrorist Attack

2002

The NSTAC provides industry-based analyses and recommendations to the President and the executive branch regarding policy and enhancements to national security and emergency preparedness telecommunications.

NSTAC Chairs

Mr. Rand V. Araskog — Dec. 1982 - Apr. 1984
Chairman, President & CEO
International Telephone and Telegraph Corporation

Dr. Joseph V. Charyk — Apr. 1984 - Oct. 1985
Chairman & CEO
Communications Satellite Corporation

Mr. Theodore F. Brophy — Oct. 1985 - Feb. 1987
Chairman of the Board & CEO
GTE Corporation

Mr. Rocco J. Marano — Feb. 1987 - Sep. 1988
President & CEO
Bell Communications Research, Inc.

Mr. Paul H. Henson — Sep. 1988 - Mar. 1990
Chairman
United Telecommunications, Inc.

Mr. Edward E. Hood, Jr. — Mar. 1990 - Oct. 1991
Vice Chairman of the Board & Executive Officer
General Electric

Mr. Robert E. Allen — Oct. 1991 - May 1993
Chairman of the Board & CEO
AT&T

Mr. Norman R. Augustine — May 1993 - Jan. 1995
Chairman & CEO
Martin Marietta Corporation

Mr. William T. Esrey — Jan. 1995 - Mar. 1997
Chairman & CEO
Sprint Corporation

Mr. Charles R. Lee — Mar. 1997 - Sep. 1998
Chairman & CEO
GTE

Mr. Van B. Honeycutt — Sep. 1998 - Sep. 2000
Chairman, President & CEO
Computer Sciences Corporation

Mr. Daniel P. Burnham — Sep. 2000 - Aug. 2002
Chairman & CEO
Raytheon

Dr. Vance D. Coffman — Aug. 2002 - Present
Chairman & CEO
Lockheed Martin Corporation

Translating Recommendations Into Results

The NSTAC has an impressive history of providing substantive recommendations to the President that have resulted in improvements to the Nation's NS/EP telecommunications capabilities. These improvements have taken the form of new operational programs and technological solutions that benefit both industry and Government. As the Nation's security requirements and communications infrastructure evolve to meet national security needs, four NSTAC solutions remain particularly relevant.

National Coordinating Center for Telecommunications (NCC)

To better respond to the Federal Government's NS/EP communications service requirements, the NSTAC recommended the creation of a joint industry/Government national coordinating mechanism. As a result of this recommendation, the NCC was established in 1984. Since its formation, the NCC's industry and Government representatives have used this unique organization to work together during day-to-day operations, coordinate NS/EP responses during crises, and produce emergency response plans and procedures during real-world events. Recently, the importance of the NCC was illustrated when NCC members leveraged their established relationship to work jointly to quickly respond to the September 11 attacks and restore access to the telecommunications infrastructure. As the NCS transitions to the DHS, the NCC's capabilities will continue to play an important role in the Information Analysis and Infrastructure Protection Directorate.

Telecom Information Sharing and Analysis Center (Telecom-ISAC)

In May 1998, the President encouraged the creation of ISACs for each critical infrastructure sector. In response, the NSTAC concluded that the NCC already performed the primary functions of an ISAC. The National Security Council concurred and designated the NCC ISAC as the Telecom-ISAC in 2000. The Telecom-ISAC facilitates voluntary collaboration and information sharing among industry and Government participants and tracks vulnerabilities, threats, intrusions, and anomalies of the telecommunications infrastructure to avert or mitigate impacts upon NS/EP communications.

Network Security Information Exchange (NSIE)

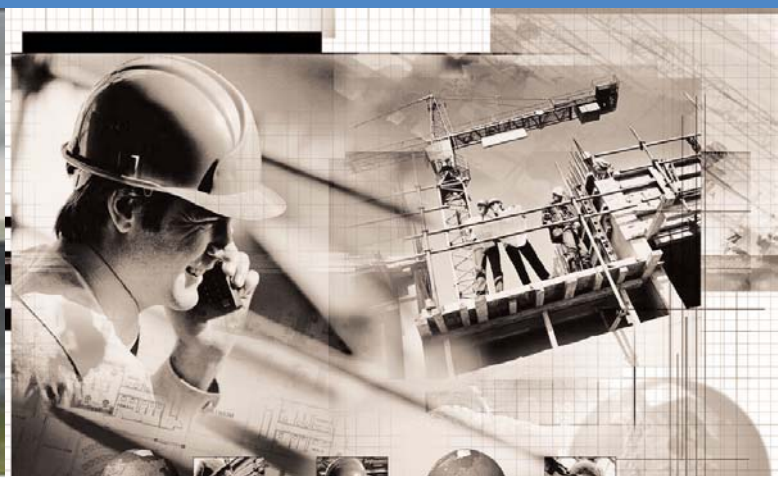
To address vulnerabilities of the Nation's communications systems to electronic intrusion, the NSTAC formed its NSIE in 1991. Within the NSIE, industry and Government representatives share information on incidents, vulnerabilities, security tools and techniques, threats, and countermeasures related to issues involving the penetration or manipulation of software and databases affecting national security and emergency preparedness communications. The NSIEs demonstrate the ongoing willingness of industry and Government to share sensitive security information relevant to protecting critical information systems in a protected and trusted environment. The NSTAC and Government NSIEs are among the most effective forums for sharing security information between industry and Government.

Priority Services

Throughout its history, the NSTAC has provided the President and the NCS assistance in the operations of priority service programs, including GETS, which provides priority processing over local and long distance segments of the public switched network, and TSP, which gives priority provisioning and restoration of circuits and was established as a result of a 1984 NSTAC recommendation. The events of September 2001 reinforced the need for, and importance of, NS/EP personnel to have priority access to communications during national emergencies. Since then, the number of TSP assignments has grown approximately 50 percent. The initiatives of the NSTAC member companies, including support for the GETS and TSP programs, were significant factors in the speed in which commercial telecommunications were re-established after the 2001 terrorist attacks in New York, Washington, DC, and Pennsylvania. The close partnership between private industry and the Federal Government also enabled homes and businesses in the affected areas to regain communications as quickly as possible.

The attacks raised the level of importance for the Federal Government to have priority service available on wireless devices. The NSTAC first recommended a wireless program in 1995. That year, the Office of the Manager, NCS, began to develop such capabilities and in 1998 the Federal Communications Commission first established rules for priority access service. Wireless Priority Service with initial operating capabilities was first activated in Washington, DC, and New York City in May 2002 with additional markets coming online later that year and in 2003. The NSTAC continues to be involved in program development by providing advice on potential barriers to ubiquitous nationwide rollout and other policy-related issues.

The initiatives of the NSTAC member companies, including support for the GETS and TSP programs, were significant factors in the speed in which commercial telecommunications were re-established after the 2001 terrorist attacks in New York, Washington, DC, and Pennsylvania.



The Way Forward

Over the past 20 years, the NSTAC has been an integral member in one of the most successful public-private partnerships. As the NCS transitions to the DHS and the Government continues to explore new ways to protect its home front and critical infrastructures—physical and virtual, the NSTAC will continue to play an important role in furthering NS/EP priorities.

The NSTAC consistently re-evaluates its priorities as changes occur in technology and in the geopolitical landscape. Over the next few years, the NSTAC will study and provide recommendations to the President and the Administration on issues related to network and cyber security; keep apprised of wireless communications issues relevant to the NS/EP user community; evaluate critical infrastructure protection as it relates to the telecommunications sector; and assess infrastructure interdependencies. In addition, the NSTAC will continue to examine new ways to encourage and remove barriers to information sharing with the increased reliance on critical infrastructure information sharing between industry and Government.

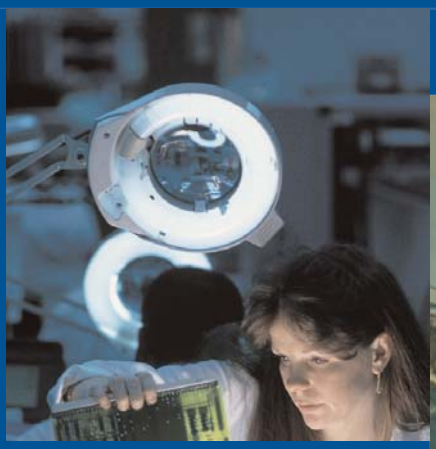
The NSTAC members and the entities they represent are committed to this partnership in support of national security and emergency preparedness on behalf of the United States and look forward to serving the President for another 20 years.

NSTAC Evolution

On September 13, 1982, President Ronald Reagan established the President's National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 to foster an industry/Government partnership to address critical government communications issues. For 20 years, the NSTAC has provided a unique forum for industry to work with the defense and civil Government agencies comprising the National Communications System. In return, the NSTAC offers Government the expertise of its member companies and associations in a variety of sectors, including telecommunications service providers, software and hardware manufacturers, information and systems security providers, major information users, and the aerospace industry.

The NSTAC's first tasking was to develop a national coordinating mechanism that could respond to Government's national security and emergency preparedness (NS/EP) requirements in a post AT&T divestiture environment. The National Coordinating Center for Telecommunications was promptly established following the NSTAC's 1983 recommendation. Other important NSTAC recommendations have also resulted in the establishment of priority service programs such as the Telecommunications Service Priority and Wireless Priority Service and other industry/Government working groups, including the Network Security Information Exchange and the Telecom Information Sharing and Analysis Center.

Since the NSTAC's inception, the telecommunications industry has undergone tremendous change. Competition among service providers was introduced in both the local and long distance markets. Internet and wireless technologies have become widely used by commercial, Government, and NS/EP users. The NSTAC has continually kept pace with these environmental changes and provided cutting edge advice to the President of the United States and Federal Government on the best ways to adapt to and utilize these new technologies to the benefit of the Nation's NS/EP posture.



More information on NSTAC
can be obtained at
www.ncs.gov/nstac.htm
or by calling (703) 607-6211