Over 25 Years of Partnership

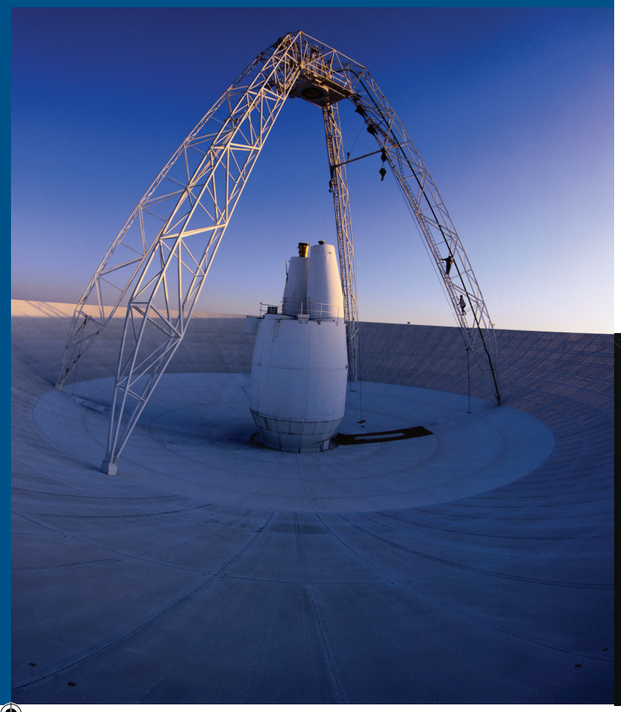
The NSTAC serves as a prominent model for trusted public/private partnerships, resulting in mutually beneficial information sharing mechanisms and the implementation of various programs to reinforce that partnership. One of the NSTAC's first efforts recommended the creation of the National Coordinating Center as an operational arm of a public/private national coordinating mechanism, and later, as the Information Sharing and Analysis Center for the communications sector, where information relevant to the protection and operation of the communications infrastructure is shared between industry and Government. The NSTAC recognized that information sharing is a key component to the industry and Government relationship, tying together all facets of the NSTAC agenda to provide resilient national telecommunications services.

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. In recent years, the Government, with the support of the NSTAC, addressed new NS/EP challenges caused by several primary factors—the convergence of traditional and broadband networks; the changing global threat environment; and the continuing global expansion of both provider and user communities. In the face of this ever-increasing complexity of the domestic and global network environment, the NSTAC's work, more so than ever, is of vital national importance, and the committee remains vigilant in aggressively addressing our Nation's highest priority NS/EP communications needs.

The President's National Security Telecommunications Advisory Committee (NSTAC)

For more information on the NSTAC, please contact—

www.ncs.gov/nstac/nstac.html
(703) 235-5516
nstac1@dhs.gov



The NSTAC Mission

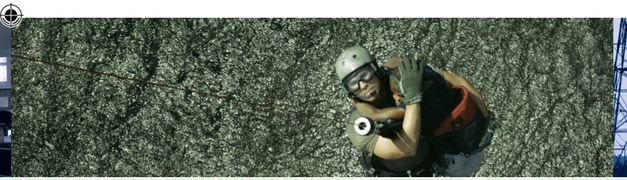
Meeting our Nation's critical national security and emergency preparedness (NS/EP) challenges requires assuring the availability and reliability of telecommunication services. The President's National Security Telecommunications Advisory Committee (NSTAC) mission is to provide the U.S. Government the best possible industry advice in these areas.

For over 25 years, the NSTAC has brought together up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. These industry leaders provide the President with advice and expertise, as well as robust reviews and recommendations. The NSTAC's goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture.

Throughout the NSTAC's history, five key themes continue to emerge as its major areas of focus—

- Strengthen national security
- Enhance cybersecurity
- Maintain the global communications infrastructure
- Assure communications for disaster response
- Address critical infrastructure interdependencies and dependencies






Strengthening National Security

A clear and constant priority for the U.S. Government as well as for the private sector is to ensure national security in today's rapidly shifting threat environment. The NSTAC continually places special emphasis on telecommunication and information system development issues to enhance national security foundations.

In its recent history, the NSTAC emphasized efforts to strengthen national security, studying issues such as network security, global infrastructure resiliency, infrastructure interdependencies, and international incident management. These examinations assist the President in securing and enhancing national security policies and technological capabilities of the Nation.

Enhancing Cybersecurity

Continuing information technology advances and the growing dependence on new forms of information services necessitate the application of strong cybersecurity practices to all critical systems supporting NS/EP requirements, especially in response to the broader threats these systems face.

- **Network Security.** To ensure up-to-date analysis and recommendations in the cybersecurity realm, the NSTAC currently is exploring key areas of network security and identifying specific issue areas to examine in greater depth. The NSTAC also is considering the legal and regulatory capabilities and restrictions to effective Government or private sector preparedness and mitigation response to cyber incidents.

- **Identity Management.** The NSTAC provided an analysis of NS/EP challenges associated with the migration from circuit-switched networks to packet-switched next generation networks (NGN). The committee developed key recommendations essential to assuring NS/EP communications in this evolving network environment, which included recommending that the Federal Government build an effective identity management framework for the NGN.

Maintaining the Global Communications Infrastructure

The U.S. public network is progressively interconnected with worldwide networks, a phenomenon that brings with it inherent risks and increased vulnerabilities. The many forms of communications services in use today dictate more complex incident management needs.

- **Satellites.** The satellite infrastructure has become a key component of communications services; consequently, the NSTAC assessed infrastructure protection policies and procedures for commercial satellite networks used for NS/EP communications. Further, the NSTAC initiated a study of the commercial communications infrastructure's dependence on the satellite-based global positioning system (GPS) and the implications of a loss of GPS to that infrastructure.

- **Globalization of the Communications Infrastructure.** To assess the implication of globalization for NS/EP communications, the NSTAC conducted an analysis of the global information infrastructure and associated NS/EP challenges; assessed the security implications of foreign network ownership; and examined technology export policies. The NSTAC reviewed processes and risks associated with network operations centers and provided operational recommendations and possible solutions with respect to the physically critical aspects of the international global infrastructure.

- **International Incident Management.** The policies and organizational mechanisms that address operational security risks and incident management in the global network community are essential components to ensuring network access and remediation during system disruptions. The NSTAC examined the existing international policy environment and incident response capabilities and made recommendations to the President intending to promote US NS/EP interests in emerging international incident management efforts.

Assuring Communications For Disaster Response

The September 11, 2001, terrorist attacks and the 2005 hurricane season underscored the criticality of resilient, reliable, and available communications in support of Government emergency response activities.

- **Priority Services.** As the underlying network elements of the Telecommunications Service Priority and the Wireless Priority Service programs evolve, the NSTAC is examining NGNs to determine how to provide the President with the necessary information to ensure the availability of communications services to critical personnel during crisis events. As a result, the NSTAC initiated an examination regarding the availability of Internet Protocol (IP) services during times of network congestion.

- **Emergency Communications Interoperability.** The NSTAC provided advice regarding the integration of a complete suite of communications technologies into the Federal Government's emergency communications capabilities. The NSTAC also addressed the communications interoperability challenges of emergency responders through an evaluation of ways in which IP-enabled capabilities and technologies might play a role in enhancing the interoperability of emergency communications.

- **Access and Credentialing.** In order to mitigate barriers to public/private sector cooperation in disaster situations, the NSTAC recommended the codification of the term "Emergency Responder (Private Sector)." This serves to incorporate telecommunications infrastructure providers into Federal response policies, and give them proper credentialing to allow priority access into disaster sites. The NSTAC is working to ensure Federal officials address NSTAC's access and credentialing concerns as they develop policy that governs national response efforts.

Addressing Critical Infrastructure Interdependencies and Dependencies

The inherent interdependencies between domestic communications networks and other infrastructure sectors pose significant threats to our national security, the availability of NS/EP communications services, and the operational capabilities of other infrastructures reliant upon communications services.

- **Telecommunications and Electric Power Interdependencies.** The NSTAC has long considered the interdependencies between the telecommunications and electric power sectors to be critical to continuous telecommunications service. The NSTAC studied the potential impact on telecommunications services in the event of a sustained power grid outage. The NSTAC has also examined the necessary criteria and processes for identifying critical industry NS/EP telecommunications facilities that qualify for priority electric power restoration and fuel distribution.

- **Critical Infrastructure Risk Assessments.** To address the dependency of various infrastructures on telecommunications, the NSTAC conducted risk assessments for the energy, financial services, and transportation sectors to heighten their awareness of cross-sector information assurance and infrastructure protection issues.

- **Financial Services.** Many financial services depend heavily upon the communications infrastructure. The NSTAC therefore examined the potential impact that a disruption of communications could have on essential financial services processes and the national economy. From this, the NSTAC identified a need for the financial services infrastructure to assure diverse and resilient access connection capabilities to the telecommunications infrastructure, and recommended the development of requirements and best practices for critical NS/EP customers.