2006-2007
NSTAC ISSUE REVIEW

THE PRESIDENT'S NATIONAL

SECURITY TELECOMMUNICATIONS

ADVISORY COMMITTEE

YEARS OF SERVING
THE PRESIDENT

The President's
National Security Telecommunications
Advisory Committee

Issue Review

A Comprehensive Review of Issues
Addressed Through April 2007

Table of Contents

Executive Summary i

Active Issues

Telecommunications and Electric Power Infrastructure Interdependencies 3
National Coordinating Center 9
Emergency Communications and Interoperability 15
International Communications 21
Global Infrastructure Resiliency 27
Influenza Pandemic 29

Standing Issues

Legislation and Regulation 33
Research and Development 43

Previously Addressed Issues

Automated Information Processing 49
Commercial Network Survivability 51
Commercial Satellite Survivability 53
Common Channel Signaling 57
Electromagnetic Pulse 59
Energy 61
Enhanced Call Completion 65
Financial Services 69
Funding of NSTAC Initiatives 71
Globalization 73
Industry/Government Information Sharing and Response 75
Industry Information Security 79
Information Assurance 81
Information Sharing/Critical Infrastructure Protection 85
Intelligent Networks 89
International Diplomatic Telecommunications 91
International National Security and Emergency Preparedness Telecommunications 93
Last Mile Bandwidth Availability 95
National Coordinating Mechanism 99
National Information Infrastructure 101
National Research Council Report 105
National Telecommunications Management Structure 107
Network Convergence 109

Network Security 119
Obtaining Critical Telecommunications Facility Protection During a Civil Disturbance 131
Physical Security of the Telecommunications Network 133
Response to September 11, 2001, Terrorist Attacks 137
Termination of Cellular Networks During Emergency Situations 139
Telecommunications Industry Mobilization 141
Telecommunications Service Priority 143
Telecommunications Service Priority Carrier Liability 145
Telecommunications Systems Survivability 147
Underground Storage Tanks 149
Wireless Security 151
Wireless Services (Including Priority Services) 155

Appendix A – NSTAC Implementing and Governing Documentation

Charter of the President's National Security Telecommunications Advisory Committee A-3
Bylaws of the President's National Security Telecommunications Advisory Committee A-5
Executive Order 12382President's National Security Telecommunications Advisory Committee A-9
1983 Correspondence from the U.S. Department of Justice, Antitrust Division A-11

Appendix B – NSTAC Membership

The President's National Security Telecommunications Advisory Committee Membership (as of April 17, 2007) B-3

Appendix C – 2006-2007 NSTAC Executive Report to the President

Executive Report on the 2007 Meeting of the President's National Security Telecommunications Advisory Committee – April 26, 2007 . . . . . C-3
Attachment 1: Report Recommendations to the President from the 2007 Meeting of the President's National Security Telecommunications Advisory Committee – April 26, 2007 . . . . . C-15
Attachment 2: Attendance of Members at the 2007 Meeting of the President's National Security Telecommunications Advisory Committee C-19

Appendix D – Acronyms

Acronym List D-3

Executive Summary

Executive Summary

Purpose

This edition of the *President's National Security Telecommunications Advisory Committee Issue Review* provides a comprehensive report of issues addressed by the President's National Security Telecommunications Advisory Committee (NSTAC) from its first meeting in December 1982 to its most recent meeting on April 26, 2007. For each active, standing, and previous issue addressed by the NSTAC, the NSTAC Issue Review provides the following information when applicable: names of the investigating groups, length of time required for the investigation, issue background, a synopsis of NSTAC actions and recommendations, actions resulting from NSTAC recommendations, reports issued, and members of the current/active investigating groups.

Background

On September 13, 1982, President Ronald Reagan issued Executive Order (E.O.) 12382, establishing the President's NSTAC. The NSTAC, a presidentially-appointed advisory body composed of up to 30 senior executive level representatives from the communications, hardware, software and security services, banking, and aerospace companies provides the President with a unique source of national security and emergency preparedness (NS/EP) communications policy expertise. Several factors influenced the establishment of the NSTAC at that time, including the divestiture of AT&T, increased Government reliance on commercial communications, and the potential impact of new technologies on communications supporting NS/EP requirements. Appendix A of this document includes E.O. 12382, as well as additional NSTAC implementing and governing documentation. Appendix B provides a listing of current NSTAC members as of April 26, 2007.

Since its inception, the NSTAC has advised seven administrations on issues pertaining to the reliability and security of communications technologies and their impact on the Nation's ability to protect its critical infrastructures — issues vital to America's security and economic interests. Today, members of the communications and information technology industries, as well as the Federal Government, recognize the NSTAC as a model for industry/Government collaboration. NSTAC accomplishments include many substantive recommendations to the President leading to enhancements of the Nation's NS/EP communications capabilities and critical infrastructure policies, and increased safeguards to the Nation's communications infrastructure.

Over the past 24 years, the NSTAC has worked cooperatively with the National Communications System (NCS), an interagency consortium of Federal departments and agencies that serves as the focal point for NS/EP communications planning for any crisis or disaster and provides staff support and technical assistance to the Committee. By virtue of its mandate to address NS/EP communications issues, the NSTAC's partnership with the NCS is unique in two ways: (1) it facilitates industry involvement with both the defense and civil agencies comprising the NCS; and (2) it regularly sustains interaction between industry and the NCS member departments and agencies through the National Coordinating Center (NCC); the Communications Information Sharing and Analysis Center; the Network Security Information Exchange (NSIE) process; and most recently through the Communications Sector Coordinating Council, which serves as a point of contact for its counterpart the Government Coordinating Council. The NSTAC's perspective and its experiences with a wide range of Federal departments and agencies make the committee a key strategic resource for the President and his national security and homeland security teams in their efforts to protect our Nation's critical infrastructures in today's dynamic and evolving environment.

Membership on the NSTAC's primary working body—the Industry Executive Subcommittee (IES)—consists of one representative from each company, appointed by his or her NSTAC Principal. The IES holds regular meetings to consider issues, analyses, and/or recommendations for presentation to the NSTAC Principals (and in turn to the

President), and assists in the formation of task forces and working groups as directed by the Committee to address specific issues requiring in-depth analyses.

From May 2006 to May 2007, the NSTAC operated the following subordinate task forces and working group:

- **The National Coordinating Center Task Force** remained active and awaited further tasking as follow-on to the *NSTAC Report to the President on the National Coordinating Center.*

- **The Telecommunications and Electric Power Interdependency Task Force** examined the NS/EP issues associated with the interdependency of the telecommunications and electric power sectors and how these interdependencies will affect the future of the telecommunications network.

- **The Emergency Communications and Interoperability Task Force** initiated an examination of how communications technologies should be integrated into the Federal Government's emergency communications planning to support NS/EP activities and to recommend a future direction to ensure a survivable and interoperable communications architecture for responders.

- **The International Task Force** examined the current international NS/EP communications environment to evaluate the present U.S. operational strategies, policies, and frameworks for international collaboration and prepare recommendations to the President to promote U.S. NS/EP interests in emerging international network security efforts.

- **The Pandemic Study Group** worked to formulate prioritization recommendations for the telecommunications infrastructure so that NS/EP services that rely heavily on the sector can remain stable and usable under any circumstances.

- **The Global Infrastructure Resiliency Working Group** examined the NS/EP concerns associated with the global communications infrastructure.

- **The Legislative and Regulatory Task Force** continued to review and analyze legislative and regulatory activities affecting the NS/EP community. In addition, the group developed recommendations to the President on the need for adequate Federal assistance to telecommunications infrastructure providers during disasters such as hurricanes.

- **The Research and Development (R&D) Task Force** held the first-ever international R&D Exchange Workshop in Ottawa, Ontario, Canada in September of 2006. The Workshop focused on international collaboration on cyber security research and development.

Many NSTAC recommendations result in operational activities that enhance NS/EP communications and information systems. For example, in its first set of recommendations to the President, the NSTAC suggested the establishment of the NCC, an industry and Government coordination center for day-to-day operational support to NS/EP communications. In addition, the NSTAC assisted the Office of the Manager, National Communications System in developing and eventually implementing the Telecommunications Service Priority (TSP) System—one of the NCS' most utilized priority service programs. Furthermore, an NSTAC recommendation also resulted in the establishment of separate NSTAC and Government NSIEs, which meet regularly to address the threat of electronic intrusions and software vulnerabilities, as well as to discuss mitigation strategies to protect the Nation's critical communications and information systems. Finally, the NSTAC recommended the development of an access and credentialing program to assist private sector companies in gaining access to federal disaster sites following an event of national significant. In response to this recommendation, the Department of Homeland Security developed, in partnership with Federal, State, and local Government entities, as well as a private sector company, an access standard operating procedure (SOP) to ensure that private critical infrastructure responders receive priority access to disaster areas. The access SOP had been adopted by the State of Georgia and has been distributed to a

broader community, including the Homeland Security Advisors and the National Association of Regulatory Commissioners.

Appendix C of this document contains the 2007 NSTAC Executive Report to the President, which includes summaries of the April 2007 NSTAC Open and Closed Sessions, as well as recommendations made to the President during the 2006-2007 NSTAC Cycle (May 2006 – April 2007).

Copies of NSTAC reports pertaining to the issues addressed in this document are available through:

Office of the Manager
National Communications System
Customer Service Division
Mail Stop # 8510
245 Murray Lane, Building 410
Washington, DC 20528
(703) 235-5525

www.ncs.gov/nstac/nstac.html
nstac1@dhs.gov

Active Issues

Telecommunications and Electric Power Infrastructure Interdependencies

Investigation Group / *Period of Activity*

Electromagnetic Pulse Task Force
September 1983 – October 1985

Telecommunications System Survivability Task Force
March 1986 – June 1989

Energy Task Force
August 1988 – March 1990;
October 1991 – May 1993

Telecommunications and Electric Power Interdependency Task Force
January 2005 – December 2006

Issue Background

For decades, professionals in the telecommunications industry have been concerned with the potential impact a sustained power grid outage would have on the telecommunications network. Recent events, including the power outage in Eastern Canada in January 1998, the terrorist attacks of September 11, 2001, the Northeast blackout in August 2003, and the devastating hurricane seasons of 2004 and 2005, continued to draw attention to the interdependencies between the two sectors and re-energized industry and Government efforts to find strategies to both dampen the impact of and mitigate against further occurrences. In addition to man-made and natural threats to the infrastructure, changing trends in telecommunications network design also raise questions about the continued reliance of the telecommunications sector on electric power sources. With the growth of the next generation network (NGN), the attendant increase in the use of wireless and mobile technologies, and the dispersion of network elements, the network and its users will increasingly rely on commercial electric service to supply the necessary power.

In this environment, the telecommunications and electric power sectors will increasingly be required to work together to ensure NS/EP services remain available to respond to terrorist incidents or natural disasters.

History of NSTAC Actions and Recommendations

The NSTAC consideration of the interdependencies between the telecommunications and electric power sectors began in 1983 with the Committee's response to a Government request for industry's perspective on the options available to industry and Government for improving the electromagnetic pulse (EMP) survivability of the Nation's telecommunications networks. Based on the analysis conducted by its Electromagnetic Pulse (EMP) Task Force, the Committee provided several recommendations to the President on the issue in its *Electromagnetic Pulse Final Task Force Report.*

The NSTAC gave further consideration to the interdependency between the telecommunications and electric power sectors when it reviewed the vulnerability of the telecommunications network to the loss of commercial electric power and presented its finding in its *Telecommunications Systems Survivability Electric Power Survivability Status Report.* As a follow-up to its vulnerability analysis, the Committee established the Energy Task Force, which it charged with analyzing solutions to mitigate against the effects of electric power outages on telecommunications. In 1988, the Energy Task Force, with participation from the Department of Energy (DOE), the NCS, and the North American Electric Reliability Council (NERC) undertook its activities, examining interdependencies between the two sectors after a major earthquake.

In October 1991, the NSTAC established a follow-on Energy Task Force and charged it to support the OMNCS in its efforts with DOE to develop criteria and a process for identifying critical industry NS/EP telecommunications facilities that qualify for electric power restoration and priority fuel distribution. Based on the task forces analysis, the NSTAC issued its recommendations to the President on the issue in its *Energy Task Force Final Report* in 1993.

Interdependency issues arose again as a result of extensive power and telecommunications outages during the hurricane season of 2004 in the southeast region of the U.S. Mr. F. Duane Ackerman, then Chairman and Chief Executive Officer of BellSouth and NSTAC Chair, highlighted his concerns about the situation in his speech at the Research and Development Task Force's October 2004 Research and Development Exchange (RDX) Workshop in Monterey, California. Due to the dependence of the telecommunications network on electric power services, Mr. Ackerman noted the need for enhanced and alternative emergency power technologies. In addition, as the network becomes increasingly distributed, he noted that issues of reliability and ease of communication and coordination between the telecommunications and electric power industries will become increasingly important during natural disasters or terrorist incidents.

As a result, in 2005, the NSTAC established the Telecommunications and Electric Power Interdependency Task Force (TEPITF) to further evaluate how the telecommunications and electric power sector interdependencies will affect the future of the telecommunications network. The task force subsequently divided the work into two streams—an examination of the people and processes involved in national security communications and restoration and an evaluation of the technological implications of future events.

Based on the completion of the first work stream, the NSTAC issued its *People and Processes: Current State of Telecommunications and Electric Power Interdependencies Report* in January 2006, In the report, the NSTAC recommended that the President direct his departments and agencies to:

- Define and establish the term Emergency Responder within the National Response Plan (NRP) and other appropriate plans, guidance, directives, and statutes, including other local, State and Federal Government emergency plans;
- Ensure key response personnel of critical infrastructure owners and operators in the telecommunications and electric power sectors be designated as Emergency Responders;
- Include fuel supply, security, site access, and other required logistical support to critical telecommunications and electric power infrastructures as part of the Emergency Responder planning process to ensure priority restoration to critical telecommunications and electric power;
- Foster and promote effective emergency coordination structures to ensure reliable and robust communication between the two sectors and local, regional, State, and Federal Governments;
    - Review examples of proven priority restoration models at the State and regional levels. Encourage States and metropolitan regions without effective models to improve and update their existing frameworks; and
    - Encourage effective information sharing models at the local/regional Emergency Responder level, both in advance of a natural disaster and during the emergency restoration period. When developing these models, liability issues should be considered.

Throughout 2006, the NSTAC continued its examination of long-term interdependency issues. Specifically, the NSTAC defined the "long-term outage" (LTO) phenomenon—an interruption of communications and/or electricity for a period long enough, and within a large enough geographic region, to hamper the provision of telecommunications and electric power even by alternative means. Such an outage has not occurred in North America to date, but could occur in any critical infrastructure and, in the worst case, have a cascading effect on other sectors. The NSTAC focused its research on an evaluation of technological interdependencies that will affect telecommunications networks in the future. Based on its investigation of the LTO phenomenon, the NSTAC issued its final report, *The NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: The*

Implications of Long-Term Outages in December 2006. In the report, the NSTAC recommended that the President direct his departments and agencies to:

- Commission a Government-funded, cross sector and cross border engineering analysis of the North American telecommunications and electric power infrastructures, with attention given to further international considerations, to determine the interdependencies in LTO situations for both the current and the next generation network environment, and to estimate the attendant costs of mitigation strategies, including the following:
  - Investigating how dependencies and interdependencies will be affected by technology and structural changes in both sectors; and
  - Supporting exercises at the local, State, regional, national, and international level that investigate the dependencies and interdependencies between the two sectors during an LTO.
- Analyze and evaluate current governance procedures applicable to an LTO to determine the appropriate transition from local to national management authority during an LTO. Internet recovery issues (as they relate to the convergence of the telecommunications network) should also be reviewed, but such a review should not be limited to an LTO event.
- To reduce dependencies between the sectors and maintain a minimum level of internal service availability during an LTO, vigorously support selected science and technology applications, including the following:
  - Transformer Prototype Technology,
  - Power Conservation Technology for Telecommunications, and
  - Fuel Cell Technology.
- In concert with industry, support the advent and development of cross sector situational analysis tools to facilitate information sharing between industry and Government in advance of, during, and after an LTO.
- As stated in the *NSTAC Report to the President on People and Processes: Current State of Telecommunications and Electric Power Interdependencies,* continue to promote increased collaboration between both the telecommunications and electric power sectors and emergency management authorities at the local, regional, State, national, and international levels to facilitate recovery from an LTO.

For further information on telecommunications and electric power interdependencies, please see the Infrastructure Interdependencies section in the Previously Addressed Issues section of this *NSTAC Issue Review.*

Actions Resulting from NSTAC Recommendations

In response to the devastation caused by Hurricanes Katrina, Rita, and Wilma, the Federal Communications Commission (FCC) established the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks. In its final report, the Panel expressed support for the NSTAC's recommendation to establish a national standard for credentialing telecommunications repair workers as well as its recommendation to designate telecommunications infrastructure providers as "emergency responders" under the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* (Stafford Act), the NRP, and other legislative documents as appropriate. Although review of the NRP is not yet complete, the NCS has worked to incorporate the term "essential service provider" (ESP) into the NRP and to ensure that these providers receive appropriate support during a national crisis. In addition, the FCC issued a Notice of Proposed Rulemaking requesting comments from industry on the recommendations found within its final panel report, including those recommendations made by the Committee.

Additionally, DHS, in partnership with Federal, State, and local Government entities, as well as a private sector company, developed an access standard operating procedure (SOP) to ensure that private critical infrastructure responders receive priority access to disaster areas. Out of state telecommunications and electric power service providers must meet the same criteria as local service providers, including placement on the authorized list or having appropriate credentials. The mechanisms for gaining a place on such a list or obtaining such credentials are only now in the initial stages of being determined by the local, State, and regional Government entities. DHS is also incorporating the Emergency Responder concept into procedures and processes for private sector resource requests. The access SOP had been adopted by the State of Georgia and will be used a model for other States.

Furthermore, section 607 of the *Security and Accountability for Every Port Act of 2006,* which President George W. Bush signed into law on October 13, 2006, amended the Stafford Act by providing a list of essential services whose providers may be defined as ESPs. The Act listed privately owned telecommunications among those services, and declared that Federal agencies may not prevent ESPs from accessing disaster sites or otherwise impede their efforts to conduct response and recovery of the telecommunications infrastructure "to the greatest extent possible." While the measure partially addresses the NSTAC's concern about site access, it does not clarify that telecommunications infrastructure providers may have access to non-monetary Federal resources during and following a disaster. ESPs include both telecommunications and electric power professionals.

Reports Issued

Electromagnetic Pulse Task Force Status Report, January 1984.

Electromagnetic Pulse Final Task Force Report, July 1985.

Telecommunications Systems Survivability Electric Power Survivability Status Report. Energy Task Force Final Report, August 1988.

Energy Task Force Final Report, February 1990.

Energy Task Force Final Report: Telecommunications Electric Service Priority and National Energy Strategy Review, April 1993.

The NSTAC Report to the President on People and Processes: Current State of Telecommunications and Electric Power Interdependencies, January 2006.

The NSTAC Report to the President on Telecommunications and Electric Power Interdependencies: The Implications of Long-Term Outages, December 2006.

Telecommunications and Electric Power Interdependency Task Force Membership

Nortel
Dr. John S. Edwards, Chair

AT&T, Incorporated
Ms. Rosemary Leffler

Bank of America Corporation
Mr. Roger Callahan

BellSouth Corporation
Mr. David Barron

Cingular Wireless LLC
Mr. Kent Bowen

Computer Sciences Corporation
Mr. Guy Copeland

CTIA – The Wireless Association
Mr. Bob Bolster

Microsoft Corporation
Mr. Philip Reitinger

Qwest Communications International, Incorporated
Mr. Jon Lofstedt

Raytheon Company
Mr. Frank Newell

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Nextel Corporation
Mr. Todd Tobis

Telcordia Technologies, Incorporated
Ms. Louise Tucker

Unisys Corporation
Ms. Linda Howard

United States Telecom Association (USTelecom)
Mr. David Kanupke

Verizon Communications, Incorporated
Mr. James Bean

Other Telecommunications and Electric Power Interdependency Task Force Industry Participants

AT&T, Incorporated
Mr. Harry Underhill

Black and Veatch Corporation
Mr. John Voeller

Computer Sciences Corporation
Mr. Peter Andersen

Consolidated Edison Company of New York
Mr. Peter Hofmann

Edison Electric Institute
Mr. Laurence Brown

Electric Power Research Institute
Mr. Thomas Kropp
Mr. Robert Schainker

George Washington University
Dr. Jack Oslund

Independent Electricity System Operator
Mr. Stuart Brindley

Industry Canada
Mr. John Kluver
Mr. Robert Leafloor

Lucent Technologies, Incorporated
Mr. Brent Greene

Lucent Technologies (Bell Labs)
Mr. Richard Krock

Microsoft Corporation
Ms. Lynn Terwoerds

MITRE Corporation
Dr. Edward Jacques

National Rural Electric Cooperative Association
Mr. Barry Lawson

National Telecommunications and Information Administration
Mr. Daniel Hurley

North American Electric Reliability Council
Mr. Larry Kezele
Mr. Louis Leffler

Pepco Holdings, Incorporated
Mr. Richard Kafka

Qwest Communications International, Incorporated
Mr. Barry Lawson

Sprint Nextel Corporation
Ms. Allison Growney
Mr. William Hitchcock
Mr. John Quigley

Telcordia Technologies, Incorporated
Mr. Arun Handa

Texas Utilities
Mr. William Muston

United Telecom Council
Mr. Brett Kilbourne
Ms. Prudence Parks

Telecommunications and Electric Power Interdependency Task Force Government Participants

Central Intelligence Agency
Mr. Thomas Donahue

Department of Defense
Mr. Michael Shanahan

Department of Energy
Mr. John Greenhill

Department of Homeland Security
Ms. Michele Bruich
Lt. Col. Cheryl Edwards
Mr. Thomas Falvey
Ms. Giang Huynh
Ms. Carolyn King
Mr. Thad Odderstol
Lt. Col. Joanne Sechrest
Capt. Thomas Wetherald

National Coordinating Center

Investigation Group / *Period of Activity*

National Coordinating Mechanism Task Force
December 1982 – November 1984

Telecommunications System Survivability Task Force
March 1986 – June 1989

National Coordinating Center for Telecommunications Vision Task Force
October 1996 – April 1997

Operations Support Group
April 1997 – September 1999

Information Sharing/Critical Infrastructure Protection Task Force
September 1999 – May 2000

National Coordinating Center Task Force
December 2004 – Present

Issue Background

Following the divestiture of the AT&T monopoly in 1982, the telecommunications industry and the Federal Government collectively developed the concept of a national coordinating mechanism (NCM) by which the public and private sectors could coordinate national security and emergency preparedness (NS/EP) telecommunications efforts. A year later, the President's National Security Telecommunications Advisory Committee (NSTAC) recommended the creation of the National Coordinating Center (NCC) as the operational arm for the NCM. Consequently, in 1984, President Ronald Reagan established the NCC within the National Communications System (NCS) via Executive Order (E.O.) 12382, *President's National Security Telecommunications Advisory Committee.*

Since that time, threats to the NS/EP telecommunications infrastructure have changed significantly, heightening the importance of daily coordination between industry and Government. In May 1998, the President released Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures,* a critical infrastructure protection (CIP) directive calling for, among other things, industry participation in the Government's efforts to ensure the security of the Nation's infrastructures. After studying the directive, the NSTAC recommended the NCC be designated the Telecommunications Information Sharing and Analysis Center (ISAC) as the NCC had already been performing similar functions in preparation for the Year 2000 rollover efforts.

The NCC played a key role in maintaining and reestablishing NS/EP communications during and after the terrorist attacks of September 11, 2001. In March 2003, the NCC became part of the DHS as a result of the transfer of the NCS from the DOD. Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection,* issued in December 2003, succeeded PDD 63 and established a new national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attacks. As DHS continues to grow and evolve, the NCC must also periodically reconsider its structure, organization, and approach to keep pace with rapid legal and regulatory changes.

In 2007, the NCC finds itself with three distinct missions:

- Serving the White House and NCS Member Agencies through its NS/EP mission;
- Serving DHS through its CIP mission; and
- Fulfilling information sharing requirements through its information sharing and analysis function.

History of NSTAC Actions and Recommendations

The NSTAC has emphasized the importance of industry/Government coordination on NS/EP telecommunications since its inception over two decades ago. In its first report to the President in May 1983, the NSTAC recommended the development of the NCC—the operational arm for the NCM approved by Government a year earlier to assist industry and

Government in coordinating NS/EP telecommunications services in times of emergency. In 1984, the NSTAC followed this first report with its *National Coordinating Mechanism Implementation Plan* to assist the Government in determining how best to execute the coordinating mechanism.

Since that time, the NSTAC has periodically revisited the NCC both conceptually and operationally to evaluate its mission, information sharing procedures, and overall effectiveness as changes occurred in the threat, policy, and technological environments facing the telecommunications industry. For instance, in 1987, the Committee's Telecommunications Systems Survivability (TSS) Task Force reviewed Government actions taken on the NCM recommendations and determined that the recommendations were carried out effectively. Furthermore, the task force determined that NCS member organizations' representation in the NCC should continue. In its *The NCC Intrusion Incident Reporting Criteria and Format Guidelines,* the NCC Vision Task Force established standardized reporting criteria and outlined steps to improve NCC electronic intrusion report collection, processing, and distribution.

In 1997, the Operations Support Group (OSG) worked closely with the NCS member organizations and NCC industry representatives to develop a common framework for assessing the Center's ongoing role in NS/EP telecommunications. In its *Operations Support Group Report,* the NSTAC recommended that the President establish a mechanism within the Federal Government with which the NCC could coordinate on intrusion incident information issues, and with which NSTAC groups could coordinate the development of standardized reporting criteria. In 1999, the Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force investigated potential recommendations to be made in support of the goals outlined in PDD-63. As a result, the NSTAC issued numerous recommendations to the President including the development of mechanisms and processes for conducting protected, operational information sharing, the designation of the NCC as the telecommunications ISAC, the necessary continued interaction with Government leaders responsible for PDD–63 implementation, and the expansion of participation in the telecommunication ISAC during subsequent phases to include a broader spectrum of IT and communications industry companies. As a result, the Federal Government officially established the NCC as the Telecommunications ISAC in January 2000.

Following the October 21, 2004, NSTAC Principals' Conference Call, the Committee established the National Coordinating Center Task Force (NCCTF) to examine how best to balance both traditional network and cyber concerns and the changing national security environment to include homeland security concerns within the NCC moving forward. Specifically, the Principals requested that the task force examine the future mission and role of the NCC, including:

- How should the industry members of the NCC continue to partner with Government?
- How should the NCC be structured relative to the dual missions of CIP and NS/EP?
- How does the new DHS Sector Coordinating Council (SCC) approach affect the NCC?

Throughout 2005 and early 2006, the NCCTF deliberated on numerous issues, focusing its discussions on the NCC's organizational structure, information sharing and analysis, leadership, incident management and response, and international mutual aid. To gain additional insight into incident management, and information sharing practices in particular, the task force co-hosted an all-day incident management subject matter experts meeting with the NGNTF on August 30, 2005. The task force also internalized lessons learned from Hurricane Katrina response and recovery efforts including those derived by the White House on improved industry and Government coordination in its *The Federal Response to Hurricane Katrina: Lessons Learned* report. Of particular interest and concern to the task force following Hurricane Katrina were questions related to the role of the NCC and the NCS in NS/EP telecommunications planning and incident response as entities within the new DHS and command and control issues associated with Emergency Support

Function (ESF) #2—Communications support agencies. The task force determined that better delineation of roles and responsibilities, especially with regard to data reporting and the prioritization and escalation of requests, would improve incident response and establish clearer points of contact to address issues, reduce duplication of effort, and improve focus on fulfilling missions.

Based on the NCCTF's analysis of issues facing the NCC, the NSTAC recommended that the President:

- Direct the Secretary of Homeland Security, the Director of the Office of Science and Technology Policy, the Secretary of Defense, and other ESF#2 Federal support agencies to develop and implement policies and procedures with respect to: (1) managing and escalating requests from the NCC, and (2) the delineation of authorities and responsibilities when ESF#2 is invoked.

- Direct the OSTP and the Homeland Security Council to join with the Communications SCC and the IT-SCC to support an industry-led task force with the primary goal of planning a regional communications and IT coordinating capability in the Gulf Coast and Southeastern regions prior to the 2006 hurricane season. Subsequently, the task force will determine the best approach for a long-term regional communications and IT coordinating capability that can serve all regions of the Nation. The task force should primarily be made up of industry representatives, as well as Federal, State, and local Government representatives.

- Direct the Secretary of Homeland Security to expand the NCC to include both communications and IT companies and organizations. The NCC would be a cross sector industry/Government facility with a round-the-clock watch, and would be brought up to full strength during emergencies.

- Direct the Secretary of Homeland Security to engage the private sector in critical infrastructure protection activities by increasing the flow of threat information to the private sector, facilitating private sector participation in impact analyses, and clarifying policies for the protection of private sector information.

- Direct the Secretary of Homeland Security to improve the ESF#2 Emergency Response Training and Exercise program, with a focus on enhancing coordination among industry members and Federal, State, and local responders during incidents of national significance. This program should focus on sector interdependencies for both physical and cyber threats, and would aim to produce actionable results. Industry must be involved from the earliest planning stages.

- Encourage the Secretary of Homeland Security to improve the Federal Government's cyber response strategy to delineate roles and responsibilities of Government and the private sector in the National Response Plan (NRP), aligning communications and cyber operations centers, and enhancing relationships with international computer emergency readiness teams.

- Direct the Secretary of Homeland Security and other Government stakeholders to examine the value derived from the NCC collaboration and, if sufficiently supported, commit the resources necessary to strengthen and support the organization and its mission.

To further these recommendations, the NCCTF developed an action item roadmap to assist the NCC in its efforts to address new issues and challenges over the next five years. The NCCTF continues to monitor the status of the implementation of these recommendations, roadmap action items, and other related issues as they arise.

Actions on NSTAC Recommendations

The NCS has initiated numerous efforts to address the recommendations in the *NSTAC Report to the President on the National Coordinating Center.* Most significantly, the Office of Cyber Security and Communications has established a "tiger team" to examine the consolidation of the NCC, the United States Computer Emergency Readiness Team, and

the Information Technology ISAC, as the NSTAC recommended. In addition, several of the NSTAC's recommendations are being addressed through the rewrite of the NRP and the ESF#2 Annex.

For more information regarding the NCC's development, please see the National Coordinating Mechanism, Information Sharing/Critical Infrastructure Protection, and the Industry/Government Information Sharing and Response sections in the Previously Addressed Issues section of this *NSTAC Issue Review.*

Reports Issued

National Coordinating Mechanism Task Force Report, May 1983.

National Coordinating Mechanism Implementation Plan (Final Report), January 1984.

Telecommunications Systems Survivability Review of Government Actions in Response to NSTAC-Recommended Initiatives, June 1988.

Operations Support Group Report, December 1997.

Information Assurance Policy Subgroup of the Information Infrastructure Group and the National Coordinating Mechanism Subgroup of the Operations Support Group Joint Report: Information Assurance, December 1997.

Operations Support Group Report, September 1998.

Operations Support Group Report, June 1999.

Information Sharing/Critical Infrastructure Protection Task Force Report, May 2000.

NSTAC Report to the President on the National Coordinating Center, May 2006

National Coordinating Center Task Force Membership

Verizon Communications
Mr. James Bean, Chair

Sprint Nextel Corporation
Mr. John Stogoski, Vice Chair

AT&T, Incorporated
Ms. Rosemary Leffler
Mr. Harry Underhill

BellSouth Corporation (Currently with Microsoft Corporation)
Ms. Cristin Flynn Goodwin

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

CTIA – The Wireless Association
Mr. Christopher Guttman-McCabe

Lockheed Martin Corporation
Dr. Allen Dayton

Lucent Bell Labs
Mr. Richard Krock

Microsoft Corporation
Mr. Philip Reitinger

Nortel
Dr. John Edwards

Qwest Communications International, Incorporated
Mr. Thomas Snee

Raytheon Company
Mr. Frank Newell

Science Applications International Corporation
Mr. Henry Kluepfel

United States Telecom Association (USTelecom)
Mr. David Kanupke

VeriSign, Incorporated
Mr. Michael Aisenberg

Verizon Communications, Incorporated
Mr. Roger Higgins

Other National Coordinating Center Task Force Industry Participants

Cingular Wireless LLC
Mr. James Bugel

George Washington University
Dr. Jack Oslund

Telecommunications Industry Association
Mr. Daniel Bart
Mr. David Thompson

Qwest Communications International, Incorporated
Mr. Jon Lofstedt

Verizon Communications, Incorporated
Ms. Ernestine Gormsen

National Coordinating Center Task Force Government Participants

Department of Homeland Security
Mr. Jeffrey Glick
Mr. Michael Lombard
Mr. Donald Smith
Ms. Christina Watson

Federal Reserve Board
Mr. Charles Madine

General Services Administration
Mr. John Migliaccio
Mr. Thomas Sellers

Office of Management and Budget
Ms. Kimberly Johnson

Office of Science & Technology Policy
Ms. Linda Haller Sloan
Mr. Mark LeBlanc

Emergency Communications and Interoperability

Investigation Group / *Period of Activity*

Emergency Communications and Interoperability Task Force
January 2006 – Present

Issue Background

Over the course of three months in the summer/fall of 2005, Hurricanes Katrina, Rita, and Wilma battered the U.S. Gulf Coast region, destroying homes and communities, as well as entire portions of the telecommunications infrastructure. The destruction posed unprecedented communications challenges and revealed a lack of sufficient operability and interoperability among the multiple public and private response and recovery organizations supporting emergency communications situations. Hurricane Katrina alone impacted an area approximately 90,000 square miles wide, disrupted service to approximately 3 million phone lines, and disabled first responder communications in multiple parishes. Restoration efforts were severely hindered by the lack of access prioritization to commercial networks for first responders. These powerful lessons magnified the importance of Government vigilance in leveraging a full suite of communications capabilities, to protect and ensure national security and emergency preparedness (NS/EP) telecommunications in the future.

History of NSTAC Actions and Recommendations

In response to concerns regarding the sufficient operability and interoperability of emergency communications systems during the 2005 hurricane season, the NSTAC established the Emergency Communications and Interoperability Task Force (ECITF) to develop recommendations regarding short-term interoperability solutions for responders in advance of the 2006 hurricane season. In addition, the Committee requested that the task force investigate how a complete suite of communications technologies, including wireline, terrestrial wireless, broadcast, and satellite communications, should be integrated into the Federal Government's emergency communications planning, and how they can more effectively support NS/EP activities; and to identify rapidly deployable interoperability solutions and recommend a strategic direction for the future that can assure a more survivable and interoperable nationwide communications architecture for responders.

Based on the ECITF's initial analysis in March 2006, the NSTAC provided short-term recommendations in a *Letter to the President on Emergency Communications and Interoperability (The Letter),* outlining emergency communications and interoperability issues and identifying immediately applicable actions to improve responder communications capabilities. Specifically, the NSTAC recommended that the President direct the Department of Homeland Security (DHS) to:

- Establish a uniform protocol working with Federal, State, and local Governments that can dynamically identify their emergency management coordinators' contact information, especially during times when regular contact information is changed due to event situations, and a capability to share that information with DHS.

- Accelerate efforts to create an initial deployable communications capability for the Gulf Coast region in accordance with Recommendation #37 of the February 2006 report, *The Federal Response to Hurricane Katrina: Lessons Learned* (Lessons Learned Report).

- Formally integrate the NCS' NS/EP priority programs into the *National Emergency Communications Strategy* pursuant to Recommendation #34 of the Lessons Learned Report.

The NSTAC recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions:*

- **Expand Use of Deployable Communications Capabilities.** Direct the Department of Homeland Security (DHS) to incorporate into its emergency

communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure. The President should also direct the DHS to expand and enhance use of the Wireless Priority Service (WPS) program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi carrier WPS end to end solutions that facilitate the rapid restoration of essential wireless network elements.

- **Enhance the Telecommunications Service Priority (TSP) Program for Wireless Networks.** Direct the DHS and other responsible Federal agencies to explore enhancements to the TSP program to accommodate expanded requests from national security and emergency preparedness (NS/EP) users of wireless telecommunications services at critical sites. The President should also direct Federal agencies, and encourage State and local agencies, to fully utilize the existing provisions of TSP and to apply for the enhanced wireless TSP coverage provisions as they are developed for use at their critical sites.

- **Improve NS/EP Policy to Support Emergency Communications.** Modernize existing NS/EP policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities. Specifically, additional Presidential policy guidance is required to:

  - Clearly delineate the NS/EP and emergency communications roles and functions of the National Communications System, the National Cyber Security Division, and the new Office of Emergency Communications, as established by the *DHS Appropriations Act of 2007,* and any other DHS organization, such as the Science and Technology Directorate and the Federal Emergency Management Agency, with a role or responsibility in the area of emergency communications;

  - Preserve and maintain critical NS/EP functions and capabilities that support the National leadership; and

  - Ensure Executive oversight across the Federal Government for a fully coordinated, integrated, and interoperable emergency response communications function and capability.

- **Include Critical Elements in the *National Emergency Communications Strategy (NECS)* and the *National Emergency Communications Plan (NECP).*** Incorporate the following critical elements in the development, maintenance, and execution of the *NECS* and associated implementation guidance, and direct the DHS and other responsible Federal agencies to incorporate the elements into the *NECP:*

  - Large-Scale State and Regional Shared Public Safety Networks and Federal Grants;

  - Yearly Benchmarks for Achieving Defined Interoperability Objectives;

  - Nationwide Outreach to Support Emergency Response Communications;

  - Consolidation of Operations Centers to Increase Coordination and Situational Awareness; and

  - Identification of Specific Private-Sector Emergency Communications and Interoperability Support Roles.

- **Address Emergency Communications in the Converged Environment.** To encourage responsive emergency communications capabilities in the converged environment, establish and incorporate the following capability objectives into the *NECS* and associated implementation guidance, and also direct the DHS to incorporate the capability objectives into the *NECP:*

  - Support for a Significantly Expanded User Base;

  - Full Leveraging of Network Assets;

- Internet Protocol based Interoperability;
- Assured Access for Key Users through Priority Schemes or Dedicated Spectrum;
- National Scope with Common Procedures and Interoperable Technologies;
- Deployable Elements to Supplement and Bolster Operability and Interoperability;
- Resilient and Disruption-Tolerant Communications Networks;
- Network-Centric Principles Benefiting Emergency Communications; and
- Enhanced Communications Features.

The ECITF is also in the process of preparing and refining long-term recommendations to the President that streamline the information provided in the first report, using key policy issues and relevant topics such as NSTAC policy initiatives to focus the content. Comments from the Executive Office of the President (EOP) have been used to frame the current work strategy, and in discussions with EOP sponsors, specific NSTAC assistance was solicited in evaluating how IP-enabled capabilities and technologies might play a role in enhancing the interoperability concerns related to emergency communications. In response to this EOP request, current work is focusing on IP interoperability technology solutions, and discussions with Government stakeholders have been initiated to gain cross-agency perspectives on the issue. Issues such as the NSTAC perspective on national security and emergency preparedness industry requirements for the IP Multimedia Subsystem core, as well as IP-based interoperability approaches, are guiding the effort to produce a salient follow-on report, expected for completion at the end of the summer of 2007.

Actions Resulting from NSTAC Recommendations

As a result of the devastation caused during the 2005 hurricane season and informed by the NSTAC's associated recommendations, the DHS through the NCS has undertaken several actions to ensure successful emergency communications for future emergencies. The activities include the establishment of protocols for contacting and communicating with State and local officials, which is also intended to assist in the identification of emergency management and coordinators' contact information; coordination of the creation of a deployable communications package to provide reliable communications to emergency responders at all levels of Government in a disaster-inflicted region; integration of NCS priority services programs, and other relevant recommendations, into the *Interim National Emergency Communications Strategy* mandated by the White House's *The Federal Response to Hurricane Katrina: Lessons Learned* report; and the development of an emergency communications asset tracking database to aggregate information on those public and private tools to be leveraged during disaster recovery operations. The NCS also drafted an ESF #2 Operations Plan, which addresses deployable communications capabilities in support of incident response, specifically deployment of ESF #2 assets and capabilities to designated mobilizations centers and staging areas.

In addition, the NCS has taken concrete steps to address the priority services needs highlighted by hurricanes Katrina, Rita, and Wilma. Specifically, the NCS increased its outreach efforts to expand the effectiveness of the WPS and GETS programs. In addition, the NCS expanded the coverage and capabilities of WPS and advanced TSP, GETS, and WPS user knowledge through education and outreach efforts. Furthermore, the NCS has initiated an examination of methods to ensure the effective evolution of priority service capabilities in the converged environment through an exploratory process that includes: (1) architecture development; (2) modeling and analysis; (3) prototyping; and (4) industry requirements.

In addition, under the newly formed Office of Cyber Security and Communications, led by Mr. Greg Garcia, is the Office of Emergency Communications (OEC), which is a new organizational element designed to support the communications abilities of emergency responders and Government officials in the event of

natural disasters, acts of terrorism, or other man made disasters, and to ensure, accelerate, and attain interoperable emergency communications nation-wide. The OEC will expedite the establishment of a nationwide interoperable emergency communications framework and will serve as the focal point for these efforts within DHS. Specifically, the OEC will focus on ensuring the development of a clear vision for interoperability at the Federal, State, and local level. Furthermore, the OEC will look beyond technology issues associated with interoperability and will consider governance and organizational solutions.

Emergency Communications and Interoperability Task Force Membership

AT&T, Incorporated
Mr. Jim Bugel, Co-Chair

Motorola, Incorporated
Mr. Michael Alagna, Co-Chair

Bank of America Corporation
Mr. Roger Callahan

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Ray Lehr

CTIA – The Wireless Association
Mr. Rick Kemper

Lockheed Martin Corporation
Dr. Allen Dayton

Lucent Technologies, Incorporated
Mr. Bernie Malone

Microsoft Corporation
Mr. Paul Nicholas

Nortel
Dr. Jack Edwards

Northrop Grumman Corporation
Mr. Peter Hadinger

Qwest Communications International, Incorporated
Mr. Thomas Snee

Raytheon Company
Mr. Frank Newell

Rockwell Collins, Incorporated
Mr. Ken Kato

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Nextel Corporation
Mr. John Stogoski

Telcordia Technologies, Incorporated
Ms. Louise Tucker

VeriSign, Incorporated
Mr. Michael Aisenberg

Verizon Communications, Incorporated
Mr. James Bean

Other Emergency Communications and Interoperability Task Force Industry Participants

AT&T, Incorporated
Mr. Kent Bowen
Mr. Thomas Hughes
Ms. Rosemary Leffler
Mr. Harry Underhill

Intelsat, Ltd.
Ms. Sallye Clark

Nortel
Mr. Michael Stolker

Sprint Nextel Corporation
Mr. Lee Fitzsimmons
Ms. Allison Growney

Telecommunications Industry Association
Mr. Daniel Bart

George Washington University
Dr. Jack Oslund

International Communications

Investigation Group / *Period of Activity*

Network Group
April 1997 – September 1999

Convergence Task Force
June 2000 – June 2001

Network Security Vulnerability Assessments Task Force
June 2001 – March 2002

Next Generation Networks Task Force
May 2004 – May 2006

International Task Force
May 2006 – present

Issue Background

For many years, global communications networks have functioned in a period of transition as customer demands and business imperatives catalyzed the convergence of traditional circuit switched networks with broadband packet-based Internet Protocol (IP) networks to create the telecommunications industry's NGN. Although the complete evolution to the NGN is expected to take many years, this evolving network infrastructure, which includes wireless, wireline, and IP technologies, will alter the way governments and private industry meet their NS/EP communications needs. In fact, the emergence of the NGN has already effected change in a profound way. Many network service providers have developed the capability to carry voice, video, text, and data transparently to numerous categories of end-user devices, a key characteristic of the NGN. Mobile phones able to access an array of Web-based services represent only one example of this enhanced ability.

The scale, scope, and character of the NGN will fundamentally change the way governments and service providers plan for, prioritize, and ultimately deliver NS/EP communications. NGN networks, which are largely packet-switched networks, differ greatly from legacy circuit-switched networks. For example, packet-switched environments place control capabilities at the network "edge" and rely heavily on intelligent devices to execute key functions. In this new environment, NS/EP and critical business communications will be subject to an increased number of cyber threats based on inherent vulnerabilities and interdependencies known or expected to exist in the NGN. With these changes, network operators, infrastructure custodians, and NS/EP users must determine how best to meet NS/EP user requirements on the NGN.

The transition to the NGN also presents challenges for ensuring the security and availability of NS/EP communications. In addition to the vulnerabilities that arise due to the packet-switched nature of the NGN, some vulnerabilities that already existed in legacy networks will persist or worsen in the NGN. For example, the enhanced interconnectedness of the NGN can be exploited by hackers to provide rapid and far-reaching propagation of malicious payload (attacks). Another vulnerability is the emulation of network control messages. Unlike legacy networks, which used separate paths to divide network control messages from normal network payload, NGN architectures have network control messages co-existing with normal payload traffic, providing more open access to hackers to interfere with these messages. These and other vulnerabilities create complex risk scenarios for NS/EP communications in an NGN environment, which also depends on other infrastructures such as the electric power industry. A further challenge is the global nature of the NGN and, thus, methods for managing incidents of national significance may require international cooperation. To ensure NS/EP functions remain a priority in the transition to the NGN, these concerns must be addressed.

At the same time, the NGN will offer significant improvements for the delivery of NS/EP communications capabilities as bandwidth and software continue to improve. New communications capabilities, including greater access to data and new services, will better support NS/EP functions in critical ways, enabling first responders, for example, to obtain real-time access to voice, data, and video

necessary for the most effective completion of their jobs. The NGN will also naturally increase network robustness and resiliency by the nature of its mesh architecture, offering many possible paths for service and redundancy of equipment and servers. To achieve the benefits of such new capabilities and greater resiliency, and to speed and enhance the transition to NGN, solutions must be found that address NS/EP functional requirements, especially for security and availability. Doing so requires forward-looking action by industry and Government.

The NGN is interconnected with worldwide networks, which are themselves developing into a global, seamless infrastructure, to deliver communications services across national borders. This global interconnectivity brings with it inherent risks, as information passes over parts of the network that are more diverse in security, architecture, and management, particularly in some foreign network segments and infrastructures. These foreign network entities may be more vulnerable to intrusion, deliberate disruption, or accidental damage. The U.S. communications infrastructure is now dispersed across numerous companies and organizations and spans the telecommunications and information technology (IT) industries.

With the emergence of this converged global network, additional operational security concerns related to access and remediation during system disruptions have emerged affecting the delivery of NS/EP communications. This convergence has prompted governments and critical infrastructure private-sector owners to reevaluate how NS/EP communications needs are being met today and in the future.

History of NSTAC Actions and Recommendations

The NSTAC has an extensive history of examining the NS/EP implications of the transition of the Nation's telecommunications networks to the NGN environment and providing the President with forward looking and innovative recommendations. In its *Internet Report: Examination of the National Security and Emergency Preparedness Implications of Internet Technologies Report,* published in June 1999, the NSTAC examined three key transition factors—the extent to which NS/EP operations depend on the Internet, the network control element vulnerabilities associated with the Internet and their ability to cause a severe disruption of Internet service, and how Internet reliability, availability, and service priority issues applied to NS/EP operations. In its June 2001 *Convergence Task Force Report,* the NSTAC furthered its network transition-related work to specifically analyze the potential security and reliability vulnerabilities associated with converged networks. Its *Network Security Vulnerability Assessments Task Force Report,* released in March 2002, addressed public network policy and technical issues related to network disruptions, the security and vulnerability of the converged network control space, and needed countermeasures to mitigate against these vulnerabilities. Issues presented by convergence also arose during the Committee's examination of the resiliency of networks supporting the financial services sector to physical disruptions.

In 2005 and 2006, the NSTAC looked at five fundamental areas of examination: (1) NGN description; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. The Committee offered recommendations to the President in March 2005 on issues that could be addressed quickly to improve NS/EP communications, and in March 2006 made its final recommendations in the areas of identity management; coordination on common operational criteria for NGN NS/EP end-to-end services; research and development; technology lifecycle assurance and trusted technology; resilient alternate communications; agreements, standards, policy, and regulations; incident management on the NGN; international policy; and first responders.

Building on prior work, at the NSTAC XXIX Meeting in May 2006, the Committee requested an in-depth examination of the NS/EP implications of international communications. The NSTAC's prior body of work, as well as the analyses in this inquiry, suggested that NS/EP communications requirements can be achieved only if industry and Government infrastructure stewards collaborate to develop

policies and best practices responsive to the international communications environment. Based on this investigation, the NSTAC plans to issue its *Report to the President on International Communications* during cycle XXXI. For further detail on the efforts of the NSTAC related to the NGN, please see the Network Convergence section in the Previously Addressed section of this *NSTAC Issue Review.*

On September 21-22, 2006, the President's NSTAC sponsored its first international Research and Development (R&D) Exchange (RDX) Workshop in Ottawa, Ontario, Canada. The purpose was to exchange ideas among representatives from industry, Government, and academia regarding international collaboration on cyber security R&D. During the two-day event, participants engaged in a facilitated dialogue including both plenary and breakout sessions. From these sessions, six overarching issue areas and corresponding agendas for action regarding international collaboration for cyber security R&D emerged:

- **Technologies and mechanisms to enable trust and build communities of interest are needed.** Enhanced security on the global communications network is dependent on an ability to interpret the trustworthiness of infrastructure, users, and devices. Several factors, such as human error, the need for commercial efficiencies, effective security policies and procedures, and personnel security and background checks, influence how trust is embedded in systems. The current network environment lacks universal applications and exercised processes and practices that allow parties to establish a high degree of confidence in the legitimacy and reliability of their counterparts, thereby stifling the development of functional communities of interest. Confidence and trust are jeopardized by a host of threats (*e.g.,* exploitation by insiders, physical destruction). To enable inter-domain trust, users and devices must be able to develop, transfer, and accept identities and credentials through systems and solutions that provide for cross-recognition.

- **International collaboration is essential for successful cyber security R&D initiatives.** Current collaboration is limited and localized. R&D partnerships need to be created to promote cooperation and interoperation across borders, infrastructures, sectors, and domains. To effectively address the compelling network security risks that threaten economic sustainability, national security, and public safety, information sharing forums and mechanisms are imperative for exchanging information and conducting collaborative R&D activities are imperative. Legislative and regulatory barriers need to be amended and incentives need to be created to facilitate appropriate levels of information sharing and international cooperation.

- **To advance cyber security research, leaders and practitioners must make investment decisions based on cost benefit analyses.** Recent innovations and advancements in networked information systems have brought about dynamic change, driven primarily by commercial forces. However, the security paradigm has not shifted to accommodate this evolving environment, thereby thwarting long-term progress. Future cyber security R&D proposals must address the cost of collaboration, articulate the value proposition, and include relevant business cases. To accomplish a posture of improved security and trustworthiness, strategies should be devised to leverage industry investments while accommodating market drivers; balance directives and incentives to stimulate progress; and blend influence and action to develop the next generation of security tools and products.

- **To maintain to the current security posture and improve future preparedness and response, NS/EP requirements must be embedded in new technologies and methodologies.** The rapid pace of technological advancement demands increased focused on the importance of ensuring the resiliency, reliability, and security of critical communications. Additional research on NS/EP scenarios and requirements is needed, as well as further development of existing systems and technologies that may have NS/EP applications. Future cyber security R&D must also consider how potential

market decisions and economic impacts affect the security of free nations. New tools and services must incorporate NS/EP requirements during the pre-R&D stages and must continue to consider NS/EP implications through technology deployment and commercial adaptation.

- **Dynamic leadership and common frameworks are critical to achieve real progress in cyber security R&D.** General agreement on the set of "grand challenges" is needed to achieve larger goals and to encourage cross-border and cross-sector partnerships. Such vision serves to encourage collaboration, justify expenditures, and build global communities of interest around cyber security R&D. In addition, a common taxonomy enables different parties to clearly define priorities. While multinational standards efforts facilitate the development of common frameworks, cross-sector agreement on a roadmap for future R&D expenditures is also vital.

- **Strengthened education, awareness, and training programs increase the effectiveness of R&D partnerships and programs.** By improving knowledge sharing, members of the research community will be able to leverage best practices and related initiatives to enhance the effectiveness of current and future R&D investments. The critical challenge is to develop an R&D strategy that engages industry, Government, and academia, as well as end-users in exchanging information about existing initiatives and successes, thereby ensuring consideration of the full range of critical issues and facilitating the development of comprehensive, holistic solutions collectively. In order to inform the development of requirements and priorities, it is necessary to maintain an inventory of ongoing activities and to create linkages between centers of excellence across the world.

Reports Issued

Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies, June 1999.

Convergence Task Force Report, June 2001.

Network Security Vulnerability Assessments Task Force Report, March 2002.

Next Generation Networks Task Force Report: Near Term Recommendations, March 2005.

Next Generation Networks Task Force Report, March 2006.

International Task Force Membership

VeriSign, Incorporated
Mr. Michael Aisenberg, Esq., Chair

Science Applications International Corporation
Dr. Marvin Langston, Co-Vice Chair

AT&T, Incorporated
Ms. Rosemary Leffler, Co-Vice Chair

Bank of America Corporation
Mr. Roger Callahan

Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Qwest Communications International, Incorporated
Mr. Kushal Jain

Sprint Nextel Corporation
Mr. John Stogoski

Telcordia Technologies, Incorporated
Ms. Louise Tucker, Esq.

Unisys Corporation
Mr. Shawn Anderson

Verizon Communications, Incorporated
Mr. James Bean

Microsoft Corporation
Mr. Phil Reitinger, Esq.

BellSouth Corporation
Mr. David Barron

Raytheon Company
Mr. Frank Newell

Juniper Networks, Incorporated
Mr. Robert Dix

Other International Task Force Industry Participants

British Embassy to the United States
Dr. Phil Budden

Centre for the Protection of National Infrastructure
Ms. Judy Baker

Centre for the Protection of National Infrastructure
Mr. Mike Corcoran

Edison Electric Institute
Mr. Larry Brown, Esq.

George Washington University
Dr. Jack Oslund

Independent Electricity System Operator Canada
Mr. Stuart Brindley

Industry Canada
Ms. Maggie Lackey
Mr. Robert Leafloor

Microsoft Corporation
Mr. Paul Nicholas

Nortel
Dr. Jack Edwards

Qwest Communications International, Incorporated
Ms. Katherine Condello

Science Applications International Corporation
Mr. Hank Kluepfel

Sprint Nextel Corporation
Ms. Allison Growney

Symantec Corporation
Mr. Wesley Higaki

Telcordia Technologies, Incorporated
Mr. Bob Lesnewich

VeriSign, Incorporated
Mr. Anthony Rutkowski, Esq.

International Task Force Government Participants

Central Intelligence Agency
Mr. Tom Donahue

Department of Homeland Security
Ms. Kathy Blasco
Mr. Kelvin Coleman
Mr. David Delaney
Ms. Liesyl Franz
Mr. Charles Lancaster
Mr. Thad Odderstol
Mr. Andrew Purdy, Esq.
Ms. Jordana Siegel
Ms. Christina Watson
Mr. Will Williams

Department of Commerce
Mr. Dan Hurley

Department of Defense
Mr. Thomas Dickinson
Mr. Mark Hall
Mr. Andrew Kimble

Department of State
Mr. David Chinn
Ms. Michelle Markoff

Federal Communications Commission
Mr. Richard Hovey

Federal Reserve Board
Mr. Chuck Madine

Global Infrastructure Resiliency

Investigation Group / *Period of Activity*

Global Infrastructure Resiliency Working Group
August 2006 – October 2006

Issue Background

The increasing dependence on and the vulnerability of the global communications infrastructure highlights the importance of establishing mitigation measures for critical services and protection measures to ensure critical national security and emergency preparedness telecommunications functions in the event of a catastrophic disruption to the global communications infrastructure.

History of NSTAC Actions and Recommendations

Due to these concerns, the President's NSTAC formed the Global Infrastructure Resiliency Working Group (GIRWG) in response to a request from the National Security Council to develop operational recommendations to improve the overall resiliency of the global communications infrastructure. The group developed a sensitive report designated For Official Use Only.

Reports Issued

NSTAC Report on Global Infrastructure Resiliency, October 2006.

Global Infrastructure Resiliency Membership

CTIA – The Wireless Association
Mr. Bob Bolster
Mr. Christopher Guttman-McCabe

Cingular Wireless LLC
Mr. Kent Bowen
Mr. James Bugel

Verizon Wireless
Ms. Alison Brontmen
Mr. Mike Hickey

Sprint Nextel Corporation
Ms. Alison Growney

Microsoft Corporation
Mr. Phil Reitinger

Motorola, Incorporated
Mr. Mike Alagna

NCS Multi-Disciplinary Working Group

Influenza Pandemic

Investigation Group / *Period of Activity*

Pandemic Study Group
July 2006 – January 2007

Issue Background

An influenza pandemic has the potential to present an array of threats to the integrity of the Nation's communications system. Widespread contagion could incapacitate vital service workers and quarantine requirements could generate network overloads as a result of mass telecommuting. Therefore, contingency planning is key to the survivability of necessary national security and emergency preparedness NS/EP services.

History of NSTAC Actions and Recommendations

At the request of the National Infrastructure Advisory Council (NIAC), and in response to a joint Department of Homeland Security and Department of Health and Human Services appeal for assistance, the NSTAC worked in partnership with the council to develop guidance for the Government on critical services that must be maintained across the Nation's infrastructures in the event of a pandemic. Consequently, the NSTAC undertook the responsibility to formulate prioritization recommendations for the telecommunications infrastructure so that NS/EP services that rely heavily on the sector can remain stable and usable under any circumstances.

Reports Issued

The Prioritization of Critical Infrastructure for a Pandemic Outbreak in the Untied States Working Group (NIAC Report), January 2007.

Pandemic Study Membership

BellSouth Corporation
Mr. David Barron

Verizon Wireless
Mr. Mike Hickey

Standing Issues

Legislation and Regulation

Investigation Group / *Period of Activity*

Funding and Regulatory Working Group
December 1982 – December 1994

Legislative and Regulatory Group
December 1994 – September 1999

Legislative and Regulatory Working Group
September 1999 – February 2001

Legislative and Regulatory Task Force
February 2001 – Present

Issue Background

Laws and regulations govern the relationship between the Government and the public and provide the framework under which public and private entities conduct business. Within the evolving telecommunications environment, it is essential that legislation and regulation keep pace with technological changes to ensure continued fulfillment of national security and emergency preparedness (NS/EP) requirements. It is within this context that the President's National Security and Telecommunications Advisory Committee (NSTAC) reviews legal and regulatory activities that could impact NS/EP services, operations, and communications and considers areas for which there is a need for further legislative and regulatory action.

History of NSTAC Actions and Recommendations

The investigation of legislative and regulatory issues of consequence to NS/EP communications comprise a key focus for the NSTAC. Over the course of its existence, the committee has examined the implications of numerous important topics including:

- Telecommunications Act of 1996 (Telecom Act);
- Widespread Telecommunications Outages;
- National Services Planning Process;
- Assessment of Federal Critical Infrastructure Recommendations;
- Information Sharing;
- Transition to the Year 2000;
- Wireless Communications;
- Convergence;
- Foreign Ownership;
- Cyber Crime;
- Potential Policy Conflicts with Homeland Security and NS/EP Missions;
- Open Source Information;
- Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act;
- Defense Production Act (DPA);
- Legislative Concerns Associated with the 2005 Hurricane Season;
- Telecommunications Circuit Route Diversity Policy;
- Protected Critical Infrastructure Information; and
- DHS Organization.

A description of the NSTAC's activities in each of these areas, as well as the evolution of the task force follows.

Task Force Evolution

At its inaugural meeting in December 1982, the NSTAC established the Funding and Regulatory Working Group (FRWG) to examine funding alternatives and regulatory issues for candidate enhancements to NS/EP telecommunications. The FRWG remained active to address additional issues of a legislative and regulatory nature until 1994 when the committee decided to stand down the group until further issues arose requiring consideration. The

NSTAC later amended the name of the FRWG to the Legislative and Regulatory Group (LRG) that same year per the guidance outlined in the December 1994 *Industry Executive Subcommittee Guidelines;* however, it did not re-activate the LRG again until January 1997 following the passage of the landmark *Telecommunications Act of 1996.* Between 1997 and 2001, the LRG was renamed the LRWG and was tasked to serve as an ad hoc group to investigate issues and also serve as a supplementary body to NSTAC task forces. In February 2001, the committee again amended the task force's name to the Legislative and Regulatory Task Force (LRTF) and formally established it as a standing body of the NSTAC.

Telecommunications Act of 1996

As the first major overhaul of telecommunications policy since 1934, the Telecom Act redefined competition and regulation in virtually every sector of the communications industry. In response to passage of the Telecom Act and the resultant evolving telecommunications environment, the NSTAC charged the LRG to examine legislative, regulatory, and judicial actions that potentially impact NS/EP telecommunications, placing particular emphasis on monitoring implementation of the Act. In addressing this charge, the LRG established a framework for analysis, and in January 1997, began working closely with industry and Government to develop a common understanding of the NS/EP implications of the new law.

Based on the analysis conducted by the task force, the NSTAC found that the Telecom Act did not alter carrier responsibilities for the provision of NS/EP services. However, the committee determined that continued change in the regulatory and industry structure warranted increased educational outreach efforts for new entrants and existing carriers with regard to their mandatory and voluntary obligations.

Widespread Telecommunications Outages

At NSTAC XIX in March 1997, the Assistant to the President for Science and Technology asked the NSTAC to investigate the possibility of a widespread telecommunications outage. Subsequently, the LRG analyzed the legal and regulatory obstacles that would hinder service restoration during widespread, major service outages. As a result, the NSTAC presented its related findings in its December 1997 report discussed during NSTAC XX. The NSTAC found the most significant legal and regulatory obstacle to be the apparent uncertainty about who could expeditiously address carriers' concerns regarding their compliance with relevant laws or regulations during emergency situations.

To further address this finding, the NSTAC charged the LRG to examine options for enhancing communication on NS/EP matters among industry, the Federal Communications Commission (FCC), and other relevant Government organizations. To that end, the LRG investigated the role of the FCC Defense Commissioner; investigated the need for an NS/EP industry advisory body to the FCC on these issues; documented the intergovernmental relationships between the FCC, the National Communications System, and the Office of Science and Technology Policy with regard to NS/EP responsibilities; and worked jointly with the NSTAC's Network Group's Widespread Outage Subgroup to draft procedural guidelines to help telecommunications carriers resolve issues with the FCC when critical emergency telecommunications services needed to be restored in a timely manner.

National Services Planning Process

In July 1997, the Network Reliability and Interoperability Council (NRIC) provided the FCC with a series of recommendations aimed at improving the planning process for National Services and deployable telecommunications services intended or required on a national or regional basis. The NSTAC agreed that a National Services planning process, as conceived by the NRIC, could serve as an effective means for promoting NS/EP telecommunications requirements. Consequently, the Committee tasked the LRG to assess what actions the NSTAC should take to ensure that industry and Government consider NS/EP requirements during the National Services planning process. During discussion at NSTAC XX, the Committee reviewed the task force's findings and recommended that the

Industry Executive Subcommittee (IES) continue to assess the development of the NRIC's National Services recommendations.

Following NSTAC XX, the LRG established the National Services Subgroup to study the feasibility of defining NS/EP telecommunications functions as National Services. The subgroup submitted its *National Services Subgroup White Paper* to NSTAC XXI in September 1998 geared to facilitating public awareness of selected NS/EP-critical telecommunications functions and capabilities. The white paper also promoted the continued consideration of NS/EP telecommunications service objectives by industry and Government during the future deployment of NS/EP National Services.

Assessment of Federal Critical Infrastructure Recommendations

In October 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) released its final report and recommendations on protecting the Nation's critical infrastructures, including the telecommunications infrastructure. Following NSTAC XX, the NSTAC charged the LRG to review the potential legislative and regulatory implications for NS/EP telecommunications as a result of the PCCIP's recommendations. To address its charge, the LRG conducted a preliminary analysis of Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection,* which the President issued on May 22, 1998, to support the PCCIP recommendations and to establish a national policy to eliminate vulnerabilities in the Nation's critical infrastructures. Based on the LRG's findings, the Committee requested that the IES undertake a more detailed assessment of the planned implementation of PDD-63 and report back to it regularly on progress made.

Information Sharing

Following NSTAC XXI, and in response to information sharing policy outlined in PDD-63, the NSTAC tasked the LRG to identify and assess the legal and regulatory obstacles to sharing outage and intrusion information. To that end, the LRG determined that identification and discussion of existing and proposed NS/EP-related outage and intrusion information sharing mechanisms could provide additional insights to assist the group in assessing critical information sharing issues, particularly those associated with the implementation of PDD-63. As a result, and to better understand the information sharing environment and the entities involved in the process, the NSTAC developed its *Telecommunications Outage and Intrusion Information Sharing Report* which outlined the entities with whom telecommunications companies shared outage and intrusion information and reviewed potential legal barriers that could ultimately inhibit the information sharing process.

During NSTAC XXIII, the NSTAC, through its LRWG, again examined information sharing issues, this time focusing on the impediments to information exchange, especially critical infrastructure information sharing. As a result, the LRWG undertook an in-depth analysis of *The Freedom of Information Act* (FOIA), examining FOIA's potential to hinder industry information sharing with the Government. FOIA permits the public to request and gain access to records that Government departments and agencies maintain, the disclosure of which could deter industry from sharing further information with the Government. Although there are a number of exemptions to FOIA's requirements for disclosure of information, none of the exemptions clearly covers information pertaining to critical infrastructure protection. The LRWG met several times with Department of Justice (DOJ) officials to exchange views on perceived problems including liability and antitrust concerns and potential legal solutions. As a result of the LRWG's deliberations, the NSTAC agreed with DOJ representatives on the need for a nondisclosure provision to protect "security-related" information voluntarily shared with the Government. The LRWG shared its analysis with the NSTAC's Information Sharing-Critical Infrastructure Protection Task Force, which addressed both the technical and legal and regulatory FOIA issues in its May 2000 *Information Sharing-Critical Infrastructure Protection Task Force Report.*

NSTAC furthered its information sharing work during the NSTAC XXIV and XXV cycles. During this time, the committee requested the LRTF to examine pending FOIA legislation from the 106th and 107th Congresses and to work with Congressional staff to

determine the status and outlook of the legislation. In response to the analysis conducted by the LRTF, the NSTAC delivered a letter to President Bill Clinton on August 7, 2000, requesting his support on legislation that would protect CIP information voluntarily shared with the Government from disclosure under FOIA and limit liability. Following the NSTAC XXIV Meeting in June 2001, the NSTAC acknowledged the continued importance of the topic and resubmitted the letter to President George W. Bush asking him to support such legislation. On September 26, 2001, President Bush replied that he supported a narrowly drafted exception to FOIA to protect information about corporations' and other organizations' vulnerabilities to information warfare and malicious hacking. In a December 17, 2001, letter to the President, the NSTAC encouraged the President to continue to support information sharing legislation.

The LRTF continued to examine information sharing in the NSTAC XXVI and NSTAC XXVII cycles as well. During these cycles, Congress passed the *Critical Infrastructure Information (CII) Act,* which provided additional FOIA and liability protections for companies that voluntarily share critical infrastructure information with the Department of Homeland Security (DHS). Following enactment of the CII Act, the NSTAC requested the LRTF to assess whether additional information sharing barriers remained and to examine other legal and nonlegal barriers for the purposes of homeland security. As a result of the LRTF's analysis, the NSTAC drafted its *Barriers to Information Sharing Report,* in which it made a series of recommendations for improving the exchange of CII between industry and the Government and for protecting voluntary CII that critical infrastructure owners and operators provide to the Government.

The *CII Act* called for the creation of a critical infrastructure protection program within DHS that would protect CII provided to the Department from public disclosure under the *Freedom of Information Act* and other mechanisms. On April 15, 2003, DHS published a Notice of Proposed Rulemaking (NPRM) in the Federal Register on *Procedures for Handling CII.* Given the implications for information sharing between the public and private sectors, the LRTF began evaluating the NPRM and the program it proposed. DHS issued its final rule on *Procedures for Handling CII* on September 1, 2006, establishing the Protected CII (PCII) Program Office. LRTF members noted many laudable provisions but remained concerned that the final rule was not sufficiently specific on whether information provided the DHS under contract would receive PCII protections. The task force requested the PCII Program Office provide clarification on this point.

The Year 2000 Readiness and Disclosure Act

In 1998, with the nearing arrival of the new century, the NSTAC tasked the LRG to examine relevant communications-related Y2K issues, particularly the success of the *Year 2000 Readiness and Disclosure Act* (Y2K Act) in urging greater information sharing within industry. In response, the LRG sent a letter to the NSTAC's IES representatives seeking their companies' comments on the Y2K Act and any additional legislative or regulatory actions that could facilitate Y2K-related information sharing and remediation. Per request by the President's Council on Y2K Conversion, the NSTAC forwarded a summary of the Committee's findings in February 1999.

Wireless Communications

During NSTAC XXII, the NSTAC charged the LRG to identify the barriers to the issuance of wireless telecommunications priority access rules by the FCC and to evaluate NSTAC's level of continued support of the Cellular Priority Access Services (CPAS), (now referred to as the Wireless Priority Service). During the course of the LRG's examination, the group learned that the NCS planned to implement a new approach for providing wireless priority access based on channel reservation, causing the NSTAC to conclude its study.

However, during NSTAC XXVI, the LRTF again engaged in wireless communications issues when the Wireless Task Force requested assistance from the LRTF in assessing the legal and regulatory aspects of the FCC Report & Order (R&O) on Priority Access Service (PAS). The LRTF reviewed the R&O and, after carefully considering the merits of reopening the PAS rulemaking, the task force concluded that revisiting the rules would be a lengthy process and could

unintentionally slow the deployment of Wireless Priority Service (WPS). As a result of this conclusion, the NSTAC sent a letter to the President offering recommendations on how to facilitate the widespread deployment of wireless PAS. In the letter, the NSTAC commended the FCC for adopting a Second R&O for PAS, which indicates that carriers providing PAS shall have liability immunity from Section 202 of the *Communications Act of 1934.* The letter also stated that the FCC and the National Telecommunications and Information Administration should accelerate ongoing efforts to improve interoperability among Federal, State, and local public safety communications agencies. The letter further encouraged the Administration to support full and adequate Federal funding for wireless PAS.

Convergence

During NSTAC XXII, the LRG reviewed convergence issues in light of legislative, regulatory, and judicial actions that might affect existing and future public networks and potentially impact NS/EP telecommunications. The LRG's preliminary analysis of convergence revealed no significant implications for NS/EP telecommunications.

During the NSTAC XXV cycle, the NSTAC tasked the LRTF to undertake a further analysis of convergence issues, examining whether the current legal and regulatory environment was adequate to ensure NS/EP services in the converged and NGN environment. To accomplish its tasking, the LRTF coordinated with participants in the Government's Convergence Task Force to discuss the status of the Government's work in the area of network convergence and the assurance of NS/EP communications services.

The LRTF concluded that until the standards for packet-based services were established and the Government's requirements in the evolving environment were certain, new legislation or regulation was premature. The task force also stated that the legal issues underlying the provisioning of NS/EP priority services to the Federal Government in an NGN environment were extremely complex and might require further study. Based on the convergence analysis conducted by the LRTF and the Network Security Vulnerability Assessments Task Force, the NSTAC issued its *Network Security Vulnerability Assessments Task Force Report* in March 2002.

Foreign Ownership

During NSTAC XXIII, the NSTAC engaged the LRWG to conduct an examination of foreign ownership regulations and their possible impact on NS/EP communications. The task force examined domestic regulatory history and analyzed several mergers and acquisitions between domestic and foreign telecommunications carriers, ultimately finding that the current regulatory structure satisfied the different interests of the industry and Government parties involved. The LRWG concluded that it was unclear whether further statutory or regulatory changes would effectively enhance the role of national security issues in foreign ownership situations at that time. The LRWG documented its findings in a working group paper and shared its analysis with the NSTAC's Globalization Task Force (GTF). Based on the analysis conducted by the LRWG and the GTF, the NSTAC issued its *Globalization Task Force Report* in May 2000.

Cyber Crime

At the request of the NSTAC during cycle XXVI, the LRTF examined existing legal penalties for committing Internet attacks to determine whether those penalties should be strengthened or whether additional penalties were needed. In its *Penalties for Internet Attacks and Cyber Crime Report,* the NSTAC concluded sufficient legal authority exists to penalize and deter those who commit cyber crimes. The NSTAC also made additional recommendations for pursuing a well-rounded and proactive approach to combating cyber crime.

Potential Policy Conflicts with Homeland Security and NS/EP Missions

During the NSTAC XXVII cycle, and in response to an NSTAC request, the LRTF reviewed the policy landscape for national policies and regulations that could potentially conflict with homeland security and NS/EP missions. More specifically, the LRTF examined telecommunications policy conflicts related to fuel storage, water sector infrastructure, critical facilities markings, jurisdictional conflicts, and

common underground facilities. The task force determined that policy conflicts existed due to the existence of overlapping and contradictory policies and regulations at the Federal, State, and local levels.

In response to the LRTF's analysis, the NSTAC sent a letter to President George W. Bush in October 2003 recommending that he ask the Homeland Security Council, the National Security Council, and Federal departments and executive agencies, including independent agencies, to undertake several activities. These activities included evaluating proposed policies and regulations to ensure that homeland security and NS/EP implications have been consolidated; completing a review of existing policies and regulations for potential cross-sector conflicts with homeland security and NS/EP priorities and working with DHS to promptly resolve any identified conflicts; and implementing a framework to resolve multijurisdictional (Federal, State, and local) conflicts and, if necessary, recommend an appropriate legislative resolution.

Open Source Information

In response to concerns that terrorists or other motivated adversaries could easily access sensitive information, such as the location of critical telecommunications facilities, on the Internet and use this information to plan an attack on the Nation's telecommunications infrastructure, the NSTAC tasked the LRTF to undertake an analysis of open source information. The LRTF completed its analysis during the NSTAC XXVIII cycle, and on April 8, 2005, the NSTAC sent a letter to President Bush recommending various activities including the development and adoption of Web publishing and access guidelines by the Federal Government incorporating provisions that protect industry-sensitive critical infrastructure information provided to the Government and the promulgation of web publishing and access guidelines for dealing with sensitive but unclassified critical infrastructure information.

The LRTF's work on open source information continued during the NSTAC XXIX Cycle, when the NSTAC, during the March 10, 2005, Principals' Conference Call, requested that the LRTF address the concern of open source information on academic web sites and report back to them about the advisability of scoping this issue. After conducting its analysis, the LRTF reported back to the Principals that the issue did not require further scoping.

SAFETY Act

During the NSTAC XXVIII Cycle, the LRTF initiated an examination of the NS/EP telecommunications implications of the implementation of the SAFETY Act at the request of the Committee. The LRTF continued to monitor the implementation of the SAFETY Act in the NSTAC XXIX Cycle, reporting to the NSTAC periodically on the status of the efforts.

Defense Production Act

During NSTAC XXVIII, the NSTAC commissioned the LRTF to begin an examination of the NS/EP implications of the DPA and the proposed amendments to the Act and to Executive Order (E.O.) 12919, *National Defense Industrial Resources Preparedness.* During the NSTAC XXIX cycle, the task force agreed to continue to monitor potential amendments to the DPA and to E.O. 12919 to ensure essential NS/EP needs are met in any revision to law.

Legislative Concerns Associated with the 2005 Hurricane Season

The 2005 hurricane season defined many of the committee's legislative and regulatory priorities during the NSTAC XXIX Cycle. The Government's response to Hurricanes Katrina, Rita, and Wilma prompted the NSTAC to request assistance from the LRTF to review the legal and regulatory environment in which Federal response took place. The LRTF analysis revealed that several legislative mechanisms needed revision including the *Robert T. Stafford Disaster Relief and Emergency Assistance (Stafford) Act* which the committee felt did not adequately provide assistance to telecommunications infrastructure providers (TIPs) in disasters. The task force also determined that difficulties carriers faced in obtaining security, fuel, water, site access, and billeting for workers could be mitigated if the Federal Government created a designation for "Emergency Responders (Private Sector)" and included TIPs in that category. Accordingly, the NSTAC sent a letter to President

Bush advising him to act no later than June 1, 2006, to establish and codify the term "emergency responder (private sector)" to include TIPs and ensure they receive non-monetary assistance, including accessing restricted areas and obtaining fuel, water, power, billeting, and workforce and asset security, by:

- Directing DHS to modify the National Response Plan and its emergency support functions to designate TIPs as Emergency Responders (Private Sector) and to establish protocols and procedures for the way in which Federal, State, local, and tribal Governments should work with TIPs before, during, and after a national disaster;

- Issuing appropriate Presidential guidance to define Emergency Responders (Private Sector) under the Stafford Act and other authorities as appropriate to align with the broadened definition of national defense in the 2003 amendments to the DPA. Specifically, the guidance should make clear that key response personnel of critical telecommunications infrastructure owners and operators should be defined as Emergency Responders (Private Sector) and should receive non-monetary Federal assistance under the Stafford Act, and

- Directing the Secretary of Homeland Security to work with Congress to align the Stafford Act and other appropriate legislative authorities with the DPA by codifying the designation of private sector TIPs as Emergency Responders (Private Sector) and by codifying the official interpretation that for-profit TIPs should receive Federal assistance.

Telecommunications Circuit Route Diversity Policy

In April 2004, the NSTAC recommended the President direct appropriate departments and agencies to support the Alliance for Telecommunications Industry Solutions (ATIS) National Diversity Assurance Initiative (NDAI), which sought to examine diversity assurance and ways to ensure it is maintained over time as well as best practices for NS/EP) organizations. In its February 2006 final report on the NDAI, ATIS found that because circuit diversity assurance cannot be offered as a commercially viable product, the Government should revise existing Federal guidance on contingency planning and continuity of operations. The LRTF agreed with the ATIS findings and during the NSTAC XXX cycle evaluated methods for disseminating the NDAI recommendations to NS/EP stakeholders.

Actions Resulting from NSTAC Recommendations

In the *Barriers to Information Sharing Report,* the NSTAC advised the President that DHS should be the clearinghouse and dispenser of CII information and that CII Act protections should cover departments and agencies other than DHS. In a related action, on February 18, 2004, DHS launched the Protected Critical Infrastructure Information (PCII) Program, pursuant to the CII Act. The PCII Program Office (PO) is part of the DHS Infrastructure Partnerships Division and serves as the clearinghouse and dispenser of CII.

On October 28, 2003, in response to the NSTAC's *Letter to President George W. Bush on National Policies and Regulations that Conflict with Homeland Security and NS/EP Missions,* the Assistant to the President for Homeland Security confirmed that the staff of the Executive Office of the President had been tasked to convene a meeting with the other White House stakeholders to review the recommendations in the NSTAC's letter and to analyze their impact to NS/EP communications.

Furthermore, the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks released its *Report and Recommendations to the FCC* on June 12, 2006, which endorsed NSTAC's recommendation that telecommunications infrastructure providers be afforded emergency responder status under the Stafford Act. In July 2006, Secretary Chertoff confirmed to the NSTAC that DHS officials had been working closely with Congress to ensure that the Committee's emergency responder provisions would be sufficiently addressed in future legislation to be formally introduced by the Senate. In addition, the DHS announced it had developed, in partnership with Federal, State, and local Government entities, as well as a private sector company, an access standard operating procedure (SOP) to ensure that private

critical infrastructure responders have priority access to disaster areas. The access SOP had been adopted by the State of Georgia and has been distributed to a broader community, including the Homeland Security Advisors and the National Association of Regulatory Commissioners.

Furthermore, the Stafford Act has been amended. While the Stafford Act amendments have yet to be fully realized, they do provide provisions for the Emergency Responder concept in the context of what the Government terms an "Essential Service Provider" (ESP). ESPs include both telecommunications and electric power professionals. Additionally, the amendments to the Stafford Act detail access provisions to disaster recovery sites for ESPs. The NCS has worked to incorporate the ESP term into the NRP and to ensure that these providers receive appropriate support during a national crisis.

Reports Issued

Legislative and Regulatory Group Report, December 1997.

Legislative and Regulatory Group Report, September 1998.

Procedure for Problem Resolution with the Federal Communications Commission and the National Coordinating Center for Telecommunications During Emergency Telecommunications Disruptions, September 1998.

National Services Subgroup White Paper, September 1998.

Legislative and Regulatory Group Report, June 1999.

Telecommunications Outage and Intrusion Information Sharing Report, June 1999.

Letter to President Bill Clinton on Protection of Critical Infrastructure Information, August 7, 2000.

Letter to President George W. Bush on Protection of Critical Infrastructure Information, June 2001.

Penalties for Internet Attacks and Cyber Crime, April 2003.

Barriers to Information Sharing, September 2003.

Letter to President George W. Bush on National Policies and Regulations that Conflict with Homeland Security and NS/EP Missions, October 16, 2003.

Letter and Addendum to President George W. Bush on Open Source Critical Infrastructure Information, April 8, 2005.

Letter and Report to President George W. Bush on Federal Support to Telecommunications Infrastructure Providers During National Emergencies, Designation as Emergency Responders (Private Sector), January 31, 2006.

NSTAC 2006-2007 Legislative and Regulatory Task Force Membership

Telcordia Technologies, Incorporated
Ms. Louise Tucker, Chair

Sprint Nextel Corporation
Mr. Michael Fingerhut, Vice Chair

AT&T, Incorporated
Ms. Rosemary Leffler

Bank of America Corporation
Mr. Roger Callahan

Bell South, Incorporated
Mr. David Barron

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Microsoft Corporation
Ms. Cristin Flynn Goodwin
Mr. Mike Hickey

Nortel
Mr. Raymond Strassburger

Northrop Grumman Corporation
Mr. Bruce Walker

Qwest Communications International, Incorporated
Mr. Jeffrey Hackman

Rockwell Collins, Incorporated
Mr. Ken Kato

Sprint Nextel Corporation
Mr. John Stogoski

Unisys Corporation
Mr. Charlie Rowan

Verizon Communications, Incorporated
Mr. James Bean

Verizon Business
Mr. Dennis Guard

Other Legislative and Regulatory Task Force Industry Participants

AT&T, Incorporated
Mr. Peter Bulter
Mr. Harry Underhill

Bank of America Corporation
Mr. Timothy Nagle

Cingular Wireless LLC
Mr. Jim Bugel

Computer Sciences Corporation
Ms. Lucy Thompson

Edison Electric Institute
Mr. Laurence Brown

George Washington University
Dr. Jack Oslund

Intelsat, Ltd.
Ms. Sallye Clark
Ms. Khalilah Wright

Lucent Technologies, Incorporated
Ms. Selma Munden

Microsoft Corporation
Mr. Phil Reitinger

Motorola, Incorporated
Mr. John Lyons

Qwest Communications International, Incorporated
Ms. Katherine Condello
Mr. Thomas Snee

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Nextel Corporation
Ms. Maria Catafesta
Ms. Allison Growney

Verizon Communications, Incorporated
Mr. Drew Arena
Ms. Margo Hammar

Legislative and Regulatory Task Force Briefers

Department of Homeland Security
Mr. Daniel Ahr
Ms. Emily Hickey
Ms. Laura Kimberly
Mr. Mark Rosen
Ms. Linda Vasta

Federal Communications Commission
Mr. Jeffrey Goldthorp

Legislative and Regulatory Task Force Government Participants

Department of Defense
Ms. Hillary Morgan

Department of Energy
Mr. John Greenhill

Department of Homeland Security
Mr. Daniel Ahr
Ms. Emily Hickey
Ms. Laura Kimberly
Mr. Mark Rosen
Ms. Linda Vasta
Ms. Christina Watson

Federal Communications Commission
Mr. Jeffrey Goldthorp

National Telecommunications Industry Association
Mr. William Belote

Research and Development

Investigation Group / *Period of Activity*

Network Security Task Force
February 1990 – August 1992

Network Security Group
December 1994 – April 1997

Network Group, Intrusion Detection Subgroup
April 1997 – September 1999

Research and Development Exchange Task Force
April 1997 – September 1999

Research and Development Task Force
July 2003 – Present

Issue Background

In today's global economy, advances in communications transform the way in which people live, work, learn, converse, and conduct business. Research is essential to ensure these transformations are productive for society, beneficial for the economy, and sustainable over the long term. Communications and information technology research and development (R&D) advances the digital technologies that power critical national security and emergency preparedness (NS/EP) capabilities. A strong, collaborative R&D program advances the resilience of telecommunications and information systems. Therefore, the President's National Security Telecommunications Advisory Committee (NSTAC) examines areas for future development and seeks to enhance coordination between the public and private sectors and the academic research community.

History of NSTAC Actions and Recommendations

Periodically, the Research and Development Task Force (RDTF) of the NSTAC's Industry Executive Subcommittee (IES) conducts its Research and Development Exchange (RDX) Workshop, the broad purpose of which is to stimulate and facilitate a dialogue among industry, Government, and academia on emerging security technology R&D activities that have the potential to both positively and negatively affect the NS/EP posture of the Nation. To ensure inclusion of all stakeholders in the R&D community, the RDTF traditionally invites representatives from a broad number of private sector companies, academic institutions, and key Government agencies with NS/EP and/or R&D responsibilities such as the Office of Science and Technology Policy (OSTP), the Defense Advanced Research Projects Agency (DARPA) the Department of Homeland Security (DHS) Science and Technology (S&T) directorate, and the National Institute of Standards and Technology (NIST). Over the course of the workshop, participants endeavor to frame key policy issues; identify and characterize barriers and impediments inhibiting R&D; discuss how stakeholders can cooperate and coordinate efforts as the communities of interest shift; and develop specific and realistic recommendations for further action by key stakeholders and decision makers.

The RDX Workshops date back to 1990 when the growing prevalence of hacker incidents led to the formation of the NSTAC's Network Security Task Force (NSTF). The task force's purpose was to assess the threats to and the vulnerabilities of the public switched telephone network. A key component of the task force's work included examining R&D issues related to security with a particular emphasis on improving commercially applicable tools.

In mid-1991, the NSTF identified six areas in which R&D on commercially applicable security tools was needed and asked the Government to share information about its R&D efforts in those areas. The subsequent briefings provided by representatives of the National Security Agency and NIST to the NSTAC, which constituted the NSTAC's first RDX Workshop, demonstrated that Government already had R&D efforts under way in all of those areas.

NSTAC R&D activities gained momentum again in March 1996 when the NSTAC's Network Security Group (NSG) facilitated a seminar for industry and Government to discuss network security R&D activities and issues. The purpose of the seminar was

threefold: (1) provide a common understanding of network security problems affecting NS/EP telecommunications; (2) identify R&D activities in progress to address those problems; and (3) identify additional network security R&D activities needed.

The NSG identified four areas of interest for further investigation from the seminar—authentication, intrusion detection, integrity, and access control—upon which it conducted the second RDX Workshop on September 18, 1996. Because the objective was to facilitate meaningful discussion among participants, participation at the workshop was limited to 50 people representing 15 companies and 11 Government organizations, including one federally funded research and development center. The committee limited industry representation to NSTAC member companies only.

In 1997, in response to a number of stimuli, including the recommendations from the 1996 RDX Workshop, the Network Group (NG)—formerly the NSG—conducted a study of intrusion detection technology R&D and analyzed it in terms of meeting NS/EP requirements. As a result of the analysis, the NSTAC made four recommendations to the President, including the need to increase R&D funding for control systems of critical infrastructures and to encourage cooperative development programs to maximize the use of existing R&D resources in industry, Government, and academia. The NSTAC's recommendations reinforced prior committee recommendations to examine the need for and feasibility of collaborative R&D approaches for security technology. It also provided the basis for the concept of the third RDX Workshop, *Enhancing Network Security Technology: R&D Collaboration,* held in October 1998 at Purdue University's Center for Education and Research in Information Assurance (IA) and Security to examine collaborative approaches to security technology R&D. The participants, which for the first time included members of the academic community, also discussed the need to train more information technology (IT) security professionals, create large-scale test beds to test security products and solutions, and promote the creation of IA Centers of Excellence in academia.

Deliberations at the RDX Workshop at Purdue University resulted in several findings and recommendations for future industry, Government, and academia work. Discussions also noted three recommendations for future NSTAC consideration, including the need to, "conduct another R&D Exchange in the spring of 2000 to continue the dialogue on the long-term issues associated with infrastructure assurance and network security," such as new threats and convergence. The third RDX Workshop also provided the model for all future workshops.

Held at the University of Tulsa in September 2000, the fourth RDX Workshop examined issues of transparent security in a converged and distributed network environment. Attendees discussed the need to address the shortage of qualified information security professionals, expand the number of universities participating in the IA Centers of Excellence program, and promote best practices, standards, and protection profiles to enhance the security of the NGN. Findings and recommendations from the workshop included the establishment of NSTAC task forces to address standards and best practices for network security.

The fifth workshop held in March 2003 at the Georgia Tech Information Security Center (GTISC) at the Georgia Institute of Technology in Atlanta, Georgia, explored the full range of telecommunications and information systems trustworthiness issues as they pertained to NS/EP telecommunications systems. Specifically, the attendees examined trustworthiness from four different perspectives: cyber and software security, physical security, integration issues, and human factors. From this event, the RDTF developed seven specific findings including the need to clearly define the term NS/EP in a post-September 11, 2001, world characterized by a rapidly changing technology and threat environment and the need for a large-scale testbed that could be used as an environment to test NS/EP systems and critical infrastructures.

To directly address the findings from the 2003 RDX Workshop during the NSTAC XXVII cycle, the RDTF developed a "living" discussion paper providing the background for the policy components of the evolving definition of NS/EP. The RDTF also examined several large-scale public and private testbeds, reviewing their capacity to test the telecommunications and information systems infrastructures for NS/EP purposes. As a result, the NSTAC finalized recommendations for a joint, collaborative, distributed industry, Government, and academia pilot testbed that could advance the current state of NS/EP and critical infrastructure protection integration activities.

The sixth workshop, held in Monterey, California in October 2004, reconsidered the R&D issues associated with trustworthy NS/EP telecommunications addressed at the 2003 RDX Workshop and examined progress made, unfinished work, and new challenges. Participants again focused on major cyber and software, physical, human factor, and integration research issue areas and discussed the need for information exchange and collaboration efforts within the R&D community.

At the 2004 RDX Workshop, participants resoundingly agreed that embedding strong, ubiquitous authentication and identity management technologies into future networks was critically important. As a result of this discussion, the NSTAC is currently evaluating whether it should conduct an analysis of identity management security concerns unique to NS/EP telecommunications.

The seventh and first-ever international workshop in Ottawa, Ontario, Canada in September 2006 focused on international multilateral collaborative R&D to enhance security on the network. Participants explored and prioritized critical issues related to international collaboration on communications and cyber R&D that enhanced preparedness and security. Participants identified and characterized barriers and impediments inhibiting multilateral, collaborative research investments and discussed how international stakeholders can cooperate and capitalize on collective advancements.

As a result of the discussions, the NSTAC began to conduct intense analysis of identity management security concerns and increase education and awareness of the subject and strengthen collaboration amongst nations in regards to Research and Development initiatives.

Actions Resulting from NSTAC Recommendations

Following the 2003 RDX Workshop in Atlanta, Georgia, the RDTF provided the Director, OSTP with policy advice on specific areas of security technology R&D that should be taken into account when providing input to the President's fiscal year 2004 budget request. The RDTF also provided its *NS/EP Definition Discussion Paper* to the Executive Office of the President to utilize in on-going discussions on NS/EP communications.

Reports Issued

Network Security Research and Development Exchange Proceedings, September 1996.

Report on the NS/EP Implications of Intrusion Detection Technology Research and Development, December 1997.

Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, October 20-21, 1998.

Research and Development Exchange Proceedings, Transparent Security in a Converged and Distributed Network Environment, September 28-29, 2000.

Research and Development Exchange Proceedings, R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness, March 13-14, 2003.

NS/EP Definition Discussion Paper, April 2004.

Research and Development Exchange Proceedings, A Year Later: R&D Issues to Ensure Trustworthiness in Telecommunications and Information Systems that Directly or Indirectly Impact National Security and Emergency Preparedness, October 28-29, 2004.

The Critical Importance of Testbeds for NS/EP R&D, May 2005.

Research and Development Exchange Proceedings: Leveraging Global Partnerships for the Security of Free Nations and All Sector Preparedness and Response, September 21-22, 2006.

Research and Development Task Force Membership

Computer Sciences Corporation
Mr. Guy Copeland, Chair

Nortel
Dr. John Edwards, Co-Vice Chair

Science Applications International Corporation
Mr. Henry Kluepfel, Co-Vice Chair

AT&T, Incorporated
Ms. Rosemary Leffler

The Boeing Company
Mr. Robert Steele

Lucent Bell Labs
Mr. Kevin Kelly

Motorola, Incorporated
Ms. Julie Kabous

Microsoft Corporation
Mr. Theodore Tanner

VeriSign, Incorporated
Mr. Michael Aisenberg

Verizon Communications, Incorporated
Mr. James Bean

Other Research and Development Task Force Participants

Department of Homeland Security
Ms. Annabelle Lee

Georgia Institute of Technology
Dr. Seymour Goodman

National Coordination Office (NCO) for Networking and Information Technology Research and Development
Dr. Simon Szykman

Previously Addressed Issues

Automated Information Processing

Investigation Group / *Period of Activity*

Automated Information Processing (AIP) Task Force
December 1982 – December 1984

Issue Background

The need to ensure a survivable AIP capability to support NS/EP telecommunications prompted the NSTAC to initiate a study of the AIP issue on December 14, 1982. The AIP Task Force addressed the issue for nearly 2 years.

History of NSTAC Actions and Recommendations

In July 1983, NSTAC II recommended that the President direct the National Security Council, in conjunction with industry, to identify essential NS/EP functions and their dependence on AIP, and to rank those functions in order of priority on a time-phased basis. In April 1984, NSTAC III recommended that the President establish an AIP vulnerability awareness program within the Government. On December 12, 1984, NSTAC IV forwarded the following AIP recommendations to the President:

- Establish a full-time management entity to implement the telecommunications AIP survivability effort;
- Conduct AIP vulnerability awareness programs in conjunction with the private sector;
- Develop NS/EP AIP policy;
- Initiate efforts to enhance the survivability of NS/EP AIP in general; and
- Provide the necessary funding and develop incentives for AIP survivability enhancements.

The TSS Task Force worked on the AIP issue. It reviewed the Government's responses to the NSTAC IV's AIP recommendations. On September 22, 1988, the NSTAC approved and forwarded the TSS Task Force findings and recommendations on AIP to the President.

Actions Resulting from NSTAC Recommendations

The TSS Task Force reviewed the Government's responses to the NSTAC's AIP recommendations. The task force found the Commercial Network Survivability program was addressing the recommendations regarding AIP embedded in telecommunications, but the Government had not implemented the recommendations on AIP for telecommunications operational support and AIP required to support

NS/EP functions in general. The TSS Task Force recommended the Government consider the implications of all operational support AIP, especially for network management, restoration, and reconstitution; and that the Government implement an NS/EP AIP awareness program. The NSTAC approved the TSS Task Force's findings and recommendations on AIP and forwarded them to the President on September 22, 1988.

Reports Issued

Working Group Proceedings on AIP Survivability, October 6, 1982.

AIP Task Force Report, June 1983.

Strategy and Recommendations for Achieving Enhanced NS/EP AIP Survivability, October 25, 1984.

Final Report Addendum, May 1, 1985.

Commercial Network Survivability

Investigation Group / *Periods of Activity*

Commercial Network Survivability (CNS) Task Force
February 1984 – October 1985

Issue Background

In September 1983, the NSTAC IES reviewed the issues associated with telecommunications systems survivability and decided its scope was too broad for a single task force to address. The IES requested that the Resource Enhancements Working Group (REWG) and the Emergency Response Procedures Working Group (ERPWG) meet to discuss and refine the issues. The REWG and ERPWG met on November 9, 1983. They suggested establishing the CNS Task Force to develop and prioritize initiatives to enhance the survivability of the terrestrial portion of commercial carrier networks. The IES initiated the assessment of the CNS issue on February 29, 1984. It formed the CNS Task Force and instructed it to improve the survivability of commercial communications systems and facilities, and identify initiatives to improve interactive emergency response capabilities among the commercial networks.

History of NSTAC Actions and Recommendations

On October 9, 1985, the NSTAC forwarded five CNS recommendations to the President regarding:

- Specification of survivability requirements for NS/EP services;
- Development of NS/EP network architecture plans;
- Development of plans and procedures for network emergency operations;
- Acquisition and maintenance of databases; and
- Government participation in standards organizations.

The President endorsed those initiatives, and the OMNCS undertook a CNS program. On November 6, 1987, the NSTAC approved the TSS Task Force's findings and recommendations on CNS and forwarded them to the President.

Actions Resulting from NSTAC Recommendations

The TSS Task Force reviewed Government actions taken on the NSTAC's CNS recommendations. The task force found the Government's actions focused on the highest threat level, but the Government had taken no action on the CNS Task Force recommendation to form a joint industry and Government group to develop network architecture plans. The TSS Task Force recommended that the CNS program be expanded to include the entire threat spectrum and all NS/EP users.

The OMNCS established a CNS Program Office which engineered and implemented enhancements in the PSN for NS/EP disaster recovery communications use during regional emergencies and national crises. The CNS Program Office evaluated the effectiveness of those enhancements by modeling the anticipated effects of natural disasters and wartime scenarios using computer simulations and through proof-of-concept testing. The OMNCS used its computer modeling capabilities and extensive database containing detailed information on the structure of the PSN to assess the CNS enhancements. Enhancements included dedicated leased lines in the local exchange carrier networks to provide alternate, survivable routes for NS/EP communications. The program office expected future enhancements to use advanced technology service offerings from those same carriers and from cellular service providers and competitive access providers.

The Mobile Transportable Telecommunications (MTT) program, an associated effort, demonstrated reconnecting isolated portions of the PSN using standard military radio equipment. The MTT program performed these demonstrations with National Guard equipment and participation. The CNS Program Office worked with other National Level NS/EP Telecommunications Program (NLP) elements to

ensure interoperability of CNS network enhancements with other NLP component programs, such as Commercial Satellite Command Interconnectivity and the Government Emergency Telecommunications Service. In September 1994, the CNS program was terminated due to budget constraints.

Reports Issued

CNS Task Force (Interim) Report, December 6, 1984.

CNS Task Force Final Report, August 1985.

Commercial Satellite Survivability

Investigation Group / *Period of Activity*

Commercial Satellite Survivability (CSS) Task Force
December 1982 – April 1984
June 1988 – March 1990

Satellite Task Force (STF)
September 2003 – January 2004

Issue Background

At its first formal meeting on December 14, 1982, the NSTAC agreed to emphasize commercial satellite communications survivability initiatives. The NSTAC directed the CSS Task Force Resource Enhancements Working Group to assess the vulnerability of the commercial satellite communications network and the enhancements to the NS/EP

telecommunications infrastructure that the use of commercial carrier satellites and Earth terminals could provide. A separate CSS Task Force reviewed a set of specific satellite initiatives selected for implementation, developed an implementation concept, and prepared a report of its actions and recommendations for the NSTAC.

In June 1988, the NSTAC IES reactivated the CSS Task Force to review the proposed objectives and implementation initiatives of the commercial satellite communications (SATCOM) Interconnectivity (CSI) Phase II Architecture and offer recommendations.

The NSTAC concurred with this action in September 1988.

In March 1990, the NSTAC approved the final report of the reactivated CSS Task Force, which concluded that the CSI Phase II Architecture approach was reasonable, and made several recommendations to the Government.

The terrorist attacks on September11, 2001, raised security concerns about the protection of the Nation's vital telecommunications systems against threats, and raised awareness that a Federal program did not exist to ensure NS/EP communications *via* commercial satellite systems and services.

In January 2003, the Director, National Security Space Architect, requested that the President's NSTAC consider embarking on a study of infrastructure protection measures for SATCOM systems. In response, the NSTAC's IES formed the STF. The STF was established to:

- Review applicable documentation that addresses the vulnerabilities of the commercial satellite infrastructure;
- Define potential policy changes that have to be made to bring the infrastructure into conformance with a standard for mitigating the vulnerabilities;
- Consider Global Positioning System timing capabilities during the deliberations;
- Coordinate this response with representatives from the NCS; and
- Draft a task force report with findings and Presidential recommendations.

History of NSTAC Actions and Recommendations

At its first formal meeting on December 14, 1982, the NSTAC established the CSS Task Force to review a set of specific satellite initiatives selected for implementation, develop an implementation concept, and prepare a report of its actions and recommendations for the NSTAC.

In September 1988, the NSTAC concurred with the IES June 1988 reactivation of the CSS Task Force to review the proposed objectives and implementation initiatives of the CSI Phase II Architecture and offer recommendations.

In March 1990, the NSTAC approved the final report of the reactivated CSS Task Force. The report concluded that the CSI Phase II Architecture approach was reasonable and it recommended the Government:

- Include Ku-band assets in the CSI program to provide "access;"
- Augment selected large Ku-band earth stations and control facilities to provide Ku-band interoperability;
- Use very small aperture terminal technology to restore selected trunking between interexchange carrier switches and local exchange carrier end offices, and selected users in the United States to access the PSN via direct connection at an access tandem; and
- Pursue investigations, analyses, and augmentations necessary to ensure NS/EP telecommunications service can be extended from the United States to NS/EP users overseas.

The NSTAC also approved several specific recommendations to the Government regarding the use and augmentation of satellite assets to achieve various types of connectivity.

In January 2003, the Director, National Security Space Architect, requested that the President's NSTAC conduct a study of infrastructure protection measures for SATCOM systems. In response, the NSTAC's IES formed the STF to analyze and assess SATCOM systems' vulnerabilities and make policy recommendations to the President on how the Federal Government should work with industry to mitigate vulnerabilities to the satellite infrastructure.

The STF engaged broad participation from representatives of NSTAC member companies, non-NSTAC commercial satellite owners and operators, commercial satellite trade associations, Government agencies, and technical experts. The STF concluded its analysis of satellite security in January 2004 and presented its findings in the STF Report. On the basis of its analysis and review of related policy issues, the NSTAC offered the following recommendations to the President:

- Direct the Assistant to the President for National Security Affairs, Assistant to the President for Homeland Security, and Director, Office of Science Technology Policy, to develop a national policy with respect to the provisioning and management of commercial SATCOM services integral to NS/EP communications, recognizing the vital and unique capabilities commercial satellites provide for global military operations, diplomatic missions, and homeland security contingency support;
- Fund the Department of Homeland Security to implement a commercial SATCOM NS/EP improvement program within the NCS to procure and manage the non-Department of Defense satellite facilities and services necessary to increase the robustness of Government communications; and
- Appoint several members to represent service providers and associations from all sectors of the commercial satellite industry to the NSTAC to increase satellite industry involvement in NS/EP.

Actions Resulting from NSTAC Recommendations

The TSS Task Force reviewed the Government actions taken on the NSTAC's CSS Task Force Phase I recommendations and found that the CSI Program and the Industry Information Security Task Force were pursuing most of the CSS initiatives. The TSS Task Force recommended that three aspects of the CSS initiatives be studied further: Ku-band interoperability, up-link jamming protection, and transportable terminals.

The first CSS Task Force's investigations resulted in the definition of 12 initiatives for improving the survivability and robustness of commercial satellite communications resources. The investigations also resulted in the incorporation of the CSS Program Office, established in November 1984, as the CSI

Program Office in 1987. In addition, the CSS Task Force approved the CSI as part of the National Level NS/EP Telecommunications Program.

The CSI Program Office reviewed the CSS Task Force Phase II recommendations. The CSI Program Office investigated satellite technologies, such as Ku-band, and enhanced capabilities, such as connecting to local exchange carriers' switches and providing PSN remote access to NS/EP users, as part of the CSI architecture development effort. The projected CSI Phase II Architecture implementation date was in FY 96, but due to budget constraints, the CSI program was terminated in September 1994.

During its 2004 review of the National Space Policy, the White House incorporated aspects of the STF report into the revised policy. In particular, aspects concerning ground and space links and potential points of failure were included in the revised policy. In addition, at the recommendation of the STF, the President appointed PanAmSat Holdings, Inc. to the NSTAC to represent the commercial satellite industry.

Reports Issued

Issue Papers for Commercial Communications Satellite Systems Survivability Initiatives, March 21, 1983.

Commercial Satellite Communications Survivability Report, prepared by the CSS Task Force Resource Enhancements Working Group, May 20, 1983.

Addendum to the Commercial Satellite Communications Survivability Report, May 20, 1983.

CSS Status Report, April 15, 1984.

Final Report of the CSS Task Force, December 1989.

Final Report of the CSS Task Force, Appendix A, Technical Subgroup Report, December 1989.

Final Report of the CSS Task Force, Appendix B, Operational Subgroup Report, December 1989.

Final Report of the CSS Task Force, Appendix C, International Subgroup Report, December 1989.

Satellite Task Force Report, March 2004.

Common Channel Signaling

Investigation Group / *Period of Activity*

Common Channel Signaling (CCS) Task Force
April 1993 – January 1994

NS/EP Panel
March 1994 – March 1995

Issue Background

At the April 28, 1993, IES Meeting, the Operations Working Group NS/EP Panel recommended that the IES establish a task force to investigate common channel signaling. The task force would determine whether widespread, long- duration CCS outages affecting multiple interconnected carriers were a significant risk to the public switched network and NS/EP telecommunications. The IES established the CCS Task Force to:

- Determine if there were failure mechanisms that could potentially lead to widespread, long-duration CCS outages among multiple interconnected carriers;
- Evaluate the risk to NS/EP user telecommunications;
- If significant risk existed, examine procedural or technological alternatives for mitigating it; and
- Present appropriate recommendations to NSTAC XVI.

The CCS Task Force received informational briefings on the CCS architecture and on CCS network security incidents and concerns, protocol changes, the role of the Network Security Information Exchange in evaluating and determining CCS failures, and the Network Reliability Council's Signaling Network System Focus Team. At NSTAC XVI, March 2, 1994, the IES deactivated the task force.

At the March 2, 1995, IES Meeting, the NS/EP Group Chair explained that during the preceding year, no significant outages had occurred during the group's monitoring of the CCS network (the panel's name was changed to the NS/EP Group in accordance with the December 1994 *IES Guidelines*). The Chair concluded that if no significant outages occurred in the next quarter, the group would discontinue monitoring the CCS network.

History of NSTAC Actions and Recommendations

The task force reported its conclusions and recommendations to NSTAC XVI on March 2, 1994. The task force concluded that the CCS architecture was inherently reliable and that the probability of a large-scale, long-duration, multiple carrier CCS outage resulting from a failure condition propagated to other CCS networks presented a low risk to NS/EP telecommunications. The IES recommended to deactivate the task force and tasked the NS/EP Panel to monitor CCS reliability for a year before reactivating or disbanding the task force.

After receiving this tasking, the NS/EP Panel developed plans for a February 1995 tabletop CCS restoration exercise. In February 1995, the Network Operations Forum conducted the CCS restoration exercise, thus fulfilling the obligations of the CSS Task Force charge.

Reports Issued

Final Report of the Common Channel Signaling Task Force, January 31, 1994.

Electromagnetic Pulse

Investigation Group / *Period of Activity*

Electromagnetic Pulse (EMP) Task Force
September 1983 – October 1985

Issue Background

The NSTAC Industry Executive Subcommittee initiated the EMP assessment on September 27, 1983, in response to a Government request for industry's perspective on the options available to industry and Government for improving the EMP survivability of the Nation's telecommunications networks. The NSTAC approved the EMP study on April 3, 1984.

History of NSTAC Actions and Recommendations

On December 12, 1984, the NSTAC forwarded the following recommendations on EMP to the President:

- Designate an appropriate Federal agency to serve as an industry point of contact for EMP mitigation efforts and information distribution;
- Support industry through its standards organizations in the development of electromagnetic standards that take the EMP environment into account; and
- Undertake a program to improve the EMP endurability of the Nation's commercial electrical power systems.

On October 9, 1985, the NSTAC approved the *EMP Final Task Force Report* and forwarded a recommendation to the President, calling for a joint industry and Government program to reduce the costs of existing techniques for mitigating high-altitude electromagnetic pulse-induced transients and to develop new techniques for limiting transient effects.

Actions Resulting from NSTAC Recommendations

The TSS Task Force reviewed the Government actions taken on the NSTAC's EMP recommendations. It found that the Government had implemented nine of the EMP initiatives or was implementing them. The TSS Task Force made the following recommendations:

- Industry and Government should continue to work together to implement the EMP initiatives;
- The Government should prepare an unclassified EMP handbook; and
- Industry, consistent with cost, should incorporate low-cost mitigation practices in its new/upgrade programs.

The NSTAC approved the TSS Task Force's findings and recommendations on EMP and forwarded them to the President on November 6, 1987.

The OMNCS designated its Office of Technology and Standards as the Federal office to serve as an industry and Government point of contact. It used the American National Standards Institute T1Y1 Committee as a forum for developing electromagnetic standards in support of industry and issued an unclassified EMP handbook (*EMP Mitigation Program Approach, NCS-TIB 87-17*). The OMNCS received results from a simulated EMP test on an AT&T PSN switch. The OMNCS assessed the EMP impact on the PSN based on test results of transmission, signaling, and switching facilities. EMP test analysis results showed little cause for concern regarding the physical EMP survivability of the PSN, but revealed an increasing PSN vulnerability to EMP-induced switch and signaling upset.

Reports Issued

EMP Task Force Status Report, January 12, 1984.

EMP Final Task Force Report, July 1985.

Energy

Investigation Group / *Period of Activity*

Energy Task Force
August 1988 – March 1990
October 1991 – May 1993

NS/EP Panel
March 1994 – October 1994

Issue Background

In 1986, the Telecommunications Systems Survivability (TSS) Task Force initially reviewed the vulnerability of telecommunications to the loss of commercial electric power and presented the results of its review at the February 8, 1987, NSTAC VII Meeting. The TSS Task Force concluded the telecommunications industry would be extremely vulnerable to an extended electric power outage. As a result, the NSTAC recommended to the President that Government initiate a study to identify options for ensuring electric power survivability as it related to telecommunications. The NSTAC also offered its services to support the effort. Following the President's reply, the NSTAC formed the Energy Task Force and it became the focal point of a joint electric power and telecommunications industry effort to address the question of electric power survivability as it relates to telecommunications. The Department of Energy (DOE), NCS, and the North American Electric Reliability Council (NERC) participated in the Energy Task Force.

The NSTAC IES charged the first Energy Task Force with developing recommendations to mitigate the effects of electric power outages on telecommunications. It examined interdependencies between electric power and telecommunications after a major earthquake. Further, at NSTAC X, the task force presented the following recommendations:

- Sponsor further research on the impact of a major earthquake on electric power, telecommunications, and transportation systems; and
- Establish a nationwide process for restoring electric power and distributing energy supplies during major emergencies.

The NSTAC approved the *Energy Task Force Final Report,* which recommended that the Government:

- Develop a program for assigning electric power restoration priorities to NS/EP telecommunications users and providers to provide the soonest possible service restoration;
- Establish a program for assigning priorities for the supply, transport, and delivery of fuels to NS/EP telecommunications users and providers;
- Grant a national security waiver from those applicable subparts of the Government's underground storage tank regulation (40 Code of Federal Regulations Part 280);
- Ensure that NS/EP telecommunications users who need electric power to operate their customer premises equipment have a backup power capability that can operate through at least a 7-day electric power outage; and
- Fund studies to examine the feasibility of the Government's developing and supplying long-lasting, cost-effective backup power sources for critical telecommunications facilities.

In October 1991, the NSTAC reactivated the Energy Task Force to advise the NCS and the DOE concerning the implementation of energy priority initiatives for telecommunications facilities. The reactivated task force assisted in developing the DOE's Telecommunications Electric Service Priority (TESP) initiative in response to the original task force's first two recommendations. When fully implemented, the TESP initiative would provide priority electric power restoration to critical NS/EP telecommunications facilities.

After reviewing DOE's National Energy Strategy (NES) in December 1991, the IES also charged the Energy Task Force to review the NES from the perspective of

benefits to NS/EP telecommunications enhancements and develop NS/EP telecommunications energy concerns/issues for incorporation into DOE's next issue/update of the NES.

The energy issue concluded when NSTAC XV charged the IES to deactivate the Energy Task Force. The NSTAC also tasked the IES to request progress reports from the Government on the status of its recommendations.

History of NSTAC Actions and Recommendations

As a result of an NSTAC VIII recommendation, the IES formed the first Energy Task Force. The task force was the focal point of an electric power/telecommunications industry effort to address the issue of electric power survivability as it relates to telecommunications. The DOE, NCS, and the NERC actively participated in the Energy Task Force.

On October 3, 1991, NSTAC XIII approved the recommendation to establish a follow-on Energy Task Force. The task force's charge was to support the OMNCS in its efforts with DOE to develop criteria and a process for identifying critical industry NS/EP telecommunications facilities that qualify for electric power restoration and priority fuel distribution.

At the May 27, 1993, NSTAC XV Meeting, members approved the *Energy Task Force Final Report* and the task force's recommendations, and forwarded both to the President. The task force recommended that the Government:

- Continue to support the operation, administration, and management of DOE's TESP initiative;
- Assign Federal responsibility for the establishment of a program to ensure priority availability of fuel supplies for telecommunications companies during emergencies;
- Encourage the Nation's electric utilities to coordinate with telecommunications companies to provide safe access to disaster areas requiring Telecommunications Service Priority provisioning or restoration;
- Encourage State and local Governments to modify their emergency plans to allow telecommunications, electric utility, and fuel supply company's access into areas experiencing outages; and
- Modify the Federal Response Plan and the National Plan for Telecommunications Support in Nonwartime Emergencies to include TESP and to address emergency fuel resupply, access, and safety issues.

The Energy Task Force also recommended that, to address the improvement of electric power survivability under disaster conditions, the President's National Energy Strategy should:

- Increase R&D and incentives to reduce transmission and distribution vulnerabilities;
- Evaluate locating dispersed power generation closer to customer loads as a possible means of further reducing transmission and distribution vulnerabilities; and
- Focus more R&D on alternative backup power technologies for the telecommunications industry by encouraging cooperative R&D agreements between the U.S. national laboratories and interested telecommunications companies.

On March 8, 1994, the NS/EP Panel discussed power outages that occurred during the recent winter storms on the East Coast and during the Northridge earthquake, and their effect on telecommunications. The panel agreed that a call from the power companies would have alerted carriers to the impending rolling blackouts and the need to switch to an emergency backup power source. Additionally, the panel agreed that the TESP initiative should be more responsive to industry's requirements during emergencies and disasters. As a consequence of this discussion, the panel scheduled briefings from the NCS Office of Plans and Programs on the status of its discussions with DOE on TESP, and then with DOE on the status of the TESP initiative.

On October 13, 1994, as a result of industry's concerns about the initiative, the NSTAC invited the DOE to address the joint Operations Working Group (OWG) and Plans Working Group (PWG) meeting. The former TESP initiative was introduced as the National Electric Service Priority (ESP) Program in Support of Telecommunications. ESP was defined as a program developed jointly between DOE, the NCS, and the telecommunications industry. Under ESP, electric utilities voluntarily add NS/EP telecommunications facilities to their ESP programs. The ESP program emphasizes local coordination between electric utilities and telecommunications facilities.

In response to criticism that the DOE was not responsive to industry's needs during the 1994 winter storms, the DOE representative noted several problems contributed to the insufficient generating capacity. Utilities had been asked to switch from natural gas; barges were unable to get through ice to deliver coal; northeastern electric power companies were purchasing power from California, Florida, and Oklahoma. However, the rising demand resulted in brownouts, followed by rolling blackouts.

In December 1994, the NCS provided an updated list of critical telecommunications facilities to DOE. The DOE collected electric utility points-of-contact information that the telecommunications industry supplied. DOE continues to work with all 50 States to ensure nationwide ESP implementation.

In regard to other telecommunications energy issues, DOE recommended industry contact each State and that the State enroll in the fuel set-aside program. DOE further stated that, as a result of Hurricane Andrew that hit Florida, power companies and telecommunications providers were working more closely together. Finally, in response to industry's request to obtain access to a disaster site, DOE stressed that such access could be dangerous. Criminal elements can harm utility workers unless there is sufficient law enforcement personnel available to ensure their protection.

Actions Resulting from NSTAC Recommendations

In response to the Energy Task Force recommendations at NSTAC X, the OWG NS/EP Panel discussed the status of NCS and DOE activities. The panel expressed support for recent NCS and DOE initiatives and concluded that industry should continue to advise the NCS and DOE on implementation of the energy initiatives. The IES and NSTAC approved the recommendation to establish a follow-on Energy Task Force. Its charge was to support the OMNCS efforts with DOE and NCS to develop criteria and a process for identifying critical industry NS/EP telecommunications facilities that qualify for electric power restoration and priority fuel distribution.

On April 2, 1991, the NCS issued Directive 3-8, Provisioning of Emergency Power in Support of NS/EP Telecommunications. The DOE and the NCS worked together to identify critical telecommunications facilities that qualify for priority electric power restoration.

In December 1993, DOE began implementing the TESP initiative and made plans to update the critical facility list. As of September 1993, 28 States indicated their desire to voluntarily participate in the TESP initiative; with additional States expected to follow.

At the October 13, 1994, OWG-PWG meeting, DOE explained that it replaced the TESP initiative with its ESP program in support of telecommunications. DOE had developed the ESP program in response to the National Security Advisor's request that the Secretary of Energy develop and implement a priority process for electric power restoration. DOE is working with all 50 States in implementing ESP nationwide. DOE's partnership with the NCS and the telecommunications industry is facilitating ESP implementation.

During NSTAC Cycle XXVIII, the NSTAC revisited issues related to interdependency between the telecommunications and electric power infrastructures and formed the Telecommunications and Electric Power Interdependency Task Force (TEPITF) to address these issues. (See the

Interdependency Between Telecommunications and Electric Power Infrastructures section in the Active Issues section of this *NSTAC Issue Review*).

Reports Issued

Report on Earthquake Hazards, June 8, 1989.

Energy Task Force Final Report, February 1990.

Energy Task Force Final Report: Telecommunications Electric Service Priority and National Energy Strategy Review, April 1993.

Enhanced Call Completion

Investigation Group / *Period of Activity*

Industry Executive Subcommittee (IES) Funding and Regulatory Working Group (FRWG)
(Assured access)
June 1990 – September 1990
(Regulatory aspect of call-by-call preferential treatment)
July 1993 – December 1993

Enhanced Call Completion (ECC) Task Force
December 1990 – July 1992

ECC Ad Hoc Group
July 1992 – August 1993

Issue Background

Following its reactivation after NSTAC XI, the NSTAC IES tasked the FRWG to investigate NS/EP issues affecting assured access to the public switched network (PSN). During FRWG discussions with the Government, the group agreed that assured access was only one component of the Government's need for enhanced NS/EP call completion. The group defined assured access as priority access to, transportation through, and egress from the PSN for NS/EP users when portions of the PSN were either physically isolated or too congested to permit unhindered access and call completion.

The FRWG prepared a study addressing the regulatory and technical components of assured access. The study reported that at its initial meeting, the FRWG concluded that the Government required enhanced call completion for NS/EP traffic. The FRWG members agreed, however, that they must further define the technical features of the issue before identifying regulatory issues.

On August 22, 1990, the FRWG recommended that it establish an ECC Task Force to determine how existing and evolving technologies could best be exploited to enhance the priority access, transport, and egress of NS/EP traffic. The FRWG's study also stated that the proposed task force should evaluate the *Intelligent Networks Task Force Final Report* and recommendations, and coordinate its efforts with those of the OMNCS to avoid duplication.

Following the FRWG's investigation of issues affecting assured access to the PSN by NS/EP callers and its subsequent recommendations, the NSTAC, at its December 13, 1990, meeting charged the IES to establish a task force to review the issue of enhancing call completion for NS/EP users during periods of congestion. Specifically, the IES directed the task force to identify technical approaches and to recommend a plan of action for obtaining enhanced call completion in both the near and long term.

The ECC Task Force studied existing and evolving technologies that would provide the NS/EP user PSN access and call completion without interruption, with minimum delay, and on a preferential basis during network damage or congestion. During its 18-month investigation, the task force identified 26 current or planned enhanced call completion features and defined their NS/EP application, availability, and acquisition procedures. The task force also determined the importance of the High Probability of Call Completion (HPC) standard in implementing an NS/EP call identifier to provide call-by-call preferential treatment and to enhance existing PSN features.

At the July 17, 1992, NSTAC XIV Meeting, members approved the ECC Task Force's report for forwarding to the President, the two proposed recommendations to the President, and the proposed NSTAC XIV charges to the IES. In response to these charges, the IES deactivated the ECC Task Force and established an ad hoc group to work with the Government to:

- Advocate and support approval of the HPC standard, investigate potential ECC regulatory issues with the FRWG and implement ECC network capabilities.

At the August 2, 1993, IES Meeting, members approved the deactivation of the ECC Ad Hoc Group, which had completed its work. The group served as a forum for issues such as cellular priority access,

preferential access for North Atlantic Treaty Organization countries, and future broadband services. It assisted the Government in its effort to obtain approval of the HPC standard—published as American National Standards Institute T1.631 in August 1993. The group also worked closely with the Government to develop ECC features demonstration scenarios. It met with the GETS integrator and Government contractors to discuss demonstration plans and scenarios.

As part of its charge to inform the Government about ECC services affecting the National Level NS/EP Telecommunications Program initiatives, the group assisted the Government in developing educational materials such as the *ECC Services Cost/Benefit Analysis Report,* and the 1993 *National Communications System (NCS) Member Agency Telecommunications Enhancement Handbook.* The group worked with the Government in addressing potential regulatory impediments to implementing enhanced call completion services. It framed and defined significant elements in the call-by-call preferential treatment issue before forwarding the issue to the FRWG for its action.

In July 1993, the FRWG responded to an April 14, 1993, memorandum to the NCS Executive Agent directing the NCS to work with the FRWG to investigate potential regulatory issues arising from the implementation of enhanced call completion attributes for NS/EP activities. The FRWG explored whether the prohibition of undue preferences in Section 202(a) of the Communications Act of 1934, as amended, required a specific FCC regulation authorizing the provision of priority calling features to NS/EP users of the PSN.

The FRWG determined FCC approval of preferential treatment would benefit both industry and Government. Following IES approval, the OMNCS forwarded a letter to the FCC requesting that the Commission issue an opinion regarding whether common carriers may provide call-by-call priority service for connecting emergency calls over the public switched network. The FCC responded by issuing a Public Notice on January 7, 1994, which requested that public comments be filed with the Commission by February 15, 1994, and that reply comments be filed by March 1, 1994. The OMNCS filed reply comments with the FCC on March 1, 1994, requesting that the Commission issue a favorable opinion.

On August 30, 1995, the FCC responded to the OMNCS regarding the call-by-call priority issue. In its letter, the FCC stated that the request for declaratory ruling filed on November 29, 1993, was moot because lawful tariffs implementing the federally managed GETS program had gone into effect. Call-by-call priority is a feature of the GETS program. Therefore, the FCC dismissed the petition for declaratory ruling without prejudice.

History of NSTAC Actions and Recommendations

On December 13, 1990, NSTAC XII charged the IES to establish the ECC Task Force as a result of the FRWG's investigation of assured access issues.

On July 17, 1992, NSTAC members approved the ECC Task Force's report for forwarding two proposed recommendations to the President:

- The Government should take the following steps to enhance call completion for NS/EP users:
  - Take advantage of existing and emerging services, features, and capabilities in the PSN
  - Continue to support the near-term adoption of the HPC standard by the Exchange Carriers Standards Association T1 Committee
  - Investigate the NS/EP advantages of a calling name delivery service
  - Work with NSTAC's FRWG to investigate potential regulatory issues
  - Sponsor industry ECC forums to further define ECC and resolve implementation issues.
- The Government should use the ECC Task Force report as a reference for modifying or implementing current or future services and technologies. In response to NSTAC XIV charges,

the IES established the ECC Ad Hoc Group. On August 2, 1993, IES members deactivated the ECC Ad Hoc Group.

Actions Resulting from NSTAC Recommendations

In response to an NSTAC XIV recommendation from the ECC Task Force, the White House issued a memorandum to the NCS Executive Agent on April 14, 1993, directing the NCS to work with the FRWG to investigate potential regulatory issues arising from the implementation of ECC attributes for NS/EP activities. The FRWG sought to clarify whether prohibitions of undue preferences in the *Communications Act of 1934* required a specific FCC regulation to authorize the provision of priority calling features to NS/EP users of the public switched network. The FCC resolved the issue on August 30, 1995, when the FCC informed the OMNCS of its decision regarding the call-by-call priority issue.

Reports Issued

Assured Access Issue Paper, October 13, 1989.

Report on the FRWG Review of Assured Access, November 7, 1990.

Final Report of the Enhanced Call Completion (ECC) Task Force, July 1992.

Final Report of the Enhanced Call Completion (ECC) Ad Hoc Group, December 1993.

Financial Services

Investigation Group / *Period of Activity*

Financial Services Task Force (FSTF)
March 2003 – April 2004

Issue Background

In November 2002, the Federal Reserve Board (FRB) and BITS—a nonprofit industry consortium of the 100 largest financial institutions in the United States that focuses on issues related to security, crisis management, e-commerce, payments, and emerging technologies—briefed the IES of the NSTAC on the significant dependence of the financial services (FS) sector on the telecommunications infrastructure to support core payment, clearance, and settlement processes of financial institutions. Given that dependence, disruption of telecommunications services could hamper critical financial services processes, potentially affecting the national economy. To minimize operational risks and ensure the timely delivery of critical financial services, the FRB recommended that the NSTAC analyze telecommunications infrastructure issues pertaining to network redundancy and diversity.

The NSTAC, therefore, established the FSTF to conduct the analysis during NSTAC Cycle XXVII.

History of NSTAC Actions and Recommendations

The FSTF emphasized that the concept of resiliency and its components of diversity, redundancy, and recoverability are critical to understanding some of the NS/EP issues currently challenging the FS and telecommunications industries. The task force acknowledged that it is imperative for the FS sector to maintain diversity as a component of resiliency. The primary challenges identified by the FSTF with respect to diversity were the failure of critical services resulting from loss of diversity; the ability to ensure that diversity is predictable and continually maintained; and the potential for lack of clear understanding of terms and conditions in telecommunications contracts or tariffs (and the potential for resulting confusion when financial services institutions establish business continuity plans).

The FSTF recognized that without a real-time process to guarantee that a circuit's path or route is static and stable, an NS/EP customer cannot be assured at all times that the diversity component of the resiliency plan will retain its designed characteristics. However, the telecommunications infrastructure was designed and engineered based on a business model directed at the general public. When necessary, networks have been modified or developed to meet specific needs at the customer level except where limited by the available technology or a customer's willingness to purchase unique requirements.

The FSTF emphasized that all interested parties should support research and development activities for improving managed network solutions and alternative technologies as a potential means for achieving high resiliency for the FS customer base. Targeted capital incentives should also be considered as a tool to encourage critical infrastructure owners, including the FS sector, to make the necessary investments to mitigate telecommunications resiliency risks to their business operations. Appropriately structured capital recovery incentives for critical business operations could be used to accelerate immediate investments to mitigate vulnerabilities to critical NS/EP operations.

The FSTF also noted that when different business continuity strategies cannot fully guarantee operational sustainability, specifically engineered and managed efforts might be required. The degree of assurance that a business operation deems adequate to achieve a high level of resiliency will dictate the decisions and the appropriate approach to be pursued. To that end, the task force concluded that cross-sector assessments or customer-provider assessments would remain useful tools to facilitate better understanding of the need for resiliency. Indeed, FSTF members acknowledged the importance of promoting mutual understanding among the FS and telecommunications sectors to

effectively address NS/EP-related issues. Both sectors pledged to continue in their efforts to engage members of their communities, as well as the public sector, in a constructive dialogue to foster mutual understanding of their operations and unique needs. Furthermore, the framework that the FSTF developed to analyze the dependencies of the FS sector on the telecommunications industry could be adapted to conduct risk assessments of other critical infrastructures.

On the basis of the FSTF report, the NSTAC recommended that the President:

- Support the Alliance for Telecommunications Industry Solutions' (ATIS) National Diversity Assurance Initiative and develop a process to:
  - Examine diversity assurance capabilities, requirements, and best practices for critical NS/EP customers and, where needed
  - Promote research and development to increase resiliency, circuit diversity, and alternative transport mechanisms.
- Support financial services sector initiatives examining:
  - The development of a feasible "circuit-by-circuit" solution to ensure telecommunications services resiliency
  - The benefits and complexities of aggregating sectorwide NS/EP telecommunications requirements into a common framework to protect national economic security.
- Coordinate and support relevant cross-sector activities (*e.g.,* standards development, research and development, pilot initiatives, and exercises) in accordance with guidance provided in Homeland Security Presidential Directive 7 (HSPD-7).
- Provide statutory protection to remove liability and antitrust barriers to collaborative efforts when needed in the interest of national security.
- Continue to promote the Telecommunications Service Priority program as a component of the business resumption plans of financial services institutions.
- Promote research and development efforts to increase the resiliency and the reliability of alternative transport technologies.
- Examine and develop capital investment recovery incentives for critical infrastructure owners, operators, and users that invest in resiliency mechanisms to support their most critical NS/EP telecommunications functions.

Actions Resulting from NSTAC Recommendations

In response to the FSTF report, ATIS agreed to work with the FRB on an in-depth assessment of diversity assurance. A final report on the assessment was completed in February 2006. Representatives from ATIS also visited the IES to brief them on the findings and recommendations discussed in the assessment.

Reports Issued

Financial Services Task Force Report, April 2004.

Funding of NSTAC Initiatives

Investigation Group / *Period of Activity*

Funding of NSTAC Initiatives (FNI) Task Force
April 1984 – December 1984

Issue Background

On April 3, 1984, the NSTAC agreed to address the funding of NSTAC initiatives issue to determine the costs and benefits associated with its recommendations to the Government. The purpose of FNI was to guide and prioritize NSTAC actions. In August 1984, the FRWG established the FNI Task Force to investigate approaches to NSTAC funding mechanisms.

History of NSTAC Actions and Recommendations

On December 12, 1984, the NSTAC approved the funding methodology developed by the FNI Task Force and instructed the IES to:

- Adopt the methodology developed by the FNI Task Force;
- Issue the funding methodology as guidance to all existing and future task forces; and
- Direct all task forces to determine costs, benefits, and applicable funding mechanisms for each recommended initiative.

The NSTAC instructed all NSTAC task forces and working groups to apply the FNI funding methodology to the recommendations they developed. The FRWG assists all active and future NSTAC task forces, when necessary, in providing cost/benefit estimates and proposed funding mechanisms for all recommended initiatives using the guidelines from the funding report.

Actions Resulting from NSTAC Recommendations

The FRWG (reconvened March 1990) reviewed the NSTAC funding methodology and worked with the Enhanced Call Completion Task Force to develop an order-of-magnitude cost model for use by all task forces.

Reports Issued

NSTAC Funding Methodology, October 25, 1984.

Globalization

Investigation Group / *Period of Activity*

National Information Infrastructure (NII) Task Force
August 1993 – March 1997

Operations Support Group (OSG)
April 1997 – September 1999

Information Infrastructure Group (IIG)
April 1997 – September 1999

Globalization Task Force (GTF)
September 1999 – May 2000

Issue Background

In 1993, the NSTAC established an NII Task Force and charged it with examining the implications of the evolving U.S. information infrastructure for NS/EP communications. The NII Task Force observed that the NII's connectivity to the emerging Global Information Infrastructure (GII) potentially presented both opportunities and risks for NS/EP communications. In its March 1997 report to NSTAC XIX, the NII Task Force concluded that the pervasive and rapidly evolving nature of the GII necessitated a continuing effort by NSTAC task forces and working groups to track the GII's implications for NS/EP communications.

As a result, the NSTAC IES tasked the OSG in April 1997 to monitor the U.S. information infrastructure's global interfaces, because of the potential for increased vulnerabilities adversely affecting the national interest. Specifically, the OSG gathered information on the International Telecommunication Union's *Global Mobile Personal Communications by Satellite Memorandum of Understanding*. In October 1998, the IES tasked the IIG to conduct a forward-looking analysis of the GII and associated NS/EP opportunities and challenges.

During a reorganization of the IES and its working group structure in September 1999, the IES formed the GTF to continue to address the GII issue. Specifically, the IES tasked the GTF with developing a "picture" of the GII in 2010, identifying NS/EP issues. The GTF was also given two additional tasks that were global in scope: assessing the security implications of foreign ownership of telecommunications networks and examining export policies dealing with the transfer of strong encryption products, satellite technology, and high-performance computers.

During the NSTAC XXII and XXIII cycles, the IIG and GTF researched and gathered information from industry and Government experts on emerging space-, airborne-, and land-based communications systems and services. These information gathering activities provided the GTF with the insights needed to characterize the GII in 2010 and draw conclusions about NS/EP telecommunications preparedness.

Drawing on these insights, the GTF was able to describe what physical network elements, services, and protocols might be prominently featured in 2010, paying specific attention to the global homogenization of communications capabilities, expected improvements to quality of service and network assurance, and the ubiquity and availability of advanced communications technologies as pertaining specifically to NS/EP users. The GTF documented its analysis in its May 2000 report to NSTAC XXIII. Based on that analysis, the NSTAC recommended that the President direct appropriate departments and agencies to:

- Conduct exercises in those areas and environments in which NS/EP operations can be expected to take place to ensure that the required high-capacity, broadband access to the GII is available; and

- Ensure that NS/EP requirements, such as interoperability, security, and mobility, are identified and considered in standards and technical specifications as the GII evolves to 2010

and identify any specialized services that must be developed to satisfy NS/EP requirements not satisfied by commercial systems.

In addition, the LRWG assisted the GTF in assessing the security implications of foreign ownership of telecommunications networks. The LRWG examined domestic regulatory history and conducted analyses of several mergers and acquisitions between domestic and foreign telecommunications carriers. Through the case studies, the group found that the current regulatory structure satisfied the different interests of the parties involved. The LRWG concluded that it was unclear whether further statutory or regulatory changes would effectively enhance the role of national security issues in foreign ownership situations at this time. The GTF May 2000 report to NSTAC XXIII includes the LRWG analysis of the issue.

Based on the GTF's report, the NSTAC recommended that the President:

- Ensure that the review process for commercial arrangements involving foreign ownership remains adequate to protect NS/EP concerns as the environment evolves and becomes more complex.

Lastly, addressing technology export, the GTF compiled some basic information on the key technology export issue areas. Given that technology progresses faster than export policy can keep up with it, the GTF recommended continued monitoring of developing export policies and regulations. The GTF also investigated guidelines to assist companies in understanding Government approval of technology sales. The GTF completed its tasking to scope the issue of technology export, concurring with the Government's efforts to periodically reevaluate the limits placed on the export of technologies.

Reports Issued

National Information Infrastructure Task Force Report, March 1997.

Operations Support Group Report, September 1998.

Information Infrastructure Group Report, June 1999.

Globalization Task Force Report, May 2000.

Global Infrastructure Report, May 2000.

Paper on Foreign Ownership: Telecommunications and NS/EP Implications, May 2000.

Industry/Government Information Sharing and Response

Investigation Group / *Period of Activity*

National Coordinating Center for Telecommunications (NCC) Vision Task Force
October 1996 – April 1997

Operations Support Group (OSG)
April 1997 – September 1999

Information Sharing/Critical Infrastructure Protection (IS/CIPTF) Task Force
September 1999 – May 2000

Issue Background

The NSTAC formed the National Coordinating Mechanism (NCM) Task Force in December 1982 to facilitate industry/Government response to the Government's growing NS/EP telecommunications service requirements in the post-divestiture environment. The task force submitted its final report, the *NCM Implementation Plan,* to the NSTAC on January 30, 1984. That report led to formation of the NCC, an emergency response coordination center that supports the Government's NS/EP telecommunications requirements.

Since 1984, threats to the NS/EP telecommunications infrastructure changed significantly. In response, the NSTAC IES established the NCC Vision Task Force in October 1996 to consider the implications of the new environment for the functions performed by the NCC. The IES charged the task force to determine whether the mission, organization, and capabilities of the NCC were still valid, considering the ongoing changes in technology, industry composition, threats, and requirements. Following the IES group reorganization in April 1997, the task force became the NCC Vision Subgroup and later the NCC Vision-Operations Subgroup under the OSG.

In 1997, the NSTAC also revisited the original concept for an industry/Government mechanism to coordinate planning, information sharing, and resources in response to NS/EP requirements. Unlike the original NCM plan that applied to the telecommunications infrastructure, this revised NCM concept involved linking all the Nation's critical infrastructures (*e.g.,* telecommunications, financial services, electric power, and transportation). In July 1997, the OSG created the NCM Subgroup to explore the need for and feasibility of an NCM across infrastructures.

In May 1998, the President released PDD-63, a critical infrastructure protection directive calling for, among other things, industry participation in the Government's efforts to ensure the security of the Nation's infrastructures. As it continued to refine the NCM concept, the NCM Subgroup considered this Government initiative.

In September 1998, the OSG formed the Year 2000 (Y2K) Subgroup to address several Y2K issues raised at the NSTAC XXI meeting, including the need for Y2K outreach efforts, the need to emphasize contingency planning and restoration scenarios, the potential for public overreaction to the Y2K problem, and the lack of a global approach to handle Y2K problems that were international in scope. The effort was a continuation of earlier efforts by the NCC Vision-Operations Subgroup, which began a study of the NCC's operational readiness and coordination capabilities for potential public network disruptions caused by the Y2K problem.

Following NSTAC XXII the IES tasked the OSG to examine potential lessons learned from Y2K experiences that could be applied to critical infrastructure protection efforts. The OSG focused on the experiences of the NCC to determine how its operations during the Y2K rollover period translated into functions to be performed as ISAC (in accordance with PDD-63). In addition the OSG continued to monitor enhancements to the NCC that ensured an electronic Indications, Assessment, and Warnings (IAW) capability to support the ISAC function.

In September 1999 following a reevaluation of NSTAC working groups, the IES created the IS/CIPTF to examine mechanisms and processes for protected, operational information sharing that would help achieve the goals of PDD-63 and further the role of the NCC as an ISAC for telecommunications. In addition, the IES directed the IS/CIPTF to continue, through outreach efforts, interaction with Government leaders responsible for PDD-63 implementation.

History of NSTAC Actions and Recommendations

During 1997, the NCC Vision Subgroup worked closely with the NCS member organizations and NCC industry representatives to develop a common framework for assessing the NCC's ongoing role. The subgroup validated the original 10 NCC chartered functions and updated the *NCC Operating Guidelines* (both written in 1984) for the current operational environment. The subgroup also determined that an electronic intrusion incident information processing function could be integrated into the NCC's activities. In August 1997, the subgroup held an industry/Government tabletop exercise to test the draft concept of operations for NCC intrusion incident information processing. The OSG documented the subgroup's activities and accomplishments in the OSG's report to the December 11, 1997, NSTAC XX Meeting.

The NSTAC approved the OSG's NSTAC XX report and recommended that the President:

- Establish a mechanism within the Federal Government with which the NCC can coordinate intrusion incident information issues and with which NSTAC groups can coordinate the development of standardized reporting criteria.

The NSTAC also endorsed NCC implementation of an initial intrusion incident information processing pilot based on voluntary reporting by industry and Government.

In 1998, the NCC modified its standard operating procedures to accommodate an electronic intrusion incident information processing capability. With the OSG's support and assistance, the NCC began its intrusion incident information processing pilot on June 15, 1998. The NCC Vision-Operations Subgroup worked closely with the OMNCS and the Manager, NCC, as the NCC implemented the intrusion incident processing pilot, which it completed in October 1998. In addition, the NCC Vision-Operations Subgroup developed a paper, the *NCC Intrusion Incident Reporting Criteria and Format Guidelines,* to establish standardized reporting criteria and to outline steps in NCC electronic intrusion report collection, processing, and distribution. The OSG report to NSTAC XXI includes the paper.

Leading up to NSTAC XX, the NCM Subgroup met jointly with the Information Infrastructure Group's IA Policy Subgroup and produced a joint report. The report concluded that the revised NCM concept provided the framework for the Federal Government and the private sector to address solutions to infrastructure protection concerns. The OSG included the joint report in its full NSTAC XX report, which the NSTAC approved. Specifically, the NSTAC recommended that the President:

- Direct the appropriate departments and agencies to work with the NCS and NSTAC in further investigating the NCM concept.

Subsequently, IES representatives presented the revised NCM concept to senior Government officials to aid the Administration's efforts to establish national policy on the protection of critical national infrastructures.

Throughout the NSTAC XXI cycle, the OSG considered the infrastructure protection efforts of the Federal Government in conjunction with the enhanced role of the NCC. IES and NCM Subgroup members met with members of the National Infrastructure Protection Center (NIPC) to address the role of industry in the Government's new IA environment. The Government created the NIPC in February 1998 as a national critical infrastructure threat assessment, warning, vulnerability, law enforcement investigation, and response entity. The NIPC's mission is to detect, deter, assess, warn of,

respond to, and investigate computer intrusions and unlawful acts, both physical and cyber, that threaten or target the Nation's critical infrastructures. As a result of these meetings, the NCC and NIPC began to develop processes to detail the flow of information between the two entities.

At the end of the NSTAC XXI cycle, the OSG concluded that the NCC provided a model for all infrastructures by which information could be gathered, analyzed, sanitized, and provided to the Government. In addition, regarding PDD-63 implementation, the OSG concluded that more than one individual or entity would be needed to serve as the sector coordinator to represent the highly diverse information and communications sector. The NSTAC approved the OSG's September 1998 report to NSTAC XXI and recommended that the President direct the lead departments and agencies as designated in PDD-63 to:

- Consider adapting the NCC model as appropriate for the various critical infrastructures to provide warning and information centers for reporting and exchange of information with the NIPC through the NCM process; and

- Establish an industry/Government coordinating activity to advise in the selection of a sector coordinator and provide continuing advice to effectively represent each critical infrastructure.

Following NSTAC XXI, the OSG's NCC Vision-Operations Subgroup worked closely with the OMNCS and the Manager, NCC, as the NCC continued its electronic intrusion incident processing function. The subgroup continued to assist the NCC in evaluating any needed revisions to the IAW reporting criteria and format guidelines.

The OSG's NCC Vision-Operations Subgroup also assessed whether the NCC requires additional industry and Government participation within the NCC to widen the scope of expertise and operational personnel available to fulfill the IAW mission. During the NSTAC XXII cycle, the subgroup developed a list of companies and Government departments and agencies for the Manager, NCS, to consider as candidates for participation in the NCC.

PDD-63 established the concept of an ISAC that would be a private sector entity responsible for gathering, analyzing, sanitizing, and disseminating to industry private sector information related to vulnerabilities, threats, intrusions, and anomalies affecting the critical infrastructures. At the end of the NSTAC XXII cycle, the OSG concluded that the NCC already performed the primary functions of an ISAC for the telecommunications sector and that industry and Government should establish it as such.

The OSG's Y2K Subgroup investigated domestic and international Y2K preparedness and contingency planning efforts for the telecommunications infrastructure. The subgroup held a number of informational meetings with Government representatives to address ongoing Y2K readiness and contingency planning efforts. To understand public concerns about the Y2K problem, the Y2K Subgroup also investigated the initiatives of grassroots Y2K community forums and those groups promulgating "doomsday" scenarios. The subgroup's findings are included in the OSG's June 1999 NSTAC XXII report.

Based on that report, the NSTAC recommended that the President:

- Direct the President's Council on Y2K Conversion and the Federal Government continue providing timely, meaningful, and accurate Y2K readiness and contingency planning information related to the information and communications critical infrastructures to State and local governments, thereby enhancing the flow of information to the general public and community Y2K groups.

Actions Resulting from NSTAC Recommendations

The NSTAC's support for the evolving role of the NCC helped pave the way for the establishment of the NCC as an ISAC for telecommunications under the provisions of PDD-63. During 1997, the NSTAC advocated and later endorsed the NCC's

implementation of an electronic intrusion incident reporting capability based on voluntary reporting by industry and Government. In January 2000, the National Security Council agreed with the NSTAC's 1999 conclusion that the NCC was performing the primary functions of an ISAC. In March 2000, the NCC formally achieved initial operating capability as an ISAC for the telecommunications sector.

Following the October 21, 2004, Principals Conference Call, the NSTAC formed the National Coordinating Center Task Force (NCCTF) to examine the future mission and role of the NCC. Please see the NCCTF section in the Active Issues section of this *NSTAC Issue Review* for further information.

Reports Issued

Operations Support Group Report, December 1997.

Information Assurance: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group, December 1997.

Operations Support Group Report, September 1998.

Operations Support Group Report, June 1999.

Industry Information Security

Investigation Group / *Period of Activity*

Industry Information Security (IIS) Task Force
August 1986 – September 1988

Issue Background

Based on widespread concern within the Government regarding the protection of sensitive but unclassified information, the President requested that the NSTAC identify initiatives that would facilitate the protection of sensitive information processing systems. On August 19, 1986, the NSTAC IES established the IIS Task Force to develop industry's perspective on the issue. The original IIS Task Force defined and identified sensitive information categories, the relationship between telecommunications and automated information systems, an analysis methodology, and areas for further investigation. The IES then established a follow-on IIS Task Force to improve information security in telecommunications and automated information systems. The IIS Task Force submitted its final report to the NSTAC on September 22, 1988. It contained 10 conclusions and eight recommendations. The NSTAC approved the report and forwarded it to the President.

History of NSTAC Actions and Recommendations

On September 22, 1988, the NSTAC approved the IIS Task Force final report and forwarded it to the President.

Actions Resulting from NSTAC Recommendations

The NSA continued and expanded the Protected Communication Zone program. NSA developed standardized encryption modules for terminal unit platforms and reendorsed the Data Encryption Standard algorithm. Federal agencies continued the information security education program.

Reports Issued

The IIS Task Force Report, Volume I, November 1986.

The IIS Task Force Report, Volume II, Appendices, November 1986.

Status Report of the IIS Task Force, October 1987.

Final Report of the IIS Task Force—Industry Information Protection, Volume I, June 1988.

Final Report of the IIS Task Force—Industry Information Protection, Volume II, Appendices, June 1988.

Final Report of the IIS Task Force Industry Information Protection, Volume III, Annotated Bibliography, June 1988.

Information Assurance

Investigation Group / *Period of Activity*

Information Assurance Task Force (IATF)
May 1995 – April 1997

Information Infrastructure Group (IIG)
April 1997 – September 1999

Financial Services Task Force (FSTF)
March 2003 – April 2004

Issue Background

At the NSTAC XVII Meeting, the Director of the National Security Agency briefed the NSTAC Principals on threats to U.S. infrastructures. In the ensuing months, the NSTAC's Issues Group sponsored a number of meetings with representatives from the national security community, law enforcement, and civil departments and agencies to discuss information warfare (defensive) and IA issues. At the May 15, 1995, IES Working Session, the members approved establishing the IATF to serve as a focal point for IA issues. More specifically, the IES charged the IATF to cooperate with the U.S. Government to identify critical national infrastructures and their importance to the national interest, schedule elements for assessment, and propose IA policy recommendations to the President.

The IATF worked closely with industry and Government representatives to identify critical national infrastructures and ultimately selected three for study: electric power, financial services, and transportation. To address the distinctive characteristics of those infrastructures, the IATF established three risk assessment subgroups to examine each infrastructure's dependence on information technology and the associated IA risks to its information systems. Following NSTAC XIX, the IES renamed the IATF the IIG and gave it the mission to continue acting as the focal point for NSTAC IA and CIP issues.

In investigating IA/CIP issues, the IIG worked closely with the President's Commission on Critical Infrastructure Protection and other Federal organizations concerned with examining physical and cyber threats to the Nation's critical infrastructures. Federal efforts in this arena culminated with the release of presidential policy guidance—PDD 63, *Critical Infrastructure Protection,* May 22, 1998. Subsequently, PDD-63 implementation became a focal point for the IIG's activities.

History of NSTAC Actions and Recommendations

The IATF's Electric Power Risk Assessment Subgroup completed its IA risk assessment report in preparation for the March 1997 NSTAC XIX Meeting. In compiling information for this report, the Electric Power Risk Assessment Subgroup met with representatives from eight electric utilities, two industry associations, an electric power pool, equipment manufacturers, and numerous industry consultants. Based on these interviews, the subgroup assessed the extent to which the infrastructure depends on information systems and how associated vulnerabilities placed the electric power industry at increased risk to denial-of-service attacks. Based on the subgroup's findings, the NSTAC recommended that the President:

- Assign the appropriate department or agency to develop and conduct an ongoing program within the electric power industry to increase the awareness of vulnerabilities and available or emerging solutions;
- Establish an NSTAC-like advisory committee to enhance industry/Government cooperation regarding regulatory changes affecting electric power; and
- Provide threat information and consider providing incentives for industry to work with Government to develop and deploy appropriate security features for the electric power industry.

The IIG's Financial Services Risk Assessment Subgroup submitted its final recommendations in a report to NSTAC XX in December 1997. In compiling

information for this report, the Financial Services Risk Assessment Subgroup conducted confidential interviews with institutions representing money center banks, securities credit firms, credit card associations, third-party processors, industry utilities, industry associations, and Federal regulatory agencies responsible for industry oversight. The subgroup found that industry organizations treated security measures as fundamental risk controls—that a system of independent, mutually reinforcing checks and balances within critical systems and networks was unique to the financial services industry, providing a high level of integrity. The subgroup concluded that at the national level the industry was sufficiently protected and prepared to address a range of threats. However, the subgroup identified security implications and potential vulnerabilities associated with the industry's dependence on the telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from mergers and acquisitions, and the introduction of Web-based financial services. Based on the *Financial Services Risk Assessment Report,* the NSTAC recommended that the President:

- Assign to the appropriate department or agency the mission of identifying external threats and risk mitigation to the financial services infrastructure, facilitating the sharing of information between industry and Government;
- Assign the appropriate department or agency the task of working with the private sector to develop a mutually agreeable solution for effective background investigations for sensitive positions;
- Assign the appropriate department or agency the task of monitoring the new/emerging areas of electronic money and commerce, including new payment services; and
- Ensure that the NSTAC continues to have at least one member from the financial services industry.

The IIG's Transportation Risk Assessment Subgroup sponsored a workshop on September 10, 1997, to discuss the transportation information infrastructure. Topics included intermodal information dependencies, industry/Government information sharing, transportation information infrastructure vulnerabilities, and Government understanding of the transportation industry's information infrastructure vulnerabilities. The workshop, held at Fort McPherson, Georgia, included representatives from many major transportation companies, including airlines, multimodal carriers, rail, highway, mass transit, and maritime. The subgroup documented its findings in an *Interim Transportation Information Risk Assessment Report* to NSTAC XX in December 1997.

The IIG continued to investigate transportation information infrastructure issues through the NSTAC XXII cycle. As part of that effort, the IIG worked with Department of Transportation representatives to conduct outreach meetings with transportation industry associations to better understand intermodal transportation trends. The IIG also hosted another workshop on March 3 and 4, 1999, in Tampa, Florida, which included representation from each transportation sector. Participants discussed industry trends, including increased reliance on information technology and the rapid growth of intermodal transportation. Workshop findings were categorized into four areas:

(1) threats and deterrents, (2) vulnerabilities, (3) protection measures, and (4) infrastructure-wide issues. Based on the IIG's final *Transportation Risk Assessment Report,* the NSTAC recommended that the President:

- Continue support for the efforts of the Department of Transportation to promote outreach and awareness within the transportation infrastructure as expressed in PDD-63, *Critical Infrastructure Protection.*

As part of the above recommendation, the NSTAC specifically recommended that the President and the Administration ensure support for the following activities:

- Timely dissemination of Government information on physical and cyber threats to the transportation industry;

- Government research and development programs to design infrastructure assurance tools and techniques to counter emerging cyber threats to the transportation information infrastructure;

- Industry/Government efforts to examine emerging industry-wide vulnerabilities such as those related to the Global Positioning System; and

- Future Department of Transportation conferences to simulate intermodal and, where appropriate, inter-infrastructure information exchange on threats, vulnerabilities, and best practices.

Following NSTAC XX, the IIG formed an Electronic Commerce (EC)/Cyber Security Subgroup to address two issues: the short-term, technical, and time-sensitive issue relating to cyber security training and forensics; and the long-term, policy oriented, high-level issue of the NS/EP implications of EC. In addressing the short-term issue, the subgroup found that industry and Government needed a stronger partnership to establish appropriate levels of trust and understanding and to foster cooperation in addressing cyber security issues. At the September 1998 NSTAC XXI meeting, the NSTAC approved the subgroup's study paper along with the IIG report and made the following recommendation:

- The President should direct the appropriate departments and agencies to continue working with the NSTAC to develop policies, procedures, techniques, and tools to facilitate industry/Government cooperation on cyber security.

To address the long-term issue, the IIG continued to investigate the NS/EP implications associated with the adoption of EC within industry and Government. The group focused its efforts on issues associated with the changing business and security processes and policies necessary to implement EC. The IIG's conclusions and recommendations were included in its June 1999 report to NSTAC XXII. Based on that report, the NSTAC recommended that the President:

- In accordance with responsibilities and existing mechanisms established by E.O. 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, designate a focal point for examining the NS/EP issues related to widespread adoption of EC within the Government; and

- Direct Federal departments and agencies, in cooperation with an established Federal focal point, to assess the effect of EC technologies on their NS/EP operations.

At the NSTAC XXI Executive Session, the U.S. Attorney General requested that the NSTAC and the DOJ work together to address cyber security and crime. The IES determined that the projects DOJ suggested should not be addressed by the NSTAC at large but agreed that the NSTAC could help facilitate a partnership between the DOJ and individual corporations.

This agreement resulted in a meeting on March 5, 1999, between the NSTAC chair and the Attorney General where they discussed the possibilities for industry and Government participation on mutually beneficial projects. These efforts ultimately resulted in DOJ's Cyber Citizen program.

Building on past NSTAC efforts in addressing IA and CIP issues, the IIG continued to coordinate with Federal officials responsible for PDD-63 implementation during the NSTAC XXII cycle. Specifically, in accordance with the PDD-63 emphasis on public-private partnerships, IIG members focused on sharing the lessons and successes of NSTAC and offering it as a possible model for other infrastructures.

Actions Resulting from NSTAC Recommendations

NSTAC advice to the President and the Administration has had significant applicability to PDD-63 implementation. PDD-63 directs Federal

lead agencies to identify infrastructure sector coordinators within industry to provide perspective on CIP programs. At NSTAC XXI in September 1998, the NSTAC concluded that more than one entity or sector coordinator would be required to represent the diverse information and communications sector. In February 1999, following IES outreach to the Administration on the issue, the Department of Commerce acted in concert with NSTAC advice and selected three industry associations to serve as sector coordinators for the information and communications sector.

PDD-63 also calls for the private sector to explore the feasibility of establishing one or multiple ISAC. On the basis of the December 1997 NSTAC recommendation regarding a cross-infrastructure National Coordinating Mechanism, IES representatives engaged in a dialogue with senior Administration officials on the prospects of creating multiple infrastructure-based ISACs. That dialogue was important to the eventual decision to establish the National Coordinating Center for Telecommunications as an ISAC for telecommunications.

Finally, PDD-63 emphasizes the importance of relying on nonregulatory solutions to address infrastructure vulnerabilities. In satisfying this objective, the Administration underscored the value of promoting industry standards and best practices to improve IA. That approach is consistent with and follows on the December 1997 NSTAC XX recommendation regarding the creation of a private sector Information Systems Security Board.

Reports Issued

Information Assurance Task Force Report, March 1997.

Electric Power Information Assurance Risk Assessment Report, March 1997.

Information Infrastructure Group Report, December 1997.

Financial Services Risk Assessment Report, December 1997.

Interim Transportation Information Risk Assessment Report, December 1997.

Cyber Crime Point Paper, December 1997.

Information Infrastructure Group Report, September 1998.

Cyber Security Training and Forensics Issue Paper, September 1998.

Information Infrastructure Group Report, June 1999.

Transportation Information Infrastructure Risk Assessment Report, June 1999.

Report on NS/EP Implications of Electronic Commerce, June 1999.

Information Sharing/Critical Infrastructure Protection

Investigation Group / *Period of Activity*

Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF)
September 1999 – March 2002

National Plan to Defend Critical Infrastructures Task Force (NPTF)
June 2001 – September 2001

Issue Background

In investigating Information Assurance issues, the NSTAC worked closely with the President's Commission on Critical Infrastructure Protection and other Federal organizations concerned with examining physical and cyber threats to the Nation's critical infrastructures. Federal efforts in this arena culminated with the release of presidential policy guidance—Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection,* May 22, 1998. Subsequently, PDD-63 implementation became a focal point for NSTAC activities.

Following a reevaluation of NSTAC subgroups in September 1999, the IES created the IS/CIPTF to address information sharing issues associated with critical infrastructure protection (CIP). Specifically, the IES directed the task force to, among other things, continue interaction with Government leaders responsible for PDD-63 implementation, and examine mechanisms and processes for protected, operational information sharing that would help achieve the goals of PDD-63.

At NSTAC XXIV, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism requested the NSTAC's assistance in developing the Administration's *National Plan for Critical Infrastructure Protection.* The NSTAC's IES established the NPTF to draft a response to the National Coordinator's request. Subsequently, NPTF leadership met with National Security Council and Critical Infrastructure Assurance Office (CIAO) staff to discuss approaches for providing input to the national plan. The chosen approach focused on providing input on capabilities for national information sharing, analysis, and dissemination to counter cyber threats.

History of NSTAC Actions and Recommendations

Building on outreach work conducted by the NSTAC Information Infrastructure Group during the NSTAC XXII cycle (see the Information Assurance section in this *NSTAC Issue Review*), the IS/CIPTF continued to provide input to the Director, CIAO, on the *National Plan for Information Systems Protection (Version 1.0).* This plan was the first major element of a more comprehensive effort by the Federal Government to protect and defend the Nation against cyber vulnerabilities and disruptions. The IS/CIPTF members shared industry concerns and developed a dialogue with the Government that helped to shape the plan. In its May 2000 report to NSTAC XXIII, the IS/CIPTF provided NSTAC-recommended input to the plan regarding the National Coordinating Center for Telecommunications (NCC) as the Information Sharing and Analysis Center (ISAC) for the telecommunications industry.

In parallel with its work associated with the *National Plan for Information Systems Protection (Version 1.0),* and as part of continuous efforts to share NSTAC expertise with industry and Government, the IS/CIPTF monitored the development of the Partnership for Critical Infrastructure Security. The Partnership is an industry/Government effort to raise awareness about critical infrastructure security and facilitates industry participation in the national process to address CIP. Through individual NSTAC member company participation, the NSTAC shared expertise, successes, lessons learned, and experiences to further facilitate the development of the Partnership in support of PDD-63 objectives.

The IS/CIPTF also examined mechanisms and processes for protected, operational information sharing that would help achieve the goals of PDD-63 and further the role of the NCC as an ISAC for telecommunications. (See the Industry/Government Information Sharing and Response section in this *NSTAC Issue Review* for a discussion of

how the NSTAC's support for the evolving role of the NCC helped pave the way for the establishment of the NCC as an ISAC for telecommunications).

Specifically, the task force examined the NCC's historical experiences to determine how and what information is shared and the utility of information sharing for industry and Government. As part of the study, the IS/CIPTF examined the NCC's Year 2000 (Y2K) experiences for lessons learned that could benefit infrastructure protection efforts. The task force also identified benefits of information sharing to both industry and Government.

The IS/CIPTF also requested that the NSTAC's Legislative and Regulatory Working Group (LRWG) examine the *Freedom of Information Act* (FOIA) as a potential impediment to information sharing and report its findings to the task force. The LRWG's work provided the task force with the background necessary to voice industry concerns about the need for legal provisions to protect critical infrastructure protection-related information from disclosure.

The IS/CIPTF documented its findings in its report to NSTAC XIII in May 2000. The IS/CIPTF concluded that historical and Y2K experiences demonstrate information sharing to be a worthwhile effort; however, for widespread information sharing over an extended period of time to take place, legal, operational, and perceived impediments must be overcome. Based on the IS/CIPTF's report, the NSTAC recommended that the President:

- Support legislation similar to the *Y2K Information and Readiness Disclosure Act* that would protect CIP information voluntarily shared with the appropriate departments and agencies from disclosure under FOIA and limit liability.

At the May 16, 2000, NSTAC XXIII Meeting, a Government request was made for industry advice and recommendations for revision of the *National Plan for Information Systems Protection.* During the NSTAC XXIV cycle, the IS/CIPTF developed a response based on the NSTAC's experience with proven processes for industry and Government partnership at the technical, operational, and policy levels. Specifically, the task force documented NSTAC findings related to the three broad objectives of Version 1.0 of the national plan—Prepare and Prevent, Detect and Respond, and Build Strong Foundations—that should be reflected in Version 2.0 of the plan. In addition, the task force proposed that a new broad objective—International Considerations—be included in the plan's Version 2.0. The NSTAC approved the response, and forwarded it to the President. This information was also shared with the Information and Communications (I&C) Sector Coordinators: the U.S. Telecom Association, the Telecommunications Industry Association, and the Information Technology Association of America; and the I&C Sector Liaison, NTIA. The information was subsequently included in the I&C Sector Report that NTIA forwarded it to the President in April 2001.

During the NSTAC XXIV cycle, the IS/CIPTF also continued to address barriers to sharing CIP-related information, including possible law enforcement restrictions on industry sharing network intrusion data with ISACs or similar information sharing forums. The task force requested that the NSTAC and Government Network Security and Information Exchanges (NSIE) assist in investigating this issue.

The NSTAC NSIE representatives reported that, historically, they had not discussed intrusions into their networks and systems with anyone else after reporting them to law enforcement because case agents had told them that doing so might compromise the investigation of their cases. In working with the Department of Justice, the NSIEs found that although common practice discourages victims of such crimes from sharing information, no laws or policies prohibit victims from discussing crimes against them even after they have reported them to law enforcement. To address the situation, the Chief, Computer Crime and Intellectual Property Section, Department of Justice, agreed to work with the law enforcement community to implement policies that encourage victims to share such information, and to educate victims on those policies. The NSIEs concluded that it would be necessary for the private sector to ensure that personnel

interacting with law enforcement on such cases are aware that they are permitted and encouraged to share this information for network security purposes using appropriate mechanisms.

At the June 6, 2001, NSTAC XXIV meeting, the National Coordinator requested the NSTAC's assistance in developing the Bush Administration's *National Plan for Critical Infrastructure Assurance*. At that meeting, Federal officials also briefed a new national initiative for information sharing and dissemination, the Cyber Warning Information Network (CWIN), to the NSTAC as part of the discussion on national information sharing capabilities. The IES formed the NPTF to discuss the proposed CWIN and develop further input to the national plan. The NPTF held discussions with members of the Government's CWIN Working Group to gain a better understanding of the CWIN initiative. The NSTAC input to the national plan—based on the NPTF work—included an industry-based assessment of a national information sharing, analysis, and dissemination capability for addressing "cyber crises." The assessment considered CWIN as a part of that larger national capability.

The NSTAC's input focused on the need for a recognized, authoritative, national-level capability to disseminate warnings and facilitate response and mitigation efforts for cyber crises across the Nation's infrastructures. The NSTAC also concluded that key elements of such a capability spanning public and private sectors should include information collection and sharing, information analysis, dissemination of alerts and warnings, and post-event analysis.

The NSTAC recognized that conceptualizing the architecture for a national capability for addressing cyber crises is a complex undertaking. Before a national capability can become fully operational, industry and Government must address—individually and in collaboration—numerous policy, legal, financial, operational, and technical issues. Nevertheless, the NSTAC clearly determined that the ISACs should be leveraged by both industry and Government in building such a national capability and should serve as the Government's primary means of interface with industry. In addition, the NSTAC determined that industry and Government should develop communications mechanisms to link the ISACs to each other as well as with Government. The NSTAC also found that infrastructures should consider alternative means for communicating during emergencies as appropriate to the sector. For example, the telecommunications industry developed an alerting and coordination mechanism, which connects key elements of the sector and provides reliable and survivable communications in the event other communications mechanisms are unavailable or requirements warrant its use. The NSTAC forwarded its report containing input on the national plan to the President in November 2001.

Reports Issued

Information Sharing/Critical Infrastructure Protection Task Force Report, May 2000.

The NSTAC's Response to the National Plan, April 2001.

Information Sharing for Critical Infrastructure Protection Task Force Report, June 2001.

The NSTAC's Input to the National Plan: An Assessment of Industry's Role in National Level Information Sharing, Analysis, and Dissemination Capabilities for Addressing Cyber Crises, November 2001.

Intelligent Networks

Investigation Group / *Period of Activity*

Intelligent Networks (IN) Task Force
August 1989 – October 1991

Issue Background

The Telecommunications System Survivability Task Force selected IN as one of five study topics focused on determining the effect of new technologies on telecommunications systems survivability. In June 1989, the NSTAC charged the IES with continuing the intelligent network effort on an interim basis pending review by the IES PWG. Upon PWG recommendation that intelligent networks become a full task force, the IES established the IN Task Force in August 1989.

NSTAC XI extended the activities of the IN Task Force until NSTAC XII, December 13, 1990. To meet its charge, the task force worked with the OMNCS to derive a set of desired NS/EP user features and compared them with intelligent network services. The task force determined the advantages and disadvantages of identified intelligent network services for NS/EP telecommunications, including interoperability considerations. The IES extended the IN Task Force until NSTAC XIII to allow the OWG to work with the task force and the OMNCS to refine the recommendations in the task force final report.

The IN Task Force presented its final report and recommendations at the November 1990 IES meeting. The IES referred the report to the IES OWG for evaluation. The OWG's New Technology Panel developed an executive report on INs in response to the IES charge to evaluate and refine the conclusions and recommendations of the *IN Task Force Final Report.* NSTAC XIII directed the IES to disband the IN Task Force. In its Executive Report to the President, NSTAC offered to provide additional support to assist the Government in meeting the challenges of intelligent networks.

History of NSTAC Actions and Recommendations

At NSTAC XIII, October 3, 1991, the NSTAC approved the following recommendation to the President in the IES *Executive Report on Intelligent Networks:*

- The Government should establish an IN Program Office to ensure advantages of evolving intelligent networks are incorporated into planning for and procurement of Government NS/EP telecommunications.

Actions Resulting from NSTAC Recommendations

The OMNCS established an Advanced Intelligent Networks (AIN) Program Office in its Office of Plans and Programs. The primary objectives of the AIN Program Office are to:

- Identify AIN service needs for NS/EP telecommunications;
- Determine the current status and planned capabilities of AIN technology;
- Demonstrate AIN capabilities supporting NS/EP requirements;
- Assess the status of AIN standards activities; and
- Develop and implement a strategy for influencing the direction of AIN standards.

The AIN Program Office awarded a 5-year AIN NS/EP contract to Bellcore to provide a mechanism for collecting IN and AIN data, analyzing new technology developments, and demonstrating AIN-based applications. By meeting those objectives and obtaining pertinent information from Bellcore, the OMNCS will help ensure NS/EP telecommunications users benefit from the evolving AIN technology.

Reports Issued

The IN Task Force Final Report: The Impact of IN on NS/EP Telecommunications, November 7, 1990.

The Industry Executive Subcommittee: Executive Report on IN, October 3, 1991.

International Diplomatic Telecommunications

Investigation Group / *Period of Activity*

International Diplomatic Telecommunications (IDT) Task Force
September 1983 – December 1984

Issue Background

National Security Decision Directive (NSDD) No. 97 stipulates that U.S. Government missions and posts overseas must have the required telecommunications facilities and services to satisfy the Nation's needs during international emergencies. The National Communications System requested that the NSTAC advise the Department of State (DOS) on the vulnerability and risks inherent in overseas leased networks and offer remedial measures. On September 27, 1983, the NSTAC IES formed the IDT Task Force to study the issue and develop recommendations.

History of NSTAC Actions and Recommendations

In April 1984, the NSTAC forwarded the following recommendations on IDT to the President:

- Review vulnerabilities and risks at overseas diplomatic posts using the guidelines established by the IDT Task Force; and
- Establish a DOS point of contact to serve the telecommunications needs of foreign missions operating in the United States.

The NSTAC also instructed the IES to assist the DOS in determining the feasibility of using telecommunications resources owned by U.S. industries to support diplomatic requirements during international emergencies.

Reports Issued

IDT Task Force Interim Report to IES, January 16, 1984.

IDT Task Force Final Report, March 15, 1984.

International National Security and Emergency Preparedness Telecommunications

Investigation Group / *Period of Activity*

Ad Hoc Group of the Industry Executive Subcommittee (IES) Plans Working Group (PWG)
July 1990 – March 1991

Issue Background

Effective worldwide communications directly influences the Nation's ability to promote its national security interests in the global arena and to meet its international responsibilities. Changes in the international environment will profoundly affect the telecommunications capabilities needed to support the U.S. NS/EP posture. Significant changes in the international telecommunications industry-Eastern European modernization, U.S. carrier involvement in other countries, and development of new technologies and international standards will also affect the means for providing the requisite capabilities.

During the last few years, the industry/Government NS/EP telecommunications planning community demonstrated increasing interest in and concern about the international dimensions of NS/EP telecommunications. After considering a variety of potential problem areas, the ad hoc group concluded that although modern telecommunications technologies are increasingly capable of supporting NS/EP needs, inadequate planning for using such technologies might impede the President's ability to effectively react to international events.

The ad hoc group recommended to the October 24, 1990, PWG meeting that it form a task force to:

- Identify and assess the biggest problem areas affecting future U.S. international NS/EP telecommunications capabilities; and
- Develop recommendations for an U.S. international NS/EP telecommunications plan of action using both Government and private sector telecommunications resources and capabilities to meet evolving U.S. international NS/EP telecommunications needs.

The PWG concluded that the ad hoc group needed to refocus the issue and directed it to review the international NS/EP telecommunications issue again with a sharper focus of the original charge. The ad hoc group met several times and presented a revised set of proposed task force charges at the March 6, 1991, PWG Meeting. The PWG concluded that an international task force was not warranted, but that the PWG Chair should send a letter to the Deputy Manager, NCS, advising of the ad hoc group's findings and gauging NSTAC's willingness to address the international issue if requested by the Government. The Deputy Manager, NCS, forwarded a copy of the PWG Chair's letter to NCS principals to convey the PWG's willingness to assist the Government in its effort to enhance overseas NS/EP communications.

Reports Issued

Ad Hoc International Group of the IES Plans Working Group, International National Security and Emergency Preparedness Telecommunications Issue, October 1990.

Last Mile Bandwidth Availability

Investigation Group / *Period of Activity*

Last Mile Bandwidth Availability Task Force (LMBATF)
January 2001 – March 2002

Issue Background

At the 23rd meeting of the President's NSTAC on May 16, 2000, the Deputy Secretary of Defense, and the Manager, NCS, addressed the inability of the Nation's military and national security organizations to obtain the timely provisioning of high-bandwidth circuits at the local level, referred to as the "last mile." Subsequently, in an October 2000 letter to the NSTAC Chair, the NCS Manager asked the NSTAC to recommend what the Government could do to expedite the provisioning of "last mile" bandwidth or mitigate the provisioning periods for such services.

After scoping the key issues in coordination with Government, the NSTAC's IES formed the LMBATF at its January 18, 2001, Working Session. The task force was to examine the root causes of the provisioning periods, how the Government might work with industry to reduce provisioning times or otherwise mitigate their effects, and what policy-based solutions could be applied to the provisioning of high-bandwidth circuits for NS/EP services. The task force included broad representation of NSTAC member companies and NCS departments and agencies. During the remainder of the NSTAC XXIV cycle, the LMBATF gathered data from both industry organizations and the Federal Government regarding their experiences with provisioning at the local level. The task force also solicited input from telecommunications service providers on the processes for provisioning at the local level and the factors affecting provisioning periods. Based on the input, the LMBATF agreed that the scope of the study should apply to non-universally available services throughout the United States, including fiber optics, T1 and T3 lines, integrated services digital network and digital subscriber line technologies.

History of NSTAC Actions and Recommendations

The LMBATF concluded its analysis of the "last mile" provisionings during the NSTAC XXV cycle and presented its findings and recommendations in the March 2002 *"Last Mile" Bandwidth Availability Task Force Report* at NSTAC XXV. The task force found that the provisioning periods for high-bandwidth services in the "last mile" are affected by a combination of complex factors, such as intricate legislative, regulatory, and economic environments; challenging site locations; and contracting policies and procedures. Furthermore, while the Telecommunications Act of 1996 sought to encourage competition, many carriers, both incumbent and competitive, are dissatisfied with the results. This, combined with a high level of marketplace uncertainty, has reduced infrastructure investment by incumbents and competitors alike.

The task force also concluded that current Government contracting arrangements also create difficulties. In many instances, contracts are only vehicles for ordering services and do not represent a firm commitment on the part of the Government to purchase a service. Because such commitments are not in place, the carrier cannot be assured of recovering its infrastructure investment. Furthermore, when the business case warrants such investment, carriers are limited by contracts' failure to list the sites to be served or the types and quantities of services to be provided. Problems also occur because Government contracts legally bind the prime contractor but make no explicit demands on subcontractors on which the prime contractor depends.

The Government is adversely affected by funding cycles that do not coincide with the time needed to obtain high-bandwidth services. Funding is not allocated until the user identifies an immediate need and obtains approval. However, the deployment of high-bandwidth infrastructure often requires years of planning and coordination for allocating capital, obtaining rights-of-way authority, and installing service facilities. The imperfect intersection of these inherently mismatched processes often results in lengthy provisioning periods.

The negative consequences of the funding process are often exacerbated by a fragmented management structure. In many cases, project managers are responsible for separate portions of the network, with no single entity responsible for planning or monitoring the provisioning of end-to-end service. Overall project management is vital to effective network deployment, systems integration, and achievement of project goals. Because telecommunications services are provided by a multitude of companies, users must track service orders and manage the network from a centralized perspective.

The task force also studied whether the TSP System can be used to expedite "last mile" provisioning requests because TSP provisioning assignments are used by the NS/EP community to facilitate the expedited installation of telecommunications circuits that otherwise could not be installed within the required time frame. Although TSP seems to be an applicable solution for many NS/EP "last mile" bandwidth requests, TSP provisioning assignments can only be applied to services originating from new business requirements. Therefore, TSP provisioning cannot be used to replace or transfer existing services, such as those associated with the contract transition. Finally, TSP cannot be used to make up for time lost because of inadequate planning or logistical difficulties. According to these parameters, many "last mile" provisioning requests are not eligible for the TSP System, even if the requested service could be used for executing an agency's NS/EP mission. An alternative for meeting Government organizations' service requirements may be the implementation of alternative technologies to fulfill bandwidth requirements on a temporary or permanent basis.

Based on this analysis, the LMBATF report recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions* and other existing authority:

- Direct the appropriate departments and agencies, in coordination with industry, to reevaluate their communications service contracting and purchasing procedures and practices and take action to:
  - Provide sufficient authority and flexibility to meet their needs, consistent with current conditions
  - Allow long lead-time ordering and funding commitments based on projected requirements
  - Allow infrastructure funding where necessary for anticipated future needs or to accelerate installation so that customer requirements can be met
  - Share or assume risk for new service capital investment to ensure timely delivery
  - Allow and provide for performance incentives for all performing parties: industry and Government, organizational and individual
  - Require end-to-end project management of communications service ordering and delivery.
- Direct the Federal Government Chief Information Officers Council to propose, and assist in implementing, improved Government contracting practices for communications services that will enhance the availability of broadband services for the "last mile."

In support of the recommendations, NSTAC *"Last Mile" Task Force Report* also suggested that both industry and Government encourage:

- Government contracting officers to engage all industry and Government representatives in joint planning sessions;
- Industry representatives to work with Government contracting officers in joint planning sessions;

- Use of a contract structure that makes all carriers involved in the delivery of the service parties to the contract with direct accountability to the Government contracting entity; and

- Contracting practices that require end users to identify requirements and to communicate future needs to network providers. End users and network providers should jointly identify complicating factors and discuss alternatives.

Finally, the NSTAC *"Last Mile" Bandwidth Availability Task Force Report* encouraged Government to:

- Establish realistic service requirements and timelines and select the service options that meet its needs with acceptable risk;

- Convene a working group consisting of industry and Government stakeholders in the provisioning process to develop and recommend a streamlined approach to all aspects of the process, including planning, ordering, and tracking. The resulting proposal should be comprehensive, simplifying steps and organizations as much as possible; should share information appropriately at all points; and should support flexibility in meeting end-user needs. The working group should give strong consideration to a single Government database to support the process and a single point of contact, such as a phone number or an e-mail address, to ensure accuracy of information and provide exception handling; and

- Establish or contract for project managers who have all necessary management control tools at their disposal; access to pertinent information; and experience, responsibility, and authority for obtaining and overseeing delivery of the end-to-end service.

The LMBATF concluded its activities upon NSTAC approval of its report.

Reports Issued

"Last Mile" Bandwidth Availability Task Force Report to NSTAC XXV, March 2002.

National Coordinating Mechanism

Investigating Group / *Period of Activity*

National Coordinating Mechanism (NCM) Task Force
December 1982 – November 1984

Issue Background

The NSTAC recognized the need to establish a mechanism for coordinating industry and Government responses to the Government's NS/EP telecommunication service requirements in the post-divestiture environment. As a result, NSTAC formed the NCM Task Force in December 1982, and charged it to identify and establish the most cost-effective mechanism to coordinate industry-wide responses to NS/EP telecommunications requests.

History of NSTAC Actions and Recommendations

The NSTAC forwarded a series of NCM recommendations to the President in 1983 and 1984. The NCC is the most significant result of these recommendations. Established on January 3, 1984, the NCC is a joint industry/Government operations center that supports the Federal Government's NS/EP telecommunication requirements.

Actions Resulting from NSTAC Recommendations

The TSS Task Force reviewed Government actions taken on the NSTAC's NCM recommendations and concluded that the NCM recommendations were carried out promptly and effectively. The task force recommended continuing NCS member organizations' representation in the NCC, and continuing Government dissemination of NS/EP information. The NSTAC approved the TSS Task Force's findings and recommendations on the NCM and forwarded them to the President on September 22, 1988.

The NCS member agencies' representation in the NCC continues, as does the Government's dissemination of NS/EP information. See the NCC Task Force section in the NSTAC XXIX Issues section, as well as the Industry/Government Coordination and Response section in this *NSTAC Issue Review* for a fuller discussion of recent NCC actions.

Reports Issued

NCM Task Force Report, May 16, 1983.

NCM Implementation Plan (Final Report), January 30, 1984.

National Information Infrastructure

Investigation Group / *Period of Activity*

National Information Infrastructure (NII) Task Force
August 1993 – March 1997

Issue Background

At the August 2, 1993, IES meeting, the Plans Working Group (subsequently reestablished as the Issues Group) recommended that a task force be established to address NS/EP telecommunications issues related to the evolution of the U.S. information infrastructure. The IES established an NII Task Force to provide a series of reports with recommendations to the President. The task force's charge was to:

- Identify, in collaboration with Government, potential dual-use applications of the NII and recommend Government actions;
- Identify potential NS/EP implications of the NII and recommend Government actions;
- As a minimum, address items identified by the Director, OSTP at NSTAC XV (for example, security, resiliency, interoperability, standards, and spectrum);
- Advise Government on technical and other considerations that will accelerate commercialization of a nationwide high speed network available to NS/EP users; and
- As a minimum, address architectural, policy, and regulatory issues, along with those research and development focus areas, pilot/demonstration projects, and civil/military telecommunications issues identified by OSTP and the National Economic Council.

The task force relied on *The National Information Infrastructure: An Agenda for Action,* released by the administration on September 15, 1993, as a guide for its work. This document called for the NSTAC to continue to offer advice to the President on NS/EP telecommunications issues, work with the Federal Communications Commission's Network Reliability Council (subsequently renamed the Network Reliability and Interoperability Council) and complement the work of the U.S. Advisory Council on the NII. To better focus on its charge and coordinate with the Information Infrastructure Task Force and its committees, the NII Task Force established three subgroups: the Policy Subgroup, the Applications Subgroup, and the Future Commercial Systems and Architecture Subgroup.

The Policy Subgroup's final report, *Approach to Security and Privacy on the NII,* summarized the findings of the subgroup in network security. It made preliminary recommendations on ways to ensure that expansion and enhancement of the information infrastructure would be compatible with telecommunications security concerns.

The Applications Subgroup assessed NII applications that the Government was developing. In doing so, the subgroup developed criteria to select applications for increased emphasis. The subgroup made a number of recommendations related to developing dual-use applications.

Additionally, the subgroup established an Emergency Health Care Information Focus Group to address health-care-specific issues for the NII. The subgroup chose this application area as a model for examining important information infrastructure application issues, such as interoperability, privacy, and security.

The final report of the Future Commercial Systems and Architecture Subgroup addressed the architectural principles and trends and NS/EP performance issues of the current and future NII. It examined the NII from the perspective of three major components: the public switched network, broadcast networks, and the Internet.

Additionally, the Issues Group addressed the information infrastructure issue, working with the OSTP to develop plans for an NII Symposium at the Naval War College (NWC), Newport, Rhode Island,

October 17 – 19, 1994. The Issues Group planned the symposium with the OSTP in response to an NWC invitation to the NSTAC to participate in a communications-focused game designed to address the NII. The NWC produced a non-attribution report for distribution to all participants, and it is available to any interested parties upon request.

History of NSTAC Actions and Recommendations

The task force presented its interim report at the NSTAC XVI Meeting on March 2, 1994. The report provides the background on the task force's establishment, its activities and future direction, and a summary that includes a proposed statement for the *NSTAC XVI Executive Report.* The statement reiterates the task force's commitment to assisting the President in ensuring it satisfies NS/EP requirements on the NII. The NSTAC approved both the report and the proposed statement for forwarding to the President.

The task force presented an *NII Task Force Status Report* at NSTAC XVII on January 12, 1995. The report discussed the work of the task force's three subgroups—the Policy Subgroup, the Applications Subgroup, and the Future Commercial Systems and Architecture Subgroup. The status report also addressed the 12 recommendations culled from the individual subgroup reports.

The task force presented its third report to NSTAC XVIII on February 28, 1996. The report included analysis and recommendations regarding three NS/EP issues: 1) the need for an NII Security Center of Excellence (SCOE), 2) the emerging GII, and 3) Emergency Health Care Information. The NSTAC approved forwarding recommendations to the President regarding the latter two issues.

Following NSTAC XVIII, the IES charged the task force to further investigate the advisability of establishing a SCOE, henceforth referred to as the Information Systems Security Board (ISSB). The task force conceptualized the ISSB as a private sector entity that would promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services. The task force developed the *ISSB Concept Paper,* which outlined the functions and processes of the ISSB and served as the centerpiece for an outreach effort undertaken to ascertain the viability of the ISSB model. After contacting more than 100 major information technology companies, industry associations, Government agencies, and major information technology users, the NII Task Force determined that there was broad support for the ISSB concept and that industry should take the lead in its formation.

The task force presented its fourth and final report at NSTAC XIX on March 18, 1997. The report focused on the ISSB initiative and the NS/EP implications of the GII. The NSTAC recommended the President endorse the private sector ISSB initiative. Lastly, the NSTAC approved a recommendation to sunset the NII Task Force.

Actions Resulting from NSTAC Recommendations

The Information Technology Industry Council (ITIC) sponsored an effort to explore formation of the ISSB; the ITIC hosted the first meeting of this group on January 21, 1997. Following the meeting, the Information Security Exploratory Committee (ISEC), a consortium of interested stakeholders, met regularly to discuss the possibility of operationalizing the ISSB concept. The ISEC issued its report in January 1998 in which it recommended that, although it supported the concept of the ISSB, studies revealed that establishment of such a board would be duplicative of private endeavors.

At the same time, however, the ISSB concept influenced the Clinton Administration's policy on implementing Presidential Decision Directive 63, *Critical Infrastructure Protection.* Specifically, in an approach consistent with the NSTAC's ISSB recommendation, the Administration's Critical Infrastructure Assurance Office underscored the value of promoting industry standards and best practices to improve infrastructure assurance.

Reports Issued

NII Task Force Interim Report, February 1994.

NII Task Force Report, January 1995.

NII Task Force Report, February 1996.

NII Task Force Report, March 1997.

National Research Council Report

Investigation Group / *Period of Activity*

National Research Council (NRC) Report Task Force
August 1989 – March 1990

Issue Background

In June 1989, the NSTAC noted that the NRC report, *Growing Vulnerability of the Public Switched Networks (PSN): Implications for National Security Emergency Preparedness,* differed from Telecommunications Systems Survivability Task Force findings. The NSTAC, therefore, charged the IES with examining those differences and reporting back in early 1990. In response, the IES formed the NRC Report Task Force and issued the following charges:

- If it agreed with the NRC report, address what actions should be taken by industry to assist the Government in implementing the NRC's recommendations;
- If it did not agree, give the reasons why and the factors bearing on the differing perspectives of the IES and the NRC; and
- Comment on the report's implications for interoperability.

The task force issued its final report in March 1990.

History of NSTAC Actions and Recommendations

In March 1990, the NSTAC approved the findings of the NRC Report Task Force. Contrary to the NRC's findings, the task force concluded the PSN was growing more survivable. This survivability stems from the increased network diversity provided by the existence of three major interexchange carriers, the increased user demand for network service availability, the deployment of robust network architectures, and the incorporation of advanced transmission, switching, and signaling technologies. The task force also noted that current technologies and competitive trends were enhancing network robustness.

Actions Resulting from NSTAC Recommendations

The NRC Report Task Force agreed with some of the recommendations of the NRC report and believed that the issue of growing vulnerabilities of the PSN needed to be further addressed. Therefore, the IES established the Network Security Task Force.

In 1991, the NRC report attracted considerable attention in Congress and at the FCC due to recurring outages of the PSN. The FCC established the Network Reliability Council on February 27, 1992, to make recommendations to the FCC on improving network reliability. The Network Reliability Council sponsored a symposium from June 10-11, 1993, in Washington, DC, on industry's best practices for avoiding and minimizing the risk and impact of future telephone network outages.

Reports Issued

NRC Report Task Force Final Report, March 1990.

National Telecommunications Management Structure

Investigation Group / *Period of Activity*

National Telecommunications Management Structure (NTMS) Task Force
August 1986 – June 1989

Issue Background

On May 22, 1986, the NSTAC concurred with the Government that there was a need for a survivable and endurable management structure to support NS/EP telecommunications requirements, and agreed that industry and Government should work jointly to develop such a capability. As a result, the NSTAC established the NTMS Task Force in August 1986 and charged it with assisting in developing an NTMS implementation plan.

History of NSTAC Actions and Recommendations

On November 6, 1987, the NSTAC forwarded to the President its recommendation to approve the *NTMS Implementation Concept.* The Executive Office of the President approved the concept on March 25, 1988. The NCS, opened the NTMS Program Office on June 17, 1988. During the week of July 12–15, 1988, the NCS conducted the NTMS trial exercise to determine the feasibility of the NTMS concept and funding requirements. The NCS successfully tested the National Telecommunications Coordinating Network concept September 27–29, 1988. The NCS completed the NTMS program plan in March 1989, and it is updated periodically. The NSTAC disbanded the NTMS Task Force on June 8, 1989.

Actions Resulting from NSTAC Recommendations

Through the NCC, industry provides advice and assistance in pursuit of NTMS operational capability.

The NCS established the COR NTMS Subcommittee to assist in achieving NTMS initial operational capability. The NTMS program became operational with the implementation of the northeast region in October 1990. In September 1991, the activation of the southwest and northwest regions provided additional capability. The subcommittee also completed NTMS regional validations in Chicago, Illinois, during November 1992; in Atlanta, Georgia, during February 1993; and in Denver, Colorado, during April 1993.

Reports Issued

NTMS Implementation Concept (Final), November 1987.

Network Convergence

Investigation Group / *Period of Activity*

Network Group (NG)
April 1997 – September 1999

Information Technology Progress Impact Task Force (ITPITF)
September 1999 – June 2000

Convergence Task Force (CTF)
June 2000 – June 2001

Network Security Vulnerability Assessments Task Force (NS/VATF)
June 2001 – March 2002

Next Generation Networks Task Force (NGNTF)
May 2004 – May 2006

Issue Background

Telecommunications carriers are implementing cost-effective packet networks to remain competitive in the evolving telecommunications marketplace and to support wide-scale delivery of diverse, advanced broadband services. However, because of their large investments in circuit switched network infrastructure, carriers are initially leveraging the best of both infrastructures, resulting in a period of network convergence during the transition to the next generation network (NGN). In this evolving network environment, the President's National Security Telecommunications Advisory Committee (NSTAC) recognizes that industry and Government must strive to identify and remedy associated network vulnerabilities to ensure sustained critical communications capabilities of the national security and emergency preparedness (NS/EP) community. Accordingly, the NSTAC established task forces to analyze various infrastructure, security, and operational vulnerabilities stemming from network convergence and to provide recommendations to mitigate the vulnerabilities.

History of NSTAC Actions and Recommendations

Following NSTAC XXII in June 1999, the Industry Executive Subcommittee (IES) created the Information Technology Progress Impact Task Force (ITPITF) to examine the potential implications of Internet Protocol (IP) network and public switched network (PSN) convergence on existing NS/EP services (such as, the Government Emergency Telecommunications Service (GETS) and the Telecommunications Service Priority (TSP)) and to prepare for a Research and Development Exchange Workshop (RDX) focusing on network convergence issues.

The ITPITF analyzed issues related to GETS functionality in IP networks. The ITPITF determined that because IP networks do not have network intelligence features analogous to Signaling System 7 (SS7), IP networks may not support activation of GETS access and transport control and features. Furthermore, without quality of service (QoS) features to enable priority handling and transport of traffic in IP networks, GETS calls may encounter new blocking sources and be subject to poor completion rates during overload conditions. The ITPITF concluded that as the NGN evolves, telecommunications carriers' SS7 networks will become less discrete and more dependent on IP technology and interfaces. Therefore, it will be necessary to consider the security, reliability, and availability of the NGN control space related to the provision and maintenance of NS/EP service capabilities.

In addition, the ITPITF analyzed potential implications of convergence on TSP services. The ITPITF concurred with the oversight committee that TSP services remained relevant in converged networks, as TSP assignments could still be applied to identifiable segments of the PSN. However, because TSP applies only to circuit switched networks, a new program may be needed to support priority restoration and provisioning in end-to-end packet networks.

The ITPITF also examined evolving network technologies and capabilities that could support NS/EP functional requirements in both converged networks and the NGN. The ITPITF concluded that

QoS and other new NGN capabilities would require some enhancement to best satisfy specific NS/EP requirements.

Based on the ITPITF's May 2000 report to NSTAC XXIII, the NSTAC recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* direct the appropriate departments and agencies, in coordination with industry, to:

- Promptly determine precise functional NS/EP requirements for convergence and the NGN; and
- Ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during NGN standards development and implementation.

Additionally, the ITPITF recommended that the NSTAC XXIV work plan include an examination of the potential NS/EP implications related to possible security and reliability vulnerabilities of the control space in the NGN.

On September 28-29, 2000, the President's NSTAC co-sponsored its fourth RDX. The event was co-sponsored by the White House Office of Science and Technology Policy (OSTP) and conducted in conjunction with the Telecommunications and Information Security Workshop 2000 held at the University of Tulsa in Tulsa, Oklahoma. The purpose was to exchange ideas among representatives from industry, Government, and academia on the challenges posed by network convergence. Discussions of convergence issues at the workshop and the RDX led to the following conclusions:

- There is a shortage of qualified information technology (IT) professionals, particularly those with expertise in information assurance and/or computer security;
- Developing a business case for security poses difficult challenges in the commercial sector, and there is a need to offset the high costs and high risks associated with R&D in security technology;
- Given the complexity and interdependence introduced to networks by convergence and the proliferation of network providers and vendors, best practices, standards, and protection profiles that help to ensure secure interoperable solutions must be evenly applied across the NGN; and
- There is a need to enhance R&D efforts to develop better testing and evaluation programs to reduce the vulnerabilities introduced by malicious software.

From these conclusions, the participants at the RDX offered several recommendations for consideration by the Government and the NSTAC. These recommendations focus on improving network security in a converged and distributed environment. Specifically, the Government should:

- Establish and continue to fund Government programs to encourage increasing the number of graduate and undergraduate students pursuing study in computer security disciplines;
- Increase the funding and support to the National Security Agency and other Government agencies to facilitate the certification of additional Information Assurance (IA) Centers of Excellence to train and educate the next generation of information technology security professionals;
- Develop tax credits and other financial incentives to encourage industry to invest more capital in the research and development of security technologies;
- Expand partnerships on critical infrastructure protection issues by encouraging more representatives from academia and State and local Governments to participate; and

- Invest in R&D programs that encourage the development of best practices in NGN security, such as improved testing and evaluation, broadband protection profiles, and NGN security standards.

To support the Government, the NSTAC should:

- Consider the issues of best practices and standards in its report to NSTAC XXIV;

- Consider the evolving standards of due care legal issues discussed at the R&D Exchange, including linked or third party liability and new privacy legislation and regulations such as the Health Insurance Portability and Accountability Act; and

- Conduct another RDX in partnership with one or more of the IA Centers of Excellence to discuss the difficulties in and strategies for both increasing the number of qualified IT security professionals and enhancing the academic curricula to meet the security challenges of the NGN.

Beginning in September 2000, the Convergence Task Force (CTF) analyzed issues related to the potential security and reliability vulnerabilities of converged networks. Based on briefings received from industry and Government representatives, the CTF concluded that the public switched telephone network (PSTN) is becomingly increasingly vulnerable as a result of its convergence with packet networks. Of particular concern to the CTF was the interoperation of the intelligent network of the PSTN with IP networks via existing gateways. The CTF noted that malicious attacks on these gateways could impact overall network availability and reliability. Members suggested that possible remedies for these vulnerabilities include signaling firewalls implemented at network gateways and embedded security capabilities defined through standards. The CTF determined that additional analysis of these security vulnerabilities is required to gain further understanding of the possible consequences of the evolving NGN. Such an analysis should include examination of the convergence of wireless data networks with the PSTN.

Furthermore, it was agreed that the NGN must offer the NS/EP community quality of service, reliability, protection, and restoration features analogous to those of the PSTN. To achieve this, the CTF suggested that Government foster strong working relationships with NGN carriers and work to specify security requirements in packet network procurements in an effort to attain network reliability commensurate with that of the PSTN.

In response to concerns expressed by prominent Government officials, the CTF also examined issues of possible single points of failure in converged networks and associated possibilities of widespread network disruptions. Through examination of related past NSTAC reports and participation in a National Coordinating Center for Telecommunications single point of failure exercise, the CTF members determined that a scenario could not be envisioned, even in the converged network environment, in which a single point of failure could cause widespread network disruption. Members found it more likely that any single points of network failure would have only local or "last mile" impacts. However, the CTF concluded that unforeseen points of failure precluded definitive assertions regarding the implausibility of a national level network failure. The CTF also found that converged network vulnerabilities and possible points of failure could impact service availability and reliability essential to NS/EP operations rather than creating network component failures. Members suggested sharing detailed network data among industry, Government, and academia was needed to further understand converging networks and achieve more accurate network modeling and simulation techniques to analyze vulnerabilities and their impacts.

The CTF also examined the ongoing standards development efforts supporting NS/EP priority requirements in the converged network. Group members concluded that, as the NGN evolves to offer more advanced broadband services, the Government must remain actively involved in the relevant standards bodies' activities to help define and ensure the consideration of NS/EP requirements in the IP environment. The CTF further encouraged the Government to remain actively involved in

working group activities related to NS/EP issues including the Internet Engineering Task Force and the International Telecommunications Union.

Based on the CTF's June 2001 report to NSTAC XXIV, the NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry, to:

- Specify network security, service level, and assurance requirements in contracts to help ensure reliability and availability of NS/EP communications during network convergence and in the developing NGN;
- Ensure that standards bodies consider NS/EP communications functional requirements during their work addressing network convergence issues, including security of PSTN-IP network SS7 control traffic and development of packet network priority services;
- Plan and participate in additional exercises examining possible vulnerabilities in the emerging public network (PN) and subsequent NS/EP implications on a national and international basis; and
- Utilize the Telecom-ISAC to facilitate the process of sharing network data and vulnerabilities to develop suitable mitigation strategies to reduce risks.

Additionally, the CTF recommended that the NSTAC XXV work plan include the following tasks:

- Examine the NS/EP security and reliability implications of the convergence of wireless data networks with the PSTN and traditional wireless networks;
- Support the efforts of the Government Subgroup on Convergence as requested by the Government in accordance with NSTAC's charter; and
- Further examine converged network control space-related vulnerabilities, including those of signaling and media gateways, and analyze possible NS/EP implications.

Following NSTAC XXIV in May 2001, the IES formed the Network Security/Vulnerability Assessments Task Force (NS/VATF) and charged the group to address public network policy and technical issues related to:

- Network disruptions, particularly distributed denial of service (DDoS) attacks;
- Security and vulnerability of the converged network control space, including wireless, network simulation and testing, standards, and consequence management issues; and
- Needed countermeasures (*e.g.,* functional requirements) to address the issues above.

The NS/VATF noted that the September 11, 2001, terrorist attacks on the World Trade Center and the Pentagon have renewed concerns regarding physical threats to the PN. While the telecommunications infrastructure had not been a direct target of terrorism, it could be in the future. Therefore, the NS/VATF concluded that Federal, State, and local Government assistance related to preventing, mitigating, and responding to such an occurrence should be coordinated through the Telecom-ISAC. In addition to the enduring physical threat to the Nation's networks, the NS/VATF concluded that cyber attacks present a growing threat to the security of U.S. information systems and, consequently, to the critical communications of the NS/EP community. As cyber network attack techniques increase in sophistication and intruders continue using DDoS techniques to exploit vulnerabilities, cyber attacks will likely cause greater collateral impacts to NS/EP communications. Because of this threat environment, the NS/VATF concluded that industry and Government should continue participating in ISACs to develop and implement unified and centralized capabilities to respond to attacks as they are occurring.

The NS/VATF also concluded that additional steps are necessary to enhance the security of the control space of the evolving PN. As network convergence continues, malicious attacks focusing on the network control space are increasingly feasible; therefore, industry and Government cooperation is necessary to address control space vulnerabilities and implement remedial tools. The NS/VATF also encouraged industry and Government support of the NSIE efforts to develop a cross-industry security posture that could help provide a foundation for protecting the control space of the emerging PN.

The NS/VATF also expressed concern about security issues affecting NS/EP communications transiting wireless networks and technologies, including the security of the interoperation of wireless and wireline networks—and, more specifically, activities addressing the wireless access protocol.

The task force also concluded that Government should deploy wireless local area networks with higher levels of security and consider policies that would reduce the risks of using personal area network devices.

On the basis of its analysis, the NS/VATF stated that some of the best strategies for countering vulnerabilities of the critical telecommunications infrastructure involved:

- Increasing Government participation in standards bodies, and developing a coordinated Government-wide approach to standards development;
- Specifying security standards in contracts and purchase orders. This process would result in more commercial off-the-shelf products and services, which the Government can then procure at reduced cost; and
- Increasing stakeholder awareness of cyber vulnerabilities and mitigation strategies, including strong cyber security and response plans.

The NS/VATF concluded that the PN and its services supporting NS/EP users would continue to be at risk from increasingly technologically sophisticated, well-coordinated threat sources. Therefore, industry and Government must continue to work together to devise countermeasures and strategies to help mitigate the impacts of physical and cyber attacks on the PN and other critical infrastructures.

Based on the NS/VATF's March 2002 report to NSTAC XXV, the NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry to:

- Coordinate and prioritize through the Telecom-ISAC, Government assistance to industry to protect the Nation's critical communications assets and to mitigate the effects of an attack as it is occurring;
- Encourage and adequately support the development and adoption of baseline standards and technologies including version 6, Internet Protocol Security, and the Emergency Telecommunications Service scheme, to help bolster core security and reliability of the NGN;
- Support the NSIEs' efforts to develop a cross-industry security posture that could help provide a foundation for containing the control space of the emerging public network;
- Work with standards bodies to ensure consideration of NS/EP communications functional requirements while addressing the security of the interoperation of wireless and wireline networks, and more specifically, activities addressing wireless access protocol;
- Ensure that all wireless local area networks used by the Government meet the highest level of security standards available, with priority given to those supporting NS/EP missions; and
- Develop policies and procedures to support the use of personal area network devices while reducing their risk of compromise.

Following the NSTAC XXVII Meeting held on May 19, 2004, the NSTAC Principals created the Next Generation Networks Task Force (NGNTF), to conduct an examination of NS/EP requirements and emerging threats on the NGN. As an initial step, the NGNTF assembled a group of subject matter experts (SMEs) and government stakeholders in August 2004 to determine how best to meet the task's significant objectives. As a result of the meeting, the group identified five fundamental areas of examination: (1) NGN description; (2) NGN service scenarios and user requirements; (3) end-to-end services provisioning; (4) NGN threats and vulnerabilities; and (5) incident management on the NGN. In response to government stakeholder questions during the meeting, the NGNTF agreed to undertake a quick turn around report on the near term actions that could be undertaken to reduce the impact of network transition issues on NS/EP communications and to identify areas where immediate government involvement was needed to foster activities in areas such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs.

Based on the near-term analysis conducted by the NGNTF, the Committee offered the following recommendations to the President in March 2005:

- Use existing and appropriate cross-Government coordination mechanisms to track and coordinate cross-agency NGN activities and investment;
- Explore the use of Government [civilian and Department of Defense (DOD)] networks as alternatives for critical NS/EP communications during times of national crisis;
- Use and test existing and leading-edge technologies and commercial capabilities to support NS/EP user requirements for security and availability;
- Support the development and use of identity management mechanisms, including strong authentication;
- Study and support industry efforts in areas that present the greatest NS/EP risks during the period of convergence, including gateways, control systems, and first responder communications systems;
- Review the value of satellite systems as a broad alternative transmission channel for NS/EP communications;
- Participate more broadly and actively in the NGN standards process in partnership with the private sector in the following areas: web services, directory services, data security, network security/management, and control systems; and
- Focus on developing cohesive domestic and international NS/EP communications policy and conduct inter-governmental discussions on NS/EP communications.

The NGNTF then turned its attention to the longer-term taskings, leveraging significant involvement from industry and government SMEs involved in the day-to-day transition of the NGN and creating working groups to address each issue area. Ultimately, the NSTAC, based upon the work of the NGNTF, agreed upon nine recommendations, the implementation of which they believed would support the ability of the NGN to meet NS/EP functional requirements while also providing greater capabilities to NS/EP users.

The NSTAC Principals approved the following recommendations to the President in March 2006:

- **Identity Management.** Direct the Office of Management and Budget (OMB), the Department of Commerce (DOC), and the Department of Homeland Security (DHS) to work with the private sector in partnership to build a federated, interoperable, survivable, and effective identity management framework for the NGN that: (1) includes a common assurance taxonomy that addresses NS/EP requirements and is usable in both the Government and commercial domains; (2) minimizes identity "silos" (identity stores containing usernames and passwords that is not

or cannot be used by another applications), allows federation between the Government and commercial domains, and supports use of Government issued credentials for identification on the NGN; (3) meets other NS/EP requirements, including priority access to NS/EP communications services; (4) supports broad use of commercial technology, along with existing and emerging protocols and standards; and (5) includes explicit protections for privacy.

- **Coordination on Common Operational Criteria for NGN NS/EP End-to-End Services.** Direct the Office of Science and Technology (OSTP), with support from the collective National Communications System (NCS) agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology (IT) industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor programs that would foster NS/EP capabilities within the NGN, including initiatives concerning:

  - A priority regime for both encrypted and unencrypted packets supported by a set of standards specifying how that priority is to be translated end to end among the different networks connected to the NGN, consistent with a user's NS/EP authorization and required class of service; and

  - NGN designs that respond to NS/EP requirements, including supporting a mixed protocol operational environment during the transition into IP version 6; peer-to-peer networks and systems for independence from centralized infrastructure; meshed networks for resiliency and deployability; and IP Security for authentication and confidentiality.

- **Research and Development (R&D).** In support of the prior recommendation, direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, the National Institute of Standards and Technology (NIST), and DOD to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/ IT and service providers.

- **Technology Lifecycle Assurance and Trusted Technology.** Direct OMB, OSTP, DOD, DHS, and DOC to drive comprehensive change in the security of NS/EP information and communications technology through policy, incentives, and research supporting the development and use of: (1) technology lifecycle assurance mechanisms; and (2) innovative trusted technologies that reduce the presence of intrinsic vulnerabilities.

- **Resilient Alternate Communications.** Direct OMB and DHS, in accordance with their respective authorities, to ensure that Federal agencies are developing, investing in, and maintaining resilient, alternate communications for the NGN environment. Specifically, DHS and OMB should require that NS/EP communicators, including incident managers and emergency responders, plan for communications resiliency especially by examining alternative or substitute access methods to the NGN to address specific threat scenarios, which methods can augment and possibly replace, at least temporarily, damaged or diminished access to the communications infrastructure.

- **Agreements, Standards, Policy, and Regulations.** Direct DHS, the Department of State, and DOC (including NIST and the National Telecommunications and Information Administration) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP

capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally-distributed NGN environment.

- **Incident Management on the NGN.** Direct DHS to establish an inclusive and effective NGN incident response capability that includes a Joint Coordination Center, incorporating and modeled on the National Coordinating Center (NCC), for all key sectors, but particularly both the Communications and IT Sectors, and supporting mechanisms such as a training academy and a collaboratively developed, broadly participatory, and regularly evaluated exercise program. This capability should be enhanced by an appropriate R&D program.

- **International Policy.** Direct departments and agencies to develop cohesive domestic and international NS/EP communications policy consistent with the recommendations in this report, in particular: (1) developing intergovernmental cooperative mechanisms to harmonize NS/EP policy regimes in participating countries consistent with the recommendations in this report; (2) establishing the rules of engagement for non-United States (U.S.) companies in NS/EP incident response in the U.S. and (3) addressing how information sharing and response mechanisms should operate in the international NGN environment.

- **First Responders.** Direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems.

Actions Resulting from NSTAC Recommendations

Based on NSTAC recommendations, the NCS is actively participating in various standards bodies to ensure consideration of NS/EP functional requirements during convergence and in the NGN. The NCS is contributing to activities of the European Telecommunications Standards Institute, Telecommunications and Internet Protocol Harmonization over Networks (ETSI TIPHON) group. ETSI TIPHON is examining several security issues related to convergence, including identification and authentication procedures for emergency calls, and issues related to cyber attacks and malicious intrusion into networks.

The NCS is also active in International Telecommunication Union Standardization Sector efforts regarding recommendation E.106, Description of the International Emergency Preference Scheme (IEPS). IEPS recognizes the requirement for priority communications among Government, civil, and other essential users of public telecommunications services in crisis situations. IEPS, which is similar to GETS, would give authorized users priority access to and transport of NS/EP-related calls on an international basis within the PSTN and integrated services digital network infrastructures.

Citing findings of the ITPITF, on March 9, 2001, the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism established, in conjunction with OSTP, an interagency Convergence subgroup under the Counter Terrorism and National Preparedness Information Infrastructure Protection Assurance Group. The purpose of this Convergence Working Group (CWG) was to address issues associated with the convergence of the voice and data networks and the implications of this convergence on NS/EP telecommunications services. The associated policy, legal, security, and technical issues were previously identified in a Report of the CTF, dated December 29, 2000. The CWG issued its final report on February 14, 2002.

Additionally, the NCS developed a route diversity methodology to help Federal departments and agencies to assess critical infrastructure communications resiliency.

Following the NSTAC XXIX Meeting held on May 9, 2006, the NSTAC established the International Task Force (ITF), to conduct an examination of the NS/EP implications of international communications. (See the International Communications section in the Active Issues section of this *NSTAC Issue Review.*)

Reports Issued

Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies, June 1999.

Information Technology Progress Impact Task Force Report on Convergence, May 2000.

Research and Development Exchange Proceedings: Transparent Security in a Converged Network Environment, September 2000.

Convergence Task Force Report, June 2001.

Network Security Vulnerability Assessments Task Force Report, March 2002.

Next Generation Networks Task Force Report: Near Term Recommendations, March 2005.

Next Generation Networks Task Force Report, March 2006.

Network Security

Investigation Group / *Period of Activity*

Network Security Task Force (NSTF)
February 1990 – August 1992

Network Security Information Exchange (NSIE)
June 2001 – Present

Network Security Standards Oversight Group (NSSOG)
August 1992 – January 1995

Network Security Steering Committee (NSSC)
August 1992 – December 1994

Network Security Group (NSG)
December 1994 – April 1997

Network Group (NG)
April 1997 – September 1999

Embedded Interoperable Security Issue Scoping Group (EISISG)
June 1999 – November 1999

Protecting Systems Task Force (PSTF)
September 1999 – May 2000

Internet Security/Architecture Task Force (IS/ATF)
April 2002 – April 2003

Operations, Administration, Maintenance, and Provisioning (OAM&P) Standard Working Group
February 2003 – August 2003

Issue Background

Network security issues lie at the core of the President's National Security Telecommunications Advisory Committee's (NSTAC) work on behalf of the President. The NSTAC initiated in-depth review of network security issues in February 1990 when the Committee's Industry Executive Subcommittee (IES) established the NSTF to address the National Security Council's concern about the vulnerability of the Nation's telecommunications networks to intentional software disruptions or manipulations that could threaten national security and emergency preparedness (NS/EP) communications. Having completed its original task, the IES reestablished the NSTF at the December 1990 NSTAC meeting and charged it to work closely with, and in support of, the Government Network Security Subgroup (GNSS). In June 1991, the NSTF established the NSTAC NSIE. The task force submitted its final report and recommendations to the NSTAC on July 17, 1992. On August 26, 1992, the IES deactivated the NSTF and established the NSSC and the NSSOG. The NSSOG completed its task and disbanded in January 1995. The IES subsequently renamed the NSSC the NSG in accordance with the December 1994 IES Guidelines. In April 1997, the IES realigned its groups and renamed the NSG the NG. In September 1999, the IES restructured and created the PSTF to accomplish the tasking formerly assigned to the NG.

During the NSTAC XXVI cycle, the IES created the IS/ATF to develop policy recommendations with respect to the vulnerabilities in pervasive software and protocols critical to the operation of the Internet.

In 2002, the NSTAC's NSIE and the Government NSIE established the Security Requirements Working Group (SRWG) to examine the security requirements for controlling access to the public switched network, in particular with respect to the emerging next generation network. Members of the SRWG, representing a cross-section of telecommunications carriers and vendors, developed an initial list of security requirements that would allow vendors, Government departments and agencies, and service providers to implement a secure telecommunications network management infrastructure. The SRWG developed this initial list of security requirements as a consensus document and submitted it as a contribution to the Alliance for Telecommunications Industry Solutions (ATIS) Committee T1– Telecommunications, Working Group T1M1.5 OAM&P Architecture, Interface and Protocols for consideration as a standard.

Representatives from T1M1.5, the NSTAC NSIE, the Government NSIE, and T1M1 liaison organizations further refined the initial document and developed the standard, entitled *Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.* Committee T1 approved the standard (T1.276-2003) in July 2003.

During the NSTAC XXVII cycle, the IES created the OAM&P Standard Working Group to further examine the standard and develop conclusions and recommendations for action.

History of NSTAC Actions and Recommendations

On July 17, 1992, the NSTAC approved the *Network Security Task Force Final Report.* The report recommended that the President:

- Publicly support the NSTAC network security initiative; and
- Establish a Government focal point for coordination on network security standards.

The NSTAC also endorsed both the NSSOG and a strong network security information exchange among industry companies. The NSTAC formed its NSIE in 1991, paralleling a GNSS effort to create a Government NSIE. The joint meetings of the NSTAC and Government NSIEs remain a unique industry and Government forum where representatives exchange information on network threats and vulnerabilities in a trusted, nondisclosure environment.

The IES established the NSSOG and the NSSC in response to NSTAC XIV charges to continue network security activities. The IES established the NSSC as a permanent IES working group with oversight responsibility for network security activities.

On May 27, 1993, the NSSC recommended that the President:

- Correct the legislative deficiencies affecting the capability to gather evidence about computer crimes and to prosecute and convict computer criminals who target computers that support the national telecommunications infrastructure.

In February 1994, the Government and NSTAC NSIEs sponsored a Network Security Symposium. These groups designed the symposium to inform attendees of the potential threats to and vulnerabilities of the public switched network (PSN) from computer intruders. Subject matter experts from industry, Government, and law enforcement presented information.

At the March 2, 1994, NSTAC XVI meeting, the NSSC updated its assessment of the risk to the PSN and noted its plans to strengthen the NSTAC NSIE and expand its membership.

On June 28, 1994, the Government and NSTAC NSIEs sponsored a network firewalls workshop. The workshop provided an overview of firewall technologies, addressed strategies for mitigating vulnerabilities, discussed firewall uses and applications, and reviewed case histories.

In October 1994, the NSSOG released a technical report focusing on network security standards issues for the PSN. In its report, the NSSOG categorized 12 recommendations on policy, procedural, and technical issues important to promoting interoperability, mitigating current or future threat scenarios, implementing realistic solutions, and/or addressing a range of technologies or architectures.

At the January 12, 1995, NSTAC XVII meeting, the NSTAC approved the NSSOG report and recommended that the President:

- Task the National Institute of Standards and Technology (NIST) and other Government organizations to support industry in the development of standards recommended in the NSSOG report.

At the February 28, 1996, NSTAC XVIII meeting, the NSTAC approved the NSG's findings with respect to determining NSTAC's potential contributions to developing a middle-ground security technology solution. The NSTAC also presented the findings of a report entitled, *An Assessment of the Risk to the Security of Public Networks,* which was co-authored by the Government and NSTAC NSIEs.

On September 11, 1996, the Government and NSTAC NSIEs sponsored a symposium on securing data networks. This event continued successful efforts by the NSIEs to share lessons learned about network security with a broader audience through workshops and analytical reports.

Also in September 1996, the NSG sponsored the Network Security Research and Development (R&D) Exchange. The event's purpose was to analyze R&D activities ongoing in both the public and private sectors and to address issues of authentication, intrusion detection, and access control from the capabilities management perspective. In November 1996, the NSG organized the Forward-Looking Analysis Panel to consider the impact of the Telecommunications Act of 1996 on network security and NS/EP telecommunications services. The panel addressed issues such as carrier interconnection, collocation, and open network architecture. The Federal Communications Commission's (FCC) Network Reliability and Interoperability Council (NRIC) considered the panel's input and subsequently included it in the NRIC's final report.

At the March 18, 1997, NSTAC XIX meeting, the NSG reported on its work to address the impact of the changing regulatory and technological environment on NS/EP telecommunications services. The NSG also reviewed its recent activities in the areas of R&D, intrusion detection, and forward-looking network control security analysis. At the meeting, the NSG outlined the efforts of the newly established Intrusion Detection Subgroup (IDSG) and its charge to explore a more cooperative approach to developing enhanced intrusion detection tools. The NSG concluded by addressing the activities of the NSIEs and noted that the NSTAC NSIE expanded its membership from nine to twenty.

Following NSTAC XIX, the NG's IDSG assessed network intrusion detection R&D activities to determine whether NS/EP considerations required additional efforts. Working with industry groups, the Defense Advanced Research Projects Agency (DARPA) and other Government groups, the IDSG identified the current state of intrusion detection research. The IDSG subsequently provided a report to NSTAC XX in December 1997 detailing its findings and recommendations for the President to consider in promoting the R&D of intrusion detection technologies. The NSTAC accepted and approved the report and recommended that the President:

- Promulgate a national technology policy to address intrusion detection;
- Establish an interagency working group for intrusion detection;
- Increase R&D funding for intrusion detection for network control systems vital to continued operation of critical infrastructures; and
- Encourage cooperative development programs.

The NG established another subgroup following NSTAC XIX to respond to a request by Dr. John Gibbons, then Assistant to the President for Science and Technology. Dr. Gibbons asked NSTAC to determine the likelihood of a widespread telecommunications outage, identify industry plans in place for intercarrier coordination to respond to such an outage, and describe how telecommunications service providers and the Government would cooperate to assure the President that restoration priorities would meet the national interest. The NG established the Widespread Outage Subgroup (WOS) to focus on these issues and provided a report to NSTAC XX reflecting its findings. The WOS determined that, given the limited precedent for telecommunications outages of such magnitude, there was a low probability of a widespread, sustained outage of public telecommunications service. In December 1997, the NSTAC approved the WOS report and recommended that the President:

- Direct the appropriate Federal departments and/or agencies to work with industry to improve intercarrier coordination plans and procedures;
- Encourage the FCC to maintain a Defense Commissioner at all times to help industry and Government overcome legal and regulatory impediments to a rapid and orderly restoration of service during a widespread telecommunications outage;
- Task the appropriate Federal departments and agencies to work with industry to advance the state-of-the-art for software integrity; and
- Direct the expansion of Government R&D efforts to address the most significant vulnerabilities of new and evolving telecommunications technologies and services.

Following NSTAC XX, the NG examined the readiness of the telecommunications industry to ensure continuity of service through the millennium change, focusing on NS/EP and the national telecommunications infrastructure. The NG surveyed telecommunications service providers, equipment vendors, system integrators, industry forums addressing the Year 2000 (Y2K) problem, and vendors providing Y2K solutions. The NG concluded that significant efforts were underway in both industry and Government to eradicate the Y2K problem within the Nation's telecommunications infrastructure. However, given the extent and complexity of the Y2K software augmentation, there were no guarantees that Y2K measures would anticipate, and/or prevent, every problem. In September 1998, the NSTAC approved the NG's Year *2000 Problem Status Report* and recommended that the President:

- Direct appropriate departments and agencies to develop contingency plans to:
- Respond to Y2K-induced service impairments of the Government's NS/EP customer premises equipment (CPE), functions, and applications
- Fulfill mission-critical NS/EP responsibilities in the event of Y2K induced PN service impairments
- Direct his Y2K focal point to ensure the coordination of the Government's requests for Y2K readiness information from the telecommunications industry

Following NSTAC XXI, the NG continued the tasking from the NSTAC XX meeting to examine how NS/EP operations might be affected by a severe disruption of Internet service. In conjunction with the gap analysis effort by the Office of the Manager, National Communications System (OMNCS), NG members provided their individual perspectives on the *Public Network (PN) Alternatives Analysis Report* developed by the OMNCS. During this cycle, the NG continued to oversee the NSTAC NSIE and worked toward facilitating the exchange of network security R&D information between industry and Government.

The R&D effort subsequently resulted in an NG-sponsored R&D Exchange in October 1998, held in collaboration with activities sponsored by Purdue University's Computer Operations, Audit, and Security Technology (COAST) Laboratory and the Institute of Electrical and Electronics Engineers (IEEE). The exchange focused on two themes. The first theme examined how industry and Government can better collaborate on R&D. The second examined the growing convergence of telecommunications and the Internet. The attendees overwhelmingly agreed on the need to identify potential centers of excellence in industry, Government, and academia and provide them with appropriate long-term funding to promote the development of computer and network security professionals, disciplines, and programs. Equally important was the need to establish large-scale testbeds to promote joint research, develop and verify metrics and evaluate security products, and address other technical needs in network security and information assurance.

The Government and NSTAC NSIEs completed an after-action report on the workshop, *The Insider Threat to Information Systems: A Framework for Understanding and*

Managing the Insider Threat in Today's Business Environment. The workshop was held in June 1998. The after-action report provided for sharing lessons learned in this vital area of insider threat that is affecting both industry and Government. In addition, the NSIEs completed their *1999 Assessment of the Risk to the Security of the Public Network*. The NSIEs concluded that the 1995 findings regarding the overall vulnerabilities of the PN were still valid. Old vulnerabilities were still being exploited even though fixes were readily available. Vulnerabilities in many of the PN's diverse technologies (including, Signaling System 7 [SS7], Intelligent Networks [IN], Asynchronous Transfer Mode [ATM], and Synchronous Optical Network [SONET]) remained unaddressed. The interconnectivity among technologies and networks had not merely persisted, but had become even greater than it was in 1995. Between 1995 and 1999, three major factors exacerbated the overall vulnerability of the PN: the *Telecommunications Act of 1996* (Telecom Act), changing business practices, and the Y2K problem.

In addition, the NSTAC NSIE revised its charter to bring it in line with how the NSIEs function. The NSIEs are primarily information sharing bodies in the area of network vulnerabilities and threat analysis.

In June 1999, the NG completed its work on the *Internet Report: An Examination of NS/EP Implications of Internet Technologies.* The report addressed the following three objectives: 1) examine the extent to which NS/EP operations will depend on the Internet over the next 3 years; 2) identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the PSN; and 3) examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

The NG concluded that the NS/EP community's direct dependence on the Internet for mission critical operations was modest. Departments and agencies with NS/EP responsibilities were using the Internet mostly for outreach, information sharing, and electronic mail. The NS/EP community was more inclined to depend on dedicated Transmission Control Protocol/Internet Protocol (TCP/IP) networks (also called intranets) for mission-critical NS/EP operations, at this time, because of significant security and reliability concerns associated with the Internet. In June 1999, the NSTAC approved the NG's report and the following recommendations:

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:
  - Work with the NS/EP community to increase understanding of evolving Internet dependencies
  - Work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements
  - Interact with the appropriate Internet organizations and initiatives to investigate, develop, and employ NS/EP-specific Internet priority services, such as end-to-end priority routing and transport
  - Examine the potential impact of IP network-PSN convergence on PSN specific priority services
- Recommend that the President direct the appropriate Government departments and agencies to use existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies

In addition, the NSTAC directed the IES to examine the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services (including, Government Emergency Telecommunications Service [GETS] and Telecommunications Service Priority [TSP]).

Following the NSTAC XXV Meeting on March 13, 2002, the IES again focused on network and Internet security issues. At the meeting, the Special Advisor to the President for Cyberspace Security discussed the serious threats posed by vulnerabilities within the Domain Name Servers and the Border Gateway Protocol. In response to these concerns, the NSTAC created the ISATF to develop recommendations to the President on how to identify and remediate vulnerabilities in pervasive software/protocols, define the "edge" elements of the Internet, and determine ways that the NSTAC could integrate its efforts to define and monitor significant critical infrastructures supporting the Internet with other industry activities.

In its *First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software/Protocols* report, the ISATF analyzed five stages relevant to identifying and remediating vulnerabilities in pervasive software and protocols: prevention, detection, information sharing, analysis, and correction. In the area of prevention, the task force advocated aggressive public-private research and development activities and cited the need to develop adequate alert and warning systems to support the operations of information sharing and analysis centers. The task force also identified barriers to the effective detection of vulnerabilities, such as the myriad number of forums devoted to detection and the lack of standardization in reporting procedures. Next, the task force emphasized that significant barriers to information sharing exist, such as the *Freedom of Information Act* (FOIA) and liability concerns, and advocated the creation of legislation that would ease the sharing of critical information. The ISATF also concluded that the analysis functions within industry that detect and publish vulnerabilities appear to be adequate, but the Government may find some benefit in better leveraging available synergies by consolidating Government-funded analysis centers where appropriate. Finally, the task force observed that while many organizations are successfully correcting and remediating vulnerabilities, they fail to utilize a streamlined method for expeditiously disseminating corrected information to the telecommunications and Internet service provider (ISP) communities.

Based on the findings of the ISATF report, the NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry, to:

- Consolidate Government-funded watch center operations of agencies and departments dedicated to the detection and dissemination of information related to Internet vulnerabilities into one organization to create a more efficient and effective collaborative industry/Government information-sharing partnership;
- Establish a lead organization within the Department of Homeland Security (DHS) to coordinate with industry a process for warning, notification, coordination, and remediation of widespread problems in a national emergency;
- Recognize the need to involve all aspects of the Internet in the process of identifying significant vulnerabilities, including the web hosting, network access provider, backbone, and ISP communities;
- Fund efforts related to identifying and mitigating vulnerabilities in the most critical protocols or software that key sectors of the Nation's infrastructure rely upon; and
- Promote and support legislation to address FOIA, antitrust, and liability concerns regarding information shared by industry for the purposes of critical infrastructure protection.

Additionally, the ISATF made other recommendations focused on developing a process for the Internet community, both private and public, to share information within its component communities, and within the larger telecommunications and Internet infrastructure context.

At the NSTAC XXV Meeting, participants also expressed concern over the ability to defend the Internet by protecting the edges of the Internet against attack or exploitation. In response to these concerns, the IES tasked the ISATF to provide guidance on how to define the edge of the Internet.

Through detailed analysis, the ISATF determined that because the Internet is not a single network but a network of interconnected networks, there is no single definition of the edge, as the definition depends on perspective. The ISATF also noted that there are many different ways to define the edge that include, but are not limited to the following: all systems that contain Internet Protocol (IP) addresses that do not route IP packets; the composition of information systems; and zones of responsibility for network operators versus end-users. In addition, the group noted that emphasis should focus not on defining the edge of the Internet but on defending the Internet as the adoption of a single definition of the edge could prevent critical security precautions from being addressed in other areas.

Based on the ISATF's analysis, the NSTAC recommended to the President that:

- The Government should continue its work to identify the critical national security and emergency preparedness missions and functions supporting those missions that rely on the Internet and encourage the parties responsible for those missions to ensure that they are adequately protected through redundancy and alternative capabilities;

- Industry, standards bodies, software vendors, equipment vendors, network operators, and end-users of all products and services that make up the Internet should ensure that these products have built-in baseline security features and that these capabilities are appropriately configured and kept current; and

- The Government should work with Internet security experts and standards bodies to develop a standard set of key warnings and indicators that all service providers can use as a baseline to measure security threats.

The NSTAC's OAM&P Working Group recognized that Executive Orders, Presidential directives, and Presidential commissions have specified infrastructures as national assets that are critical to the defense and economic security of the United States. Telecommunications is one of these critical infrastructures. Security for the network management functions controlling this infrastructure is essential. Many standards for network management security exist; however, compliance is low and implementation is inconsistent across the various telecommunications equipment and software providers. In addition, service providers are specifying contradicting requirements for products, which results in inconsistent vendor feature sets and potentially higher costs for vendors. Finally, as the telecommunications industry transitions to a converged network environment, new security challenges emerge; and threats in the public network become threats in the management and control planes.

Previous NSIE security assessments of the public network have also documented the management plane's vulnerabilities and susceptibility to intruder attacks. Because an increasing number of networks are closely tied to intranets, these networks are susceptible to hacker threats. Furthermore, the lack of standards to address this issue enables intruders to penetrate vulnerabilities and further deteriorate the telecommunications networks. Therefore, an urgent need exists for this baseline standard to provide much-needed security mechanisms for telecommunications carriers and vendors to implement.

The OAM&P Standard Working Group reviewed T1.276-2003 and concluded that the current standard addresses only one aspect (such as, the management plane) of an overall end-to-end security solution. T1.276-2003 addresses security for network element, management system, and element management system equipment only; it does not specifically address security for other equipment, such as customer premises equipment. Apart from the T1.276-2003 requirements, the current standard assumes that effective hardware and software controls provided by the operating system protect the data and resources being managed.

In addition, the OAM&P Standard Working Group developed recommended to the President that:

- The National Institute of Standards and Technology (NIST) review the T1.276-2003 standard. If a review finds a conflict between the T1.276-2003 standard and existing Federal Information Processing Standards and NIST publications, NIST should make these conflicts known to the appropriate standards bodies;
- Federal departments and agencies be encouraged to use the T1.276-2003 standard in requests for proposals, as appropriate; and
- Through the DHS, encourage officials responsible for other infrastructures to consider the elements of the T1.276-2003 standard as a baseline for security requirements and adapt appropriate requirements for their respective infrastructure.

Actions Resulting from NSTAC Recommendations

In response to an NSTAC XIV charge to continue network security activities, the IES established the NSSC and the NSSOG. The IES charged the NSSC to:

- Oversee the NSIE and recommend NSIE follow-on activities;
- Establish and oversee the NSTAC NSSOG;
- Continue involvement in R&D information exchange;
- Represent the NSTAC on NSIE matters to the FCC Network Reliability Council (subsequently renamed the Network Reliability and Interoperability Council) and the Manager, NCS; and
- Support other network security issues as required.

The IES charged the NSSOG to establish and prioritize industry objectives for network security standards to support NS/EP capabilities, and to work with the standards community to provide guidance and motivation to develop and accept industry-wide standards.

In response to recommendations at NSTAC XV, Congress included provisions in the Violent Crime Control and Law Enforcement Act of 1994 that expanded the law's applicability to telecommunications operations, administration, maintenance, and provisioning systems. However, the Act did not fully address the concerns that prompted NSTAC's recommendations. Congress subsequently passed the National Information Infrastructure (NII) Protection Act of 1996, which provides measures to strengthen Federal laws against computer crime.

As the IDSG focused primarily on R&D issues related to intrusion detection technology, the Government was exploring broader R&D issues. In particular, the President's Commission on Critical Infrastructure Protection (PCCIP) examined R&D issues affecting the security of all critical infrastructures. NSTAC's findings and recommendations are consistent with those resulting from the PCCIP's work. Further, Presidential Decision Directive (PDD) 63 assigned the Office of Science and Technology Policy (OSTP) responsibility for coordinating R&D agendas and programs for the Government through the National Science and Technology Council.

Since NSTAC XX, three events occurred to address the WOS's recommendations. First, the OMNCS began expanding the National Telecommunications Coordination Network (NTCN) to provide a mechanism to support intercarrier coordination in the event of a widespread outage. Second, the FCC designated a Defense Commissioner, and industry and Government developed procedural guidelines to help telecommunications carriers resolve issues with the FCC. Third, Government began focusing more attention on R&D and the need to advance the state-of-the-art equipment for software integrity and address the most significant vulnerabilities of new and evolving telecommunications technologies and services.

Following NSTAC XXI, the Government took measures to make critical Government systems Y2K compliant and to develop contingency plans to deal with any potential system failures that might occur. NSTAC's Year *2000 Problem Status Report*, issued in September

1998, influenced the President's Council on Year 2000 Conversion on the need to develop comprehensive contingency plans to mitigate any potential harmful effects on the Nation's NS/EP posture.

In response to the recommendation from the NSTAC's June 1999 *Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies*, the OMNCS established a permanent program to address NS/EP issues related to the Internet. The Priority Services and Internet Technology and Standards program actively promotes NS/EP requirements among pertinent standards bodies, including the Internet Engineering Task Force, the European Telecommunications Standards Institute, and the International Telecommunication Union.

Following NSTAC XXII in June 1999, the NSTAC tasked the IES to develop recommendations for the President regarding how the Government can optimally focus its efforts to enhance the security of the Nation's NS/EP telecommunications and information technology systems.

The IES subsequently formed the PSTF to address this task, The PSTF's objective was to examine current network security strategies to determine whether alternative strategies might more effectively diminish risk and, if appropriate, develop recommendations regarding those alternatives. The PSTF based the methodology for its study, inpart, on a model of network security developed by the IDSG in 1997. The IDSG identified four basic components of network security: prevention, detection, response, and mitigation. Using this model, the PSTF sought to answer the question: Could the risk to network security be more effectively reduced by changing the relative focus of network security efforts among these four components?

While the PSTF initially expected to find an optimal focus that might apply to all organizations, analysis of the data yielded a different answer, such as, security is not a "onesize-fits-all" proposition. While it is not feasible to specify an optimal focus among prevention, detection, response, and mitigation that will be suitable for all organizations, it is reasonable for each individual organization to consider how it focuses its network security efforts among these four components and ensure that it employs a strategy that is optimal for its own needs.

The PSTF subsequently identified a number of common themes among the organizations providing input to the study as well as some barriers that may impede the ability of an organization to implement an optimal focus among the four components. While the PSTF gathered a representative sample of data to reflect a broad range of industry perspectives, the PSTF determined that it did not have sufficient information to adequately reflect the Government's perspective. Consequently, the PSTF decided to provide a status report to NSTAC XXIII in May 2000 and recommended that the IES consider including in the NSTAC XXIV work plan the following task:

- Based on the preliminary analysis and general observations of the PSTF report, complete the analysis of the focus of network security efforts by seeking a broader range of input from Government and academia, as well as additional input from industry.

At the NSTAC XXII meeting, the Honorable John Hamre, Deputy Secretary of Defense, discussed the need for open dialogue between industry/Government in the current era of dynamic technological change. Dr. Hamre requested NSTAC's assistance to "tackle the much deeper, more complicated problem, which is how do we embed security in depth in the infrastructure upon which we, the Government, depend and upon which you and your customers depend." NSTAC's IES subsequently began to scope this issue to determine how to respond to Dr. Hamre's request. The IES tasked the EISISG to determine the depth and breadth of this request and provide the IES with a recommended action plan.

The scoping concluded, through briefings and various interactions with industry and Government, that the NSTAC can help in two distinct ways:

- Promote the Federal Government's efforts to work with industry to accomplish their mission of incorporating electronic commerce into their operations; and

- Individually support and participate in existing, successful industry and Government forums.

Following the recommendation of the NSTAC based on the ISATF's recommendation to establish a lead organization within the Department to coordinate with industry regarding threat warnings and notifications, DHS created the Information Analysis and Infrastructure Protection Directorate (which was reorganized in 2005 into other directorates within the Department) to identify and assess intelligence information concerning threats to the United States, issue warnings, and take preventative and protective action against those threats. Moreover, DHS consolidated the watch center capabilities of several Federal Government agencies under its auspices.

The U.S. Congress included a provision (section 214) in the Homeland Security Act of 2002 establishing the protection of voluntarily shared critical infrastructure information.

The National Cyber Security Partnership (NCSP) Task Force 4, Working Group 5 designated a liaison to work with T1M1 as they explore technical standards and Common Criteria. T1.276-2003 will be one of the many standards that will be considered as the NCSP works to secure cyberspace. In addition, the International Telecommunication Union is developing an international standard based on the requirements outlined in T1.276-2003.

Finally, the General Services Administration required compliance by all Federal departments and agencies with the American National Standard T1.276-2003 on OAM&P security requirements for the management plane.

Reports Issued

Network Security Scoping Task Force Report: Report of the Network Security Task Force, October 1990.

Network Security Task Force Final Report, July 1992.

NSTAC/NSIE Report on Deficiencies in Federal Laws on Computer Crime, April/May 1993.

Network Security Standards for the Public Switched Network: Issues and Recommendations, October 1994.

An Assessment of the Risk to the Security of Public Networks, Government and NSTAC NSIEs, December 12, 1995.

Report of the Network Security Group Research and Development Exchange, September 18, 1996.

Network Security Group Forward Looking Analysis Panel Proceedings, November 19, 1996.

Local Number Portability and Its Implications for the Public Switched Network: An NSIE White Paper, July 1997.

Software Integrity: An NSIE White Paper, July 1997.

Report on the Likelihood of a Widespread Telecommunications Outage, December 1997.

Report on the NS/EP Implications of Intrusion Detection Technology Research and Development, December 1997.

The Insider Threat: Legal and Practical Human Resources Issues: An NSIE White Paper, April 1998.

The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment: An NSIE White Paper, June 1998.

The President's NSTAC Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration, October 1998.

An Assessment of the Risk to the Security of the Public Network, April 1999.

Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies, June 1999.

Protecting Systems Task Force Report on Enhancing the Nation's Network Security Efforts, May 2000.

First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software/Protocols, April 2003.

Defining the Edge of the Internet, June 2003.

Operations, Administration, Maintenance, and Provisioning (OAM&P) Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane, August 2003.

Obtaining Critical Telecommunications Facility Protection During a Civil Disturbance

Investigation Group / *Period of Activity*

NS/EP Panel
September 1993 – April 1994

Issue Background

The April 1992 civil disturbance in Los Angeles identified the need for standardized guidelines in requesting the protection of critical telecommunications facilities. In response to the problems noted, the NS/EP Panel met with California State, Federal Government, and telecommunications industry representatives in San Francisco. The meeting participants generally agreed that emergency response personnel were not sufficiently prepared to respond to the crisis that overwhelmed local law enforcement and fire protection services.

Telecommunications industry representatives discussed their difficulties in obtaining protection for their facilities, while other participants acknowledged they had been confused about whom to contact and who had authority during the widespread civil unrest. Because the President declared the crisis to be a Federal emergency, points of contact and authorities changed, causing some confusion. Participants raised this issue at the meeting and questioned how to obtain critical telecommunications facility protection during a Federal emergency. DOJ and Department of Defense (DOD) representatives briefed the panel on the roles of the DOJ, the National Guard, and active duty military personnel during national emergencies.

As a result of the meeting, the NCC, working closely with the NS/EP Panel, agreed to develop guidelines to assist emergency planners during their preparations for and response to civil disturbances. The NS/EP Panel and the NCC developed the document in close coordination with the California Office of Emergency Services and the California Utilities Emergency Association.

In May 1994, the NCC and the NS/EP Panel issued *Guidelines for Obtaining Protection of Critical Telecommunications Facilities During Civil Disturbances.* The document serves as a guide for telecommunications industry emergency planners when discussing their facility protection needs with local, State, and Federal authorities.

On October 4, 1995, the NS/EP Panel conducted an industry/Government Critical Telecommunications Facilities Protection exercise simultaneously at three separate locations using video teleconferencing linking sites in Arlington, Virginia; Oakland, California; and Los Angeles, California. The exercise provided an opportunity for key emergency response planners at the local, State, and national levels to develop working relationships, gain a better understanding of the many planning factors required by each participant, and define the critical steps in the protection process.

Participants noted this exercise helped clarify the lines of communication when requesting protection from the city to county to State to national levels and helped clarify the various roles and responsibilities of the organizations involved. The activity also highlighted planning shortfalls that required correction to streamline the protection process. The NS/EP Panel identified two key issues for inclusion in the *Guidelines for Obtaining Protection of Critical Telecommunications Facilities During Civil Disturbances* document: (1) adding procedures for transitioning from Federal control back to State control and (2) discussing the legal aspects of federalized versus non-federalized troops.

In an October 1996 conference call, participants of the industry/Government exercise discussed options for clarifying the federalization issues. The NS/EP Panel added new language to the document, indicating that both federalized and non-federalized National Guard troops, each with different chains of command, may participate in restoring and

maintaining law and order. In addition, the panel added a section authorizing the Secretary of Defense to determine when Federal military forces should withdraw from the disturbance area and when National Guard units would return to State control.

Reports Issued

Guidelines for Obtaining Protection of Critical Telecommunications Facilities During Civil Disturbances, May 1994.

Protection of Critical Facilities Exercise, After-Action Report, December 1995.

Physical Security of the Telecommunications Network

Investigation Group / *Period of Activity*

Plans Working Group
December 1990 – September 1991

Vulnerabilities Task Force
May 2002 – February 2003

Trusted Access Task Force
April 2003 – April 2004

Issue Background

The United States Government recognizes the telecommunications sector as a critical component of national security and emergency preparedness (NS/EP) services and the potential for risk due to the growing reliance on the availability of telecommunications resources by the Government, other critical infrastructures, and the general public. Like all other critical infrastructures in the United States, the communications infrastructure remains vulnerable to physical attacks that could significantly damage a facility or free standing component of the network severely enough to interrupt service.

History of NSTAC Actions and Recommendations

On December 13, 1990, at NSTAC XII, an NSTAC Principal questioned the physical security of the public switched network, due to issues surfaced by a National Research Council report on the growing vulnerability of the Nation's communications network. As a result, the NSTAC established and tasked the Plans Working Group (PWG) with investigating the Committee's growing concerns related to physical security of the telecommunications infrastructure.

In response, the PWG, in conjunction with the National Communications System (NCS) Office of the Joint Secretariat, prepared a physical security study that examined current industry/Government activities, including results from a questionnaire given to the National Coordinating Center's industry representatives on physical security policy, operational procedures, and methods. The study also documented past NCS efforts regarding physical security of NS/EP telecommunications facilities, sites, and assets and relevant conclusions and recommendations of those past efforts. The study concluded that current industry/Government activity and past NCS documents demonstrated industry and Government had made substantial progress in addressing the physical security of telecommunications facilities, sites, and assets. According to the study, physical security was well planned and managed in general.

After reviewing the information in this study, the NSTAC concluded that the document required no further NSTAC action at that time.

The NSTAC again addressed physical security concerns during the business and executive sessions of the NSTAC XXV Meeting, at which time the Principals again raised concerns related to the physical security of the telecommunications infrastructure in the wake of the attacks against the United States on September 11, 2001. As a result, the NSTAC chartered the Vulnerabilities Task Force (VTF) to examine possible risks associated with the concentration of critical telecommunications assets in telecom hotels and Internet peering points, as well as vulnerabilities involving equipment chain of control and trusted access procedures to telecommunications facilities. The VTF concluded that, while the telecommunications infrastructure is inherently vulnerable to physical attack, the existence of multiple interconnection facilities, such as telecom hotels, has helped to disperse telecommunications assets over numerous locations, thereby reducing service impacts caused by the loss of any one facility. The task force acknowledged that the physical destruction of individual critical telecommunications facilities could disrupt service at the local level and restrict access to the infrastructure. Therefore, site by site mission critical risk analyses are the only way for organizations to identify possible vulnerabilities that could affect critical functions supporting those missions.

The VTF also addressed the Government's concern that the telecommunications infrastructure may be especially vulnerable because trusted physical access is granted to individuals requiring entrance to sites where critical telecommunications assets are concentrated. During its deliberations, the task force stressed how the nationwide web of telecommunications assets has become far too extensive to ensure full access control to prevent tampering. While owners can secure critical sites and equipment to the extent possible with electronic locks, padlocks, fences, alarms, security cameras, and the like, access control remains an important issue because the loss of or damage to a site housing numerous critical telecommunications assets could have local or "last mile" impacts and adversely affect NS/EP services. Primary factors influencing the efficacy of access control procedures include individuals with malicious intent, the omnipresent insider threat, the lack of a standard personal identification and background check capabilities, and a lack of universally applied access control procedures and best practices.

Furthermore, the VTF addressed chain of control issues regarding the security of products and services delivered to critical locations. The task force concluded that, although security will remain a priority, no policy actions are deemed necessary at this time. However, if networks become reliant on commodity equipment, this could become an issue for consideration.

In response to the analysis conducted by the VTF, and to mitigate any risks associated with concentration of assets, such as telecom hotels, the NSTAC presented four consecutive reports to the President titled *Chain of Control, Telecom Hotels, Trusted Access,* and *Internet Peering Security* with specific recommendations on measures to be undertaken to secure the telecommunications industry.

In direct response to the work delineated in the *Trusted Access Report,* the NSTAC established the Trusted Access Task Force (TATF) and charged it to examine how industry and the Government can work together to address concerns associated with implementing a national security background check program for access to key facilities.

In response to the NSTAC's earlier findings in this area, the TATF further examined the concerns that the telecommunications infrastructure may be vulnerable because trusted physical access is granted to individuals who require entrance to sites where telecommunications assets are concentrated without ensuring that the individual does not pose a threat to the facility or infrastructure. The task force proposed that a national standard for personnel screenings using Federal databases, such as the program used by the Department of Homeland Security's (DHS) Transportation Security Administration (TSA), may be beneficial for industry in mitigating threats to the telecommunications infrastructure.

The TATF also examined the need for a standard, industry-wide, certificate-based picture identification (ID) card. The group noted that the creation of such a card would further solidify the security of the Nation's telecommunications infrastructure, and also assist in the identification of those employees who have passed the national screening. In an emergency or crisis the credential will also expedite recovery efforts by helping to easily identify personnel who are needed at the site.

During the May 2004 NSTAC XXVII Meeting, the Assistant Secretary for Infrastructure Protection, DHS, emphasized the importance of the group's work and commented on the need for short-term initiatives that could be undertaken to increase security at numerous upcoming National Special Security Events (NSSE), and could also be used as the basis for long-term perimeter access guidelines. As a result, the TATF, with the assistance of the NCC's Information Sharing and Analysis Center (ISAC) member companies, proposed the establishment of a pilot program to pre-screen, against Federal terrorist lists/Government databases, a small group of industry employees who may need access to physical sites or critical information concerning NSSEs and associated critical facilities. The TATF deemed the United States Secret Service (USSS) the most appropriate resource for conducting industry screenings on the specified personnel due to their role in planning NSSEs. The pilot screening program produced a list of key lessons learned, as well as several human resources concerns from industry.

Based on the TATF's analysis the NSTAC recommended that the President direct the appropriate departments and agencies to:

- ▶ Coordinate with industry to:
  - Implement and support a standardized screening process for industry to voluntarily conduct screenings on persons who have regular and continued unescorted access to critical telecommunications facilities (*e.g.,* switching facilities), including telecommunications employees and vendors, suppliers, and contractor staff, including:
    - Modeling such a program after the current TSA program by including different relative background investigation levels for various facilities and personnel types;
    - Partnering with DHS, through TSA, to upon request from industry, conduct screenings for industry personnel working at critical private telecommunications facilities; and
    - Working with NRIC to develop industry best practices defining specific criteria for determining which telecommunications employees should be subject to screenings.
  - Make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of screened individuals at critical sites and to support both physical and logical access for such individuals to critical telecommunications facilities and the networks and information concerning them by building on the ongoing work of the General Services Administration's Federal Identity Credentialing Committee.
  - Build on the recommendations in the NCC ISAC report, *Preparing for a National Special Security Event,* to develop a national plan for controlling access at the perimeter of an NSSE or a disaster area. To facilitate the development of a national perimeter access plan to be incorporated in the *National Response Plan,* the Government should continue to support the screening program coordinated by the NCC ISAC with screenings facilitated by DHS and the USSS.
- ▶ Partner with the ISACs across infrastructures to implement screening, credentialing, and access control policies mirroring those recommended for the telecommunications infrastructure for all critical infrastructures.

Actions Related to NSTAC Recommendations

In accordance with the NSTAC's recommendations and the NCC's *Preparing for a National Special Security Event Report,* the Government implemented a pilot program to coordinate industry access for the 2005 Presidential Inauguration. In addition, in a related effort, the NCS developed in early 2006, in partnership with Federal, State, and local Government entities, as well as a private sector company, an access standard operating procedure (SOP) to ensure that private critical infrastructure responders have priority access to disaster areas. The access SOP has been adopted by the State of Georgia and is currently being used as an example for other States.

Reports Issued

IES Plans Working Group, A Review of Physical Security, September 1991.

Vulnerabilities Task Force Report: Chain of Control, March 2003.

Vulnerabilities Task Force Report: Telecom Hotels, March 2003.

Vulnerabilities Task Force Report: Trusted Access, March 2003.

Vulnerabilities Task Force Report: Internet Peering Security, April 2003.

Trusted Access Task Force Report: Screening, Credentialing, and Perimeter Access Controls Report, January 2005.

Response to September 11, 2001, Terrorist Attacks

Investigation Group / *Period of Activity*

September 11 "Lessons Learned" Ad Hoc Group
October 2001 – December 2001

Issue Background

The terrorist attacks of September 11, 2001, required industry and Government to marshal resources at the national, State, and local levels to support response and recovery efforts. A critical part of those efforts was the restoration of emergency telecommunications services and the provisioning of communications to emergency response personnel. The National Communications System and the NCC, in partnership with NSTAC companies, played a major role in ensuring a quick response and recovery of telecommunications capabilities in the wake of the September 11th attacks. Subsequently, in response to a request from the Special Advisor to the President for Cyberspace Security, the NSTAC formed the September 11th "Lessons Learned" Ad Hoc Group to provide an industry perspective on lessons learned in responding to the September 11th tragic events. The NSTAC Chair discussed the ad hoc group's analysis in its December 12, 2001, letter to the President.

History of NSTAC Actions and Recommendations

After identifying nearly 40 policy and operational lessons learned from the September 11, 2001, response, the ad hoc group narrowed its focus to the following issues: access procedures to disaster sites, communications procedures, and industry representation within the NCC.

The major issue dealt with procedures for access to disaster sites affected by the attacks. Specifically, inconsistent access control procedures for moving telecommunications equipment and personnel into and out of the World Trade Center disaster area created confusion and presented obstacles for the telecommunications companies engaged in the restoration of the infrastructure. Procedures were revised each time a new authority took responsibility for managing access to the disaster area. Depending on the phase of the response, local responders, State authorities, or Federal personnel were in control. The invocation of both crisis management, *i.e.* law enforcement officials treated the disaster area as on ongoing crime scene, and consequence management measures served to complicate the access control issue even further.

Based on the ad hoc group's analysis, the NSTAC recommended that the President direct the appropriate departments and agencies to lead a national effort to examine remedies to perimeter access control issues. The NSTAC determined that these remedies should consider overlapping jurisdictions and result in consistent processes and procedures for incorporation into the Federal Response Plan and State and local emergency response plans. The objective was to ensure that any future national response efforts to unanticipated attacks would be fully planned and coordinated and consistently carried out without delay.

Additionally, the ad hoc group addressed communications procedures during emergencies. The events of September 11, 2001, demonstrated the need for standard procedures to improve communications among decision makers, operational personnel, and other stakeholders during emergencies. Such procedures would have to take into account the severity of the emergency, the classification of the communications, the location of the communicators, and the telecommunications capabilities available, among other factors. The ad hoc group found that the requisite operational procedures were already developed and in place at the NCC, including procedures related to the NCC's Telecom-ISAC function. The NSTAC had consistently identified ISACs as the appropriate focal points for coordinating communications among industry players and between industry and Government in the new threat environment. Consequently, the ad hoc group concluded that the telecommunications industry should work through NCC representatives to address communications requirements during emergencies.

The ad hoc group also analyzed NCC industry representation. The group acknowledged that the NCC must maintain proper industry representation to meet operational challenges in the evolving threat and technology environments. In the aftermath of the September 11, 2001, attacks, the NS/EP community reaffirmed the critical role wireless communications plays in response to national emergencies. Similarly, Internet services were deemed to be increasingly important in disaster response and central to the mission-critical operations of business and Government agencies. Accordingly, the ad hoc group examined the mix of industry representation in the NCC and found that NCC members represented (1) the majority of the wireless carrier market share; (2) more than half of the Internet backbone provider market; and (3) a minority of the Internet access provider market. The ad hoc group concluded that augmenting Internet access provider membership in the NCC could help the NCC better address potential network security issues. Such issues included the threat of distributed denial of service attacks and software viruses launched by end users *via* dial-up connections to the network.

As part of its lessons learned analysis, the ad hoc group reviewed previous NSTAC recommendations, recognizing that the NSTAC's cumulative work could provide valuable information related to ensuring reliable infrastructure services and securing the Nation's critical facilities. The group also recognized that the sharing of such information had gained new importance with the national focus on homeland security. Previous NSTAC studies selected for review by the group were in the areas of cellular priority access, energy service priority, protection of critical facilities, public network convergence and vulnerabilities, and national information sharing, analysis, and warning. The group concluded that such studies and associated recommendations could demonstrate best practices for use by other organizations concerned with the physical and cyber security of critical infrastructures supporting multiple sectors.

Reports Issued

NSTAC Letter to the President, December 17, 2001.

Termination of Cellular Networks During Emergency Situations

Investigation Group / *Period of Activity*

Cellular Service Shutdown Ad Hoc Working Group
August 2005 – January 2006

Issue Background

As a direct result of the bombings that took place in the London transportation system in July 2005, U.S. authorities initiated the shut down of cellular network services in the Lincoln, Holland, Queens, and Brooklyn Battery Tunnels. The Federal Government based this precautionary measure on the suspicion that similar attacks might also be perpetrated in the tunnels leading to and from New York City. Though the decision was rooted in vital security concerns, the resulting situation, undertaken without prior notice to wireless carriers or the public, created disorder for both Government and the private sector at a time when use of the communications infrastructure was most needed. Shortly following these activities, the National Coordinating Center (NCC) hosted a teleconference to discuss the need to develop a process for determining if and when cellular shutdown activities should be undertaken in the future in light of the serious impact these efforts could have had, not only on access by the public to emergency communications services during these situations, but also on public trust in the communications infrastructure in general.

History of NSTAC Actions and Recommendations

These actions highlighted, within the President's National Security Telecommunications Advisory Committee (NSTAC) community, the need for a process to ensure that future similar decisions meet the Nation's security goals and ensure the protection of critical infrastructures. Consequently, on August 18, 2005, the NSTAC established a Principal level task force to formulate, on an expedited basis, recommendations to effect efficient coordinated action between industry and Government in times of national emergency.

To facilitate more coordinated action, the NSTAC recommended that the President direct his departments and agencies to:

- Work to implement a simple process, building upon existing processes, with the Department of Homeland Security (DHS) and National Communications System (NCS) coordination enabling the Government to speak with one voice, provide decision makers with relevant information, and provide wireless carriers with Government-authenticated decisions for implementation; and

- Achieve rapid implementation through the Homeland Security Advisor of each State, in conjunction with the NCS and the Office of State and Local Government Coordination, DHS.

The group concluded its activities upon NSTAC approval of the Letter and recommendations in January 2006.

Actions Resulting from NSTAC Recommendations

In support of the recommendations, the NCS approved Standard Operating Procedure (SOP) 303, "Emergency Wireless Protocols," on March 9, 2006, codifying a shutdown and restoration process for use by commercial and private wireless networks during national crises. Under the process, the NCC will function as the focal point for coordinating any actions leading up to and following the termination of private wireless network connections, both within a localized area, such as a tunnel or bridge, and within an entire metropolitan area. The decision to shutdown service will be made by State Homeland Security Advisors, their designees, or representatives of the DHS Homeland Security Operations Center. Once the request has been made by these entities, the NCC will operate as an authenticating body, notifying the carriers in the affected area of the decision. The NCC will also ask the requestor a series of questions to determine if the shutdown is a necessary action. After making the determination that the shutdown is no longer required, the NCC will initiate a similar process to reestablish service. The NCS continues to work with the Office of State and

Local Government Coordination at DHS, and the Homeland Security Advisor for each State to initiate the rapid implementation of these procedures.

Reports Issued

NSTAC Cellular Shutdown Letter to the President, January 2006

Telecommunications Industry Mobilization

Investigation Group / *Period of Activity*

Telecommunications Industry Mobilization (TIM) Task Force
June 1985 – June 1989

Issue Background

Recognizing the prominent role of the telecommunications industry in a national mobilization, the NSTAC formed the TIM Task Force and instructed it to develop an issue statement. Meanwhile, the OMNCS developed the *NS/EP Telecommunications Plan of Action* to implement relevant portions of E.O. 12472 and National Security Decision Directives 47 and 97. The plan, approved by the NCS Committee of Principals (COP) in 1985, included an action to provide Government leadership in telecommunications industry mobilization planning activities.

In September 1985, the TIM Task Force identified the following mobilization subjects as needing further study:

- Telecommunications service surge requirements;
- Personnel issues;
- Maintenance of stockpiles and inventories;
- Dependence on foreign sources;
- Dependence on other infrastructure systems;
- Industry and Government mobilization management structure; and
- Jurisdictional issues.

The TIM Task Force recommended a industry and Government forum be established to assess the seven TIM subject areas. In December 1985, industry and Government concurred with the formation of the Joint Industry/Government TIM Group, which began addressing TIM subjects on January 29, 1986.

History of NSTAC Actions and Recommendations

The NSTAC approved and forwarded to the President the Joint TIM Group's reports, *Personnel Issues and Dependence on Foreign Sources,* on November 6, 1987, and approved and forwarded to the President the reports, *Government and Industry Mobilization Management Structure* and *Maintenance of Stockpiles and Inventories* on September 22, 1988.

On June 8, 1989, the NSTAC approved and forwarded to the President the Joint TIM Group's final reports on *Telecommunications Service Surge Requirements, Dependence on other Infrastructure Systems,* and *Jurisdictional Issues,* a final report with overall recommendations on telecommunications industry mobilization. The NSTAC then disbanded the Joint TIM Group.

Actions Resulting from NSTAC Recommendations

The original Energy Task Force further defined the TIM recommendations on energy issues, including underground storage tank regulations.

The National Security Council and the Executive Office of the President initiated a review of overall national security mobilization preparedness. The Federal Emergency Management Agency implemented several TIM recommendations as part of the *Graduated Mobilization Response Plan.* The OMNCS Office of the Joint Secretariat developed a plan of action, involving all NCS member organizations, designed to track implementation of the TIM recommendations. The plan included identification of task responsibilities, a time-phased work plan, and a schedule of status reports. The Baseline Mobilization program involved assigning "lead" organizations to follow up and take actions necessary to implement each TIM recommendation during a 3-year period, with 36 tasks distributed among the NCS member organizations.

In September 1993, the OMNCS Office of the Joint Secretariat issued its *Final Report on TIM Recommendations.* The report presented the actions taken by various NCS

member agencies on 11 recommendations having a significant and immediate effect on NS/EP telecommunications. The remaining 25 recommendations, while of considerable importance, were of somewhat lesser significance relative to their immediate impact on NS/EP telecommunications. The telecommunications industry had substantially implemented those recommendations and the report addressed them. The OMNCS believed that the agencies assigned to implement the recommendations had responded favorably, and that the TIM program could be considered a success. The OMNCS also believed that further formal monitoring of the TIM program was not necessary.

Reports Issued

Volume I, TIM Issue Statement, September 5, 1985.

Volume II, Background and Supporting Material, September 5, 1985.

Personnel Issues, September 1987.

Dependence on Foreign Sources, October 1987.

Government and Industry Mobilization Management Structure, June 1988.

Maintenance of Stockpiles and Inventories, June 1988.

Telecommunications Service Surge Requirements, January 1989.

Dependence on Other Infrastructure Systems, April 1989.

Assessment of TIM Capabilities (V. I), April 1989.

TIM Subject Reports (V. II), April 1989.

Jurisdictional Issues, April 1989.

Exercise Participation, April 1989.

Final Report on TIM Recommendations, September 1993.

Telecommunications Service Priority

Investigation Group / *Period of Activity*

Telecommunications Service Priority (TSP) Task Force
December 1984 – December 1990

Issue Background

In December 1984, the NSTAC identified TSP as an urgent issue because of the need for a system that authorized both priority provisioning and restoration of NS/EP services for Federal, State, and local governments and private users. The TSP System replaced the Restoration Priority (RP) System, which covered only the restoration of Federal Government, inter-city, and private lines. The NSTAC IES established the TSP Task Force on February 21, 1985, to advise and assist the OMNCS in developing the TSP System, specifically regarding provisioning, restoration, maintenance, legal, and regulatory issues.

History of NSTAC Actions and Recommendations

The task force worked closely with the OMNCS in the development of the TSP System and provided assistance with its implementation. Specifically, the task force had a significant advisory role in creating the *Petition for Rulemaking and Proposed Federal Communications Commission (FCC) Rules* for the TSP System. The task force also assisted the TSP Program Office in establishing the initial TSP System Oversight Committee charter. The NCS Council of Representatives (COR) TSP Subcommittee and the TSP Task Force drafted and approved the charter in February 1990, and the DOD and the General Services Administration (GSA) approved the charter in November 1990. Subsequently, adoption of an amendment occurred in April 1991.

The task force had a role in both the creation of the TSP Oversight Committee and the selection of Oversight Committee members. During the week of September 28 through October 3, 1987, the TSP Task Force and NCS COR met and discussed the operational framework for the TSP System, including the establishment of the TSP Oversight Committee. On March 29, 1990, the TSP Task Force recommended that the Manager, NCS, appoint the following initial members to the TSP Oversight Committee: AT&T, Contel, McCaw Cellular, MCI, Bellcore, Sprint, GTE, State of California, State of South Carolina, Department of Transportation, Federal Emergency Management Agency, DOD, GSA, Department of Energy, Department of Commerce, National Telecommunications and Information Administration, and the FCC. The NSTAC approved the membership list and delegated future industry TSP Oversight Committee membership nominating authority to the IES.

Additionally, the task force assisted in developing the documentation that made the TSP System operational. The task force helped create the *TSP Service Vendor Handbook,* which provides operational details of the TSP System that service vendors will use as guidance for implementation and operation of TSP. The task force developed the *TSP Information Guide,* a TSP primer for small telephone companies, published by the United States Telephone Association in December 1989. Furthermore, the task force had a significant advisory role in creating NCS issuances on TSP procedures. Specifically, the task force helped develop NCS Directive 3-1, which clarified the responsibilities of and procedures for all TSP System entities. The task force also assisted in the development of the *TSP Service User Manual,* which provided a set of guidelines for all users of the TSP System.

The task force presented its final report at NSTAC XII in December 1990, including a recommendation to the President, which stated that the Federal Government should continue to support and administer the TSP System, as defined in NCS Directive 3-1.

Actions Resulting from NSTAC Recommendations

TSP System implementation began on September 10, 1990. The implementation plan included a 2.5-year period for transition from the RP to the TSP System. The TSP System became fully operational on March 9, 1993.

Today, the TSP Oversight Committee continues to meet on a biannual basis. Likewise, the OMNCS continues to provide the operational support for the TSP System.

Reports Issued

TSP Information Guide, December 1989 *(published for the TSP Task Force by the U.S. Telephone Association, now the U.S. Telecom Association).*

TSP Service Vendor Handbook (NCSH 3-1-2), July 1990.

Final Report of the TSP Task Force, September 1990.

Telecommunications Service Priority Carrier Liability

Investigation Group / *Period of Activity*

Industry Executive Subcommittee (IES)
Funding and Regulatory Working Group (FRWG)
November 16, 1990 – January 31, 1991

Issue Background

The Federal Communications Commission *Telecommunications Service Priority (TSP) Report and Order* authorizes telecommunications carriers to install or restore NS/EP telecommunications on a priority basis over services that do not serve NS/EP requirements. The FRWG reviewed this issue to further define the protection against liability offered by the *TSP Report and Order.* One area of concern identified by the working group was 911 service. The working group concurred that the *TSP Report and Order* offered adequate protection to carriers. The FRWG also observed that services provided under contract rather than through tariffs may not be protected by the *TSP Report and Order* language. The FRWG reached the following conclusions:

- The *TSP Report and Order* offered sufficient protection against liability charges arising from the disruption of non-NS/EP user tariffed services;
- The *TSP Report and Order* had not fully defined the legal ramifications of preempting a contracted versus a tariffed service; and
- Carriers should develop internal policies for preempting non-NS/EP users.

On March 15, 1991, the FRWG reported its findings to the IES. The IES concurred with the FRWG's findings.

Telecommunications Systems Survivability

Investigation Group / *Period of Activity*

Telecommunications Systems Survivability (TSS) Task Force
March 1986 – June 1989

Issue Background

The NSTAC developed the TSS issue in December 1982 to address all aspects of the telecommunications survivability question. The Commercial Satellite Survivability (CSS) and Commercial Network Survivability (CNS) issues evolved from the NSTAC's initial focus on TSS. On March 6, 1986, the NSTAC IES established the TSS Task Force and directed it to determine whether NSTAC recommendations had inconsistencies, whether the recommendations met the Government's NS/EP telecommunications policy requirements, and whether the Government effectively responded to the recommendations. In early 1987, the NSTAC charged the TSS Task Force to assess the impact of new technologies on telecommunications survivability.

The TSS Task Force concluded that no serious inconsistencies or gaps existed among NSTAC recommendations and the recommendations sufficiently met the Government's NS/EP telecommunications policy objectives. The NSTAC forwarded to the President the TSS Task Force recommendation to initiate a study to identify options for ensuring survivable electric power. The TSS Task Force completed reports on Government actions taken in response to NSTAC recommendations from the CNS, CSS, and Electromagnetic Pulse Task Forces, and submitted them to the NSTAC on November 6, 1987. The task force submitted similar reports on automated information processing and the National Coordinating Mechanism to NSTAC IX on September 22, 1988. The NSTAC approved these reports and forwarded them to the President on the respective dates. The TSS Task Force also completed an assessment of the applicability of network management technology to NS/EP telecommunications survivability, which the NSTAC forwarded to the President on September 22, 1988. The TSS Task Force assisted the OMNCS in developing the Federal Government's policy on essential line service (ELS).

On June 8, 1989, the NSTAC approved the TSS Task Force's final report and disbanded the task force. The NSTAC also directed the IES to proceed with the study of intelligent networks and virtual networks usefulness for enhancing network survivability, which the TSS Task Force initiated, pending review of the issue by the IES Plans Working Group (PWG).

History of NSTAC Actions and Recommendations

The NSTAC approved the TSS Task Force's final report and disbanded the task force on June 8, 1989.

Actions Resulting from NSTAC Recommendations

The TSS Task Force's electric power recommendations led to the establishment of the original Energy Task Force, and the intelligent networks study led to the establishment of the Intelligent Networks Task Force. The IES, through the OWG NS/EP Panel, provides a continuing evaluation of the overall progress and direction of TSS. The NS/EP Panel identifies any new concerns relating to TSS, advises the OWG of areas requiring NSTAC or NCS actions or study, monitors the status of general survivability of telecommunications systems, and reports periodically on the status of TSS to the OWG.

As part of the CNS program, the OMNCS Office of Plans and Programs monitored network management developments, including local exchange carrier network management capabilities. In addition, members assigned to the OMNCS Office of Technology and Standards Network Management and Technology Planning task assessed the effects of congestion on NS/EP telecommunications and how expert systems could improve network management for NS/EP telecommunications. The NCS continued to encourage compliance with NCS Notice 3-0-1, NS/EP ELS, which recommended that Federal departments and agencies having NS/EP telecommunications missions consider obtaining ELS to increase their probability of obtaining a timely dial

tone. The Department of Energy was directed to implement several Energy Task Force recommendations.

Reports Issued

TSS: Industry Responses to May 13, 1983 Questionnaire, September 1983.

TSS Task Force–Subgroup 1 Review, September 1986.

TSS Task Force–Review of Power, September 1986.

TSS Task Force–Review of Security, September 1986.

TSS Network Management Report, June 21, 1988.

TSS Review of Government Actions in Response to NSTAC-Recommended Initiatives, June 21, 1988.

TSS Electric Power Survivability Status Report, August 9, 1988.

TSS Task Force Final Report: Telecommunications System Survivability–Assessment and Future Directions, May 2, 1989.

Underground Storage Tanks

Investigation Group / *Period of Activity*

Industry Executive Subcommittee Funding and Regulatory Working Group (FRWG)
April 1990 – March 1991

Issue Background

In 1988, the Energy Task Force voiced concerns that the Environmental Protection Agency (EPA) regulations on underground fuel storage tanks would encourage telecommunications carriers to reduce the amount of fuel available for their backup generators. The EPA regulations (40 *Code of Federal Regulations* Part 280), originally proposed in April 1987, included standards for maintaining the integrity of the tank, protecting against spill and overfill, and detecting leaks. The telecommunications industry modified or replaced several thousand underground storage tanks (UST) pursuant to these regulations and added detection monitoring systems.

The Energy Task Force considered the implications of the regulations and concluded that if the telecommunications industry complied with the new EPA regulations, the public switched network might not have enough backup fuel storage capacity in all locations to operate through normal power outages. The Energy Task Force recommended that the Government grant a national security waiver from those parts of the regulations that affected NS/EP telecommunications providers.

The FRWG received briefings from the EPA and support staff on EPA UST regulations. The FRWG also investigated UST regulations at the Federal, State, and local levels. The group also surveyed several local exchange carriers and interexchange carriers to determine UST policies and procedures. The survey revealed that industry was reviewing the UST requirements as a result of the EPA regulations, and that companies used several criteria when developing UST requirements. The FRWG developed a paper outlining the UST issue and recommended the following:

- A waiver of EPA UST regulations should not be pursued. The waiver would not make a significant contribution to meeting Government backup power needs because companies were already pursuing their own UST programs, State and local regulations would be addressed regardless of any Federal waiver, and telecommunications companies would probably not use Federal waivers unless mandated by the Government.

The FRWG supported the implementation of an Energy Task Force recommendation:

- Government should specify an NS/EP backup fuel requirement in cooperation with industry.

Actions Resulting from NSTAC Recommendations

At the December 12, 1990, NSTAC XII Meeting, members agreed with the recommendation not to pursue a waiver of EPA UST regulations.

Reports Issued

Energy Task Force Final Report, February 1990.

Wireless Security

Investigation Group / *Period of Activity*

Wireless Task Force (WTF)
April 2002 – January 2003

Issue Background

Numerous wireless technologies are being used with greater regularity to transmit voice, data, and video in support of NS/EP operations. However, there are increasing concerns that wireless communications could expose NS/EP users to new security threats and vulnerabilities. As such, the NS/EP community needs to understand its security requirements and identify potential wireless vulnerabilities.

Challenges exist at many levels, including product design, wireless standards, and wireless/Internet convergence. First, the wide use of commercial off-the-shelf products and legacy equipment by the NS/EP community is an important consideration because these devices and equipment were not designed with NS/EP security requirements in mind and sometimes without security features at all. Second, interoperability issues arise from the implementation of different security models and standards—for instance, there are several conflicting policies either established or in development, designed to inhibit or prohibit the use of particular wireless capabilities and connectivity to classified networks and computers. Third, the extension of the Internet into the wireless domain adds new security challenges.

At the NSTAC XXV Meeting held on March 13, 2002, participants discussed the topic of security vulnerabilities in wireless communications devices and networks. Since subscribers use wireless technologies to transmit voice, data, and video in support of NS/EP operations, meeting participants agreed that the NS/EP community needed to identify its security requirements and understand potential wireless vulnerabilities. After an initial scoping of wireless security and other related wireless issues, the NSTAC IES formed the WTF at its April 18, 2002, meeting. The IES tasked the WTF to determine how the NS/EP user can operate in a secure environment and to provide conclusions and recommendations to the President regarding wireless security.

History of NSTAC Actions and Recommendations

To adequately discuss these subjects and formulate actionable recommendations designed to help offset wireless threats and vulnerabilities, the WTF agreed to: (1) define the terms "wireless" and "wireless security;" (2) identify NS/EP wireless users' unique requirements; (3) compile a list of wireless vulnerabilities and threats; and (4) where known, identify mitigation approaches to address wireless vulnerabilities and threats. The task force used the expertise of subject matter experts from NSTAC member companies, as well as other information technology companies, industry associations, and Government participants, throughout its study of wireless security.

After defining NS/EP user requirements, the task force identified advantages to using wireless systems for NS/EP communications, as well as vulnerabilities and threats that must be addressed before using wireless capabilities for mission-critical NS/EP communications. The WTF's findings concurred with other prevalent studies, which determined that any vulnerabilities that exist in conventional wired and computer communications and networks are applicable to wireless technologies.

The WTF concluded that there is a range of wireless security, which varies from effective, practical security on the commercial wireless networks, to significantly less security on the public wireless networks. As such, an NS/EP agency must ensure that its NS/EP communications are secured appropriately for its mission. The WTF also agreed that the extent to which these vulnerabilities have been or can be addressed would be a function of the degree to which organizations with experience in security issues manage the network.

The WTF concluded its analysis of wireless security in January 2003 and presented its findings in its WTF Report on Wireless Security. The task force found that wireless security challenges exist at many levels, including product design, wireless standards, and wireless/Internet convergence. Based on its analysis of issues related to wireless security, the NSTAC offered the following recommendations to the President:

- Direct Federal departments and agencies to construct mitigation and alleviation policies regarding wireless vulnerabilities and further consider the applicability of the recent wireless security policies of the NIST and the Department of Defense to all Federal departments and agencies;
- Direct Government chief information officers to immediately emphasize enterprise management controls, with respect to wireless devices, to ensure that appropriate security controls are implemented, given that the banning of wireless devices is counterproductive and ignores the efficiency that such devices brings to users;
- Direct Federal departments and agencies to work in concert with industry to develop security principles and to resolve security-related deficiencies in wireless devices when employed by NS/EP users;
- Direct Federal departments and agencies using wireless communications to address wireless security threats and vulnerabilities, and to consider the end-to-end security of their respective communications and information system capabilities;
- Direct Federal departments and agencies using wireless communications to purchase and implement fully tested and compliant secure wireless products and services;
- Direct appropriate staff to advocate funding initiatives for replacing non-secure analog with secure digital NS/EP equipment and systems;
- Direct Federal departments and agencies using microwave communications facilities to address unprotected link security vulnerabilities. In addition, advise State and local Governments and other critical infrastructure providers of the vulnerability of unprotected microwave communications as part of the homeland security initiative; and
- Establish policies regarding the public availability and dissemination of Federal critical infrastructure information (such as the policies on Internet availability of the FCC and the Federal Aviation Administration databases of tower locations).

At a December 2, 2002, IES Meeting briefing, the Chair of the President's Critical Infrastructure Protection Board requested that the 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 WTF scoped the issue.

The WTF reported a number of observations on the security of Internet-enabled wireless devices in its *Wireless Task Force Findings: Security of Internet-Enabled Wireless Devices,* January 2003. The task force agreed that it is a serious issue, which is not limited exclusively to "wireless" or "third generation" wireless devices, because any device connected to the Internet can be attacked. The WTF concluded that although the tasking referenced wireless specifically, the NSTAC has already studied the larger issue as it relates to the convergence of telecommunications networks and the Internet. The complete findings based on the task force's initial scoping were forwarded to NSTAC stakeholders for review.

The WTF concluded its activities upon NSTAC approval of its reports and finalization of its findings on the security of Internet-enabled wireless devices.

Actions Resulting from NSTAC Recommendations

NSTAC wireless security recommendations were formed after considerable collaboration with experts from industry and the Government. The recommendations were provided to and well received by other technical and policy advisory groups. For example, the Network Reliability and Interoperability Council (NRIC) VI, which assures homeland security, optimal reliability, interoperability, and interconnectivity of, and accessibility to, the public telecommunications networks, maintained close coordination with NSTAC efforts and recommendations. NRIC's best practices and recommendations complemented NSTAC findings regarding wireless security principles and the resolution of security-related deficiencies in wireless devices.

Reports Issued

Wireless Task Force Report: Wireless Security, January 2003.

Wireless Task Force Findings: Security of Internet-Enabled Wireless Devices, January 2003.

Wireless Services (Including Priority Services)

Investigation Group / *Period of Activity*

Wireless/Low-Bit-Rate Digital Services Task Force (W/LBRDSTF)
March 1991 – October 1991

Wireless Services Task Force (WSTF)
December 1991 – September 1995

Legislative and Regulatory Task Force (LRTF)
February 2001 – Present

Wireless Task Force (WTF)
April 2002 – January 2003

Issue Background

At its March 15, 1991, meeting, the President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) established the Wireless/Low-Bit-Rate Digital Services Task Force (W/LBRDSTF) to address Office of the Manager, National Communications System (OMNCS) concerns about the possible adverse effects of developments in the rapidly evolving wireless telecommunications sector that would impact the public switched network's ability to handle secure voice and data communications. The OMNCS recommended that the task force's charge be to: (1) define the scope of the issues regarding wireless services, and (2) advise the Government on how to minimize any adverse effects of emerging digital mobile communications standards and technologies on mobile national security and emergency preparedness (NS/EP) users.

On October 3, 1991, in its final NSTAC XIII report, the W/LBRDSTF concluded that no Government organization existed for defining NS/EP requirements for wireless digital communications. In addition, the task force determined that compatibility problems existed between certain existing and developing voice/data devices (for example, secure telephone unit [STU]-III analog) and the emerging digital wireless network. Based on the task force's report, the NSTAC recommended that the Government determine the appropriate organization to address and monitor wireless digital interface issues. Accordingly, the Government tasked the OMNCS Wireless Services Program Office (WSPO) with the responsibility.

In December 1991, following the establishment of the WSPO, the IES approved the establishment of a follow-on Wireless Services Task Force (WSTF). The IES tasked the WSTF to provide an industry perspective to the WSPO and to assist in developing a plan of action for addressing NS/EP wireless issues. This included identifying Government requirements and developing a white paper to support standards activities. The IES also instructed the task force to continue its investigation into wireless services supporting NS/EP. To that end, the task force surveyed the evolving wireless services environment and identified and assessed candidate solutions that would ensure interoperability and connectivity among wireless services and between wireless and non-wireless systems. The WSTF, in conjunction with the OMNCS WSPO and the Federal Wireless Users Forum, addressed methods for incorporating priority access into wireless systems for NS/EP use. In addition, they determined the potential for emerging wireless technologies to complement existing communications support in the *Federal Response Plan* (FRP) Emergency Support Function (ESF) #2 (Communications).

The WSTF established the Cellular Priority Access Services (CPAS) subgroup in July 1994 to investigate technical, administrative, and regulatory issues associated with the deployment of a nationwide priority access capability for NS/EP cellular users.

On March 2, 1995, the IES instructed the WSTF to determine the NS/EP implications of, and scope the future task force involvement in, wireless technologies. These technologies include land mobile radio/specialized mobile radio, mobile satellite services, personal communications services, and mobile wireless access to data networks.

At its September 22, 1995, meeting, the IES placed the WSTF on standby status until needed by the Government. At that meeting, the IES also voted to place the CPAS subgroup under the direction of the NS/EP group. Since then, the subgroup has assisted in developing CPAS forms and a manual for the administration of CPAS. Additionally, the subgroup monitored the development and modifications of standards and regulatory issues relevant to CPAS, which is now referred to as Wireless Priority Service (WPS).

The NSTAC revisited WPS issues during the NSTAC XXVI cycle (March 2002–April 2003). After scoping current wireless issues related to NS/EP users, the IES formed the Wireless Task Force (WTF) to study issues relating to the ubiquitous rollout of WPS at its April 18, 2002, meeting. In addition to analyzing the impediments to the ubiquitous rollout of WPS, the IES detailed the task force to study how WPS can be promoted publicly and explore non-device specific and secure solutions for deploying WPS.

History of NSTAC Actions and Recommendations

At the October 3, 1991, NSTAC XIII Meeting, the NSTAC approved the following W/LBRDSTF recommendations to the President:

- The Government should establish a focal point, supported by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), to address and monitor wireless digital interface issues; and

- The Government should formulate policies at a high level to ensure that all wireless digital service acquisition activities take NS/EP needs into account.

The NSTAC reconvened the task force following the establishment of the WSPO.

At the March 4, 1994, NSTAC XVI Meeting, the NSTAC approved the WSTF report and forwarded recommendations to the Government on pursuing implementation of a single, nationwide priority access capability for NS/EP users and expanding the FRP ESF#2 planning process to make more effective use of wireless technologies and services.

At the NSTAC XVII Meeting, held on January 12, 1995, the task force reported on its activities in the areas of wireless interoperability and cellular priority access.

At the NSTAC XVIII Meeting, the WSTF presented its task force report and recommendations on the NS/EP implications of land mobile radio/specialized mobile radio, mobile satellite services, personal communications services, and wireless data to the President. The report had several recommendations related to the Government continuing to actively exploit emerging technologies in support of NS/EP activities by working at the international, Federal, State, and local levels in defining wireless requirements.

Additionally, the subgroup submitted the *Cellular Priority Access Services Subgroup Report,* which recommended the Government continue to gain a consensus on CPAS regulatory, administrative, and technical issues to finalize a comprehensive CPAS implementation strategy.

At the NSTAC XXV Executive Breakfast on March 13, 2002, Senator Robert Bennett (R-UT) requested that the NSTAC revisit the issue of WPS and further examine obstacles to the ubiquitous rollout of WPS. In response to this charge, the NSTAC tasked the WTF with assessing the issues related to the ubiquitous deployment of WPS. The WTF closely monitored the deployment of WPS, noting that the ubiquitous deployment of the program had not been achieved for a variety of operational, technical, funding, and regulatory reasons. WTF members agreed that the ubiquitous, nationwide deployment of WPS would be achieved through the inclusion of all wireless technologies in the solution set, satellite back-up capabilities, and the participation of large and small wireless carriers. Members also cited inadequate Government funding, lack of liability protection for carriers, and technological limitations as additional impediments to the ubiquitous rollout of WPS. Lastly, the WTF determined the need for an effective WPS outreach

campaign to State and local Governments, smaller wireless carriers, private sector critical infrastructure protection providers, and the general public. Providing these entities with timely and accurate information would dispel misconceptions regarding the WPS program and facilitate the inclusion of WPS in various NS/EP homeland security, contingency, and disaster recovery plans.

As a result of this analysis, the NSTAC offered the following recommendations to the President:

- Encourage the development of WPS solutions for all wireless technologies (*e.g.,* cellular/personal communications service, third generation networks, paging, and other wireless data services) to maximize WPS coverage, increase ubiquity, and give NS/EP users the flexibility to handle a variety of emergencies and disasters;

- Reaffirm that the Federal Communications Commission's (FCC) Second Report and Order (R&O) on Priority Access Service (PAS) does extend liability protection to wireless priority solution providers equivalent to liability protection found in wireline priority communications programs;

- Encourage and support adequate funding for the development and deployment of a multi-technology and multi-carrier WPS program, including a satellite backup capability to continue through WPS full operational capability and later generations and integration with the Government Emergency Telecommunications Service (GETS);

- Direct the appropriate departments and agencies to conduct outreach and educational campaigns regarding WPS and its role in homeland security, specifically targeting:

  - State and local Governments—Emphasizing the role of WPS in homeland security and the importance of expediting zoning and siting requests from wireless carriers, including the use of Government sites and buildings, to increase WPS coverage and ubiquity

  - Smaller carriers—Educating them on WPS and encouraging their involvement in the program

  - Private sector critical infrastructure providers—Facilitating greater awareness of the WPS program and enabling improved contingency and disaster recovery programs

  - The general public—Detailing the benefits WPS provides for public safety and homeland security

- Direct the National Communications System (NCS), Government agencies and departments, and organizations with NS/EP missions to implement proactive policies regarding the implementation and use of the WPS program, including:

  - Stockpiling WPS-enabled phones for large-scale distribution to NS/EP users during emergencies

  - Monitoring WPS usage following distribution of WPS handsets to protect against fraud and abuse

  - Developing a WPS directory assistance function, enabling NS/EP users to locate one another during emergencies

- Direct the NCS and Government agencies and departments involved in WPS planning and program management to address the technical limitations of wireless and other network technologies that may have a negative impact on the assurance, reliability, and availability of an end-to-end WPS solution. These limitations include but are not limited to:

  - Insufficient commercial capacity available to support NS/EP users

  - Technical infeasibility of offering wireless priority at the network egress within the initial operating capability time frame

  - Processing limitations of Signaling System 7 (SS7) during periods of congestion

- Security vulnerabilities resulting from the convergence of voice and data networks and the SS7

- Challenges associated with the integration of GETS with WPS.

In addition, the WTF worked jointly with the Legislative and Regulatory Task Force (LRTF) to assess the legal and regulatory concerns with WPS during the NSTAC XXVI cycle. Specifically, they addressed whether the FCC should revise the Second R&O for PAS. The NSTAC reviewed the R&O and, on January 22, 2003, sent a letter to the President offering recommendations on PAS. In the letter, the NSTAC commended the FCC for adopting a Second R&O for PAS, which indicates that carriers providing PAS shall have liability immunity from Section 202 of the Communications Act; states that the FCC and the National Telecommunications and Information Administration (NTIA) should accelerate on-going efforts to improve interoperability between Federal, State, and local public safety communications agencies; and encourages the Administration to support full and adequate Federal funding for PAS.

Actions Resulting from NSTAC Recommendations

A Memorandum of Understanding established the WSPO as the Government focal point within the OMNCS Technology and Standards Division (now the OMNCS Technology and Programs Division), with full-time participation from NSA and NIST.

On October 19, 1995, the OMNCS, through the WSPO, submitted a CPAS Petition for Rulemaking to the FCC to authorize the nationwide CPAS service. After two years of soliciting comments from industry on the CPAS Petition for Rulemaking, the FCC adopted the First R&O for PAS on August 6, 1998.

The OMNCS worked on CPAS implementation through four parallel approaches: modifying cellular standards to incorporate CPAS, encouraging the FCC to issue CPAS rules, developing CPAS administrative processes, and stimulating competitive interests of service providers to implement the CPAS capability.

On July 3, 2000, the FCC adopted the Second R&O for PAS, establishing the regulatory, administrative, and operational framework enabling commercial mobile radio service providers to offer WPS to NS/EP personnel. The R&O also provided WPS priority levels and qualifying criteria to be used as the basis for all WPS assignments. In their rulemaking, the FCC determined that: (1) WPS was in the public interest; (2) WPS offering should be voluntary; (3) carriers should have limited liability if uniform operating procedures were followed; and (4) the NCS is responsible for day-to-day administration of the program.

After the terrorist attacks of September 11, 2001, the NS/EP community had a renewed interest in fully implementing WPS and White House personnel directed the NCS to establish an active program. A WPS-like solution was made available in Salt Lake City in time for the 2002 Olympic Winter Games and the NCS launched an immediate solution in May 2002 in the greater metropolitan areas of Washington, DC, and New York City. As a result of the NCS integration into the Department of Homeland Security (DHS), WPS is now offered through the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. WPS is offered in most major metropolitan markets on the Global System for Mobile Communications platform. The initial carrier for WPS is T-Mobile, which will reach full operating capability in 2004. In addition, the WPS program expanded to additional GSM carriers in 2004, including AT&T Wireless, Cingular, and Nextel. There are also plans to expand WPS to be offered on the Code Division Multiple Access platform in the future.

Reports Issued

Wireless/Low-Bit-Rate Digital Services Task Force Final Report: Towards National Security and Emergency Preparedness Wireless/Low-Bit-Rate Digital Services, September 1991.

Wireless Services Task Force Report, January 1994.

Emerging Wireless Services Report, September 1995.

Cellular Priority Access Services Subgroup Report, September 1995.

Wireless Task Force Report: Wireless Priority Service, August 2002.

NSTAC Implementing and Governing Documentation

Charter of the President's National Security Telecommunications Advisory Committee

I. Official Designation

Under Executive Order 12382, dated September 13, 1982, and Executive Order 13316, dated September 30, 2003, this Committee is officially designated the President's National Security Telecommunications Advisory Committee ("the Committee").

II. Membership and Organization

A. Membership and organization will be in accordance with Executive Order 12382, dated September 13, 1982.

B. There will be an Executive Secretary who will be the Manager, National Communications System, under section 10(e) of the Federal Advisory Committee Act as amended (5 U.S.C. App. II).

C. The Committee will provide such guidance and direction as is necessary and appropriate to ensure the effective functioning of any subcommittee so established. Except where a special rule applicable to such subcommittees appears in an amendment to this Charter, the provisions of this Charter shall apply (with necessary changes appropriate to subcommittees) to the subcommittees.

D. The Chairman of the Federal Communications Commission will be invited to participate in the activities of the Committee and its subcommittees. Agencies and officials of the Executive Branch may also be invited to participate.

III. Objective, Scope of Activity, and Duties

A. The Committee will function in accordance with Section 2 of Executive Order 12382, dated September 13, 1982. The Committee will provide information and advice to the President on all telecommunications aspects affecting national security and emergency preparedness. Key policy statements include, but are not limited to, Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions and National Security Decision Directive Number 97 (NSDD-97), "National Security Telecommunications Policy."

B. The Committee's officers will have the following responsibilities:

1. The Chair will convene, preside at, and adjourn all meetings at his discretion, with the advance approval of the Executive Secretary. However, the Chair will also be obliged to adjourn any meeting the Executive Secretary advises him to adjourn when the Executive Secretary determines an adjournment to be in the public interest.

2. The Vice Chair will act as Chair in the absence of the Chair.

3. The Executive Secretary, who will be the Manager, National Communications System, will attend all meetings and will advise the Chair to adjourn, or will adjourn, any meeting when the Executive Secretary determines it is in the public interest. The Executive Secretary will invite agencies and officials from the Executive Branch to attend the meetings, as he deems appropriate. The Executive Secretary will prepare the minutes of each meeting, the accuracy of which the Chair will certify and that will at a minimum contain: a record of the membership present and the members of the public who participate in the meeting including the interests and affiliations they represent; a description of matters and materials

discussed and the conclusions, if any, reached; and the rationale for any recommendations made by members of the Committee. The Executive Secretary will also maintain copies of all reports which the Committee receives, issues, or approves.

C. The Committee may consult with interested parties, agencies, interagency committees, or groups of the United States Government and with private groups and individuals as the Committee decides is necessary or desirable.

D. The NSTAC will address all matters pertaining to National Security/Emergency Preparedness (NS/EP) Communications (Cyber and Telecommunications). The NSTAC will coordinate NS/EP communications interdependency issues with the National Infrastructure Advisory Council.

IV. Official to Whom the Committee Reports

A. The Committee will report in writing to the President of the United States through the Secretary of Homeland Security, in his capacity as Executive Agent for the National Communications System by Executive Order 13286, dated February 28, 2003.

B. The Committee, and any subcommittees established by the Committee, will work with the Office of the Manager, National Communications System, and appropriate representatives from National Communications System member organizations.

C. Any subcommittee established by the Committee will report to the Committee.

V. Estimated Costs and Staff Support

A. Members of the Committee will serve on it without any compensation for their work and in accordance with Section 3 of Executive Order 12382, dated September 13, 1982.

B. The estimated annual cost of operating the Committee and its subcommittees is $2.6 million, including travel expenses, per diem, contractor support, and staff support.

C. The Department of Homeland Security, in its capacity as Executive Agent for the National Communications System, will supply staff and support functions for the Committee. The estimated annual personnel staffing of such functions is 7.5 staff years, excluding contract support.

VI. Meetings and Termination

A. The Committee will meet approximately every 12 months in person and otherwise at the call of the Chair. Subcommittees will meet as necessary for their assigned responsibilities.

B. Under Executive Order 13385, dated September 29, 2005, effective September 30, 2005, the Committee will terminate on September 30, 2007, unless formally determined to be in the public interest to continue it for an additional period. A continuing need for the advice offered by this Committee is anticipated.

VII. Filing Date

December 14, 2005.

Bylaws of the President's National Security Telecommunications Advisory Committee

Adopted: **July 20, 1983**
Amended: **June 8, 1989**
Amended: **January 12, 1995**
Amended: **April 18, 2000**
Amended: **April 7, 2003**

Article I Organization and Operation

Section 1 The National Security and Telecommunications Advisory Committee (NSTAC) shall be organized and operate in accordance with the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2), Executive Order 12382, 13 September 1982, the Charter of the NSTAC, and these Bylaws.

Section 2 The provisions of the Federal Advisory Committee Act, as amended (5 U.S.C. App. 2), Executive Order No. 12382, 13 September 1982, and the Charter of the NSTAC shall govern in the event of any conflict between the provisions thereof and these Bylaws.

Section 3 The NSTAC shall be supported by an Industry Executive Subcommittee (IES). The IES is authorized to form subordinate Groups, titled Working Groups, Task Forces, or other appropriate title, necessary to carry out the direction provided by the NSTAC and to develop recommendations for the NSTAC in accord with the NSTAC Charter and the IES's mission. The purpose of the IES is to advise the NSTAC on matters concerning procedures, plans, and policies for the telecommunications and information systems that support national security and emergency preparedness. The IES shall meet approximately one month before and one month after an NSTAC meeting. At additional Working Sessions of the Subcommittee of the whole, the IES shall carry out its role as the NSTAC'S principal working body. The IES performs the following functions: identifies, plans, and defines NSTAC issues; strengthens industry and Government coordination; examines legislative and regulatory issues; oversees network security activities; provides feedback on the status of NSTAC recommendations; and directs and oversees the work of subordinate Groups. The IES shall report to the NSTAC and the subordinate Groups shall report to the IES.

Article II Membership

Section 1 The members of the NSTAC shall be appointed by the President in accordance with the provisions of Section 1(a) of Executive Order No. 12382, dated 13 September 1982.

Section 2 Each member of the NSTAC shall have the authority to appoint one member of the IES. The same individual may represent an industry entity on the IES and on one or more subordinate Groups. Except as provided in Article II, Section 5, the membership of the subordinate Groups shall consist of IES members elected by the IES for a term of two NSTAC cycles.

Section 3 Only NSTAC entities may be represented on the IES or subordinate Groups.

Section 4 Members of the NSTAC may not designate alternates. Members of the IES or any subordinate Group may designate an alternate. Such designation must be in writing with a copy provided to the Office of the Manager, National Communications System (OMNCS). An alternate shall have the privileges of a member.

Section 5 Consistent with any applicable security clearance requirements, any member of the IES or his or her duly designated alternate may be accompanied at any meeting by advisors. Any member or alternate may authorize an adviser to speak on behalf of the member or alternate.

Article III Chair and Voting

Section 1 The Chair and Vice Chair of the NSTAC shall be appointed by the President in accordance with the provisions of Section 1(b) of the Executive Order No. 12382, dated 13 September 1982.

Section 2 The Chair of the IES shall be the Deputy Manager of the National Communications System and not number in the count for a quorum nor vote on issues before the IES. At an IES Working Session, the IES member from the NSTAC Chair's company shall chair the Working Session. The Chairs of subordinate Groups formed by the IES will be appointed by the IES Working Session Chair.

Section 3 A quorum of the Committee, the IES or subordinate Group is required to vote on issues being addressed. Except as set forth in Section 5, a quorum is constituted by the presence of more than half of the membership of the Committee, IES or subordinate Group.

Section 4 Only members of the NSTAC, the IES, or subordinate Group may vote. All issues will be decided, and recommendations or decisions made, by a majority vote of those members present at any NSTAC, IES, or subordinate Group meeting.

Section 5 Absent a request for a recorded and/or secret ballot vote, all votes shall be by either a show of hands or by voice vote. Any member may request a recorded and/or secret ballot vote at any time. With or without a quorum at a meeting, the Chair of the IES or subordinate Group may conduct a recorded vote by mail at any time absent objections of any member. In the case of a mail vote, a quorum is constituted by receipt of votes from more than half of the membership. A non-response from an IES or subordinate Group member will be considered a vote in the affirmative.

Article IV Minutes and Reports

Section 1 Committee records will be maintained as set forth in the Federal Advisory Committee Act, 5 U.S.C. App.2.

Section 2 A written summary will be prepared for each IES meeting and meeting of the IES Working Session. Summaries of the meetings will be prepared by the OMNCS and forwarded to members of the meeting body and other participating entities to review for accuracy and completeness.

Section 3 A consolidated annual report of results of all NSTAC activities shall be prepared and distributed to all members, and to any Federal Government entity upon request. Other reports shall be prepared as directed by the NSTAC.

Section 4 All reports except minority reports shall be prepared by the OMNCS and forwarded to the members for review and comment at least 15 days prior to final distribution.

Section 5 Minority reports may be prepared by any industry member(s) and forwarded to the OMNCS. The OMNCS will attach the minority report to the majority report.

Article V Issue Development

Section 1 Issues for consideration by the NSTAC may be suggested by any Government or industry entity, or any other person. The OMNCS will prepare suggested issues into issue papers for consideration by the IES.

Section 2 The IES will review all issue papers and recommend to the NSTAC their approval or disapproval for further consideration, or recommend such other action as is deemed necessary. For issues sent to a subordinate Group for study, analysis and/or the development of recommendations or options, the IES will provide guidance and direction as necessary.

Section 3 Studies, analyses, recommendations, or options developed by any subordinate Group shall be submitted to the IES, by report or briefing, for consideration prior to presentation or submission to the NSTAC.

Article VI Amendment of the Bylaws

Section 1 Amendment of the Bylaws may be proposed by any member of the NSTAC at any time. Such amendments may be adopted or dismissed only by majority vote of the NSTAC.

Section 2 An amendment to the Bylaws shall become effective immediately following its adoption.

Executive Order 12382—President's National Security Telecommunications Advisory Committee

(Amended by Executive Order 12454 as of December 29, 1983, and Executive Order 13286 as of February 28, 2003)

By the authority vested in me as President by the Constitution of the United States of America, and in order to establish, in accordance with the provisions of the Federal Advisory Committee Act, as amended (5 U.S.C. App. I), an advisory committee on National Security Telecommunications, it is hereby ordered as follows:

Section 1. *Establishment.*

(a) There is established the President's National Security Telecommunications Advisory Committee which shall be composed of no more than 30 members. These members shall have particular knowledge and expertise in the field of telecommunications and represent elements of the Nation's telecommunications industry. Members of the Committee shall be appointed by the President.

(b) The President shall annually designate a Chairman and a Vice Chairman from among the members of the Committee.

(c) To assist the Committee in carrying out its functions, the Committee may establish appropriate subcommittees or working groups composed, in whole or in part, of individuals who are not members of the Committee.

Section 2. *Functions.*

(a) The Committee shall provide to the President through the Secretary of Homeland Security, among other things, information and advice from the perspective of the telecommunications industry with respect to the implementation of Presidential Directive 53 (PD/NSC-53), National Security Telecommunications Policy.

(b) The Committee shall provide information and advice to the President through the Secretary of Homeland Security regarding the feasibility of implementing specific measures to improve the telecommunications aspects of our national security posture.

(c) The Committee shall provide technical information and advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability.

(d) In the performance of its advisory duties, the Committee shall conduct reviews and assessments of the effectiveness of the implementation of Presidential Directive/National Security Council 53 (PD/NSC-53), National Security Telecommunications Policy.

(e) The Committee shall periodically report on matters in this Section to the President and to the Secretary of Homeland Security in his capacity as Executive Agent for the National Communications System.

Section 3. *Administration.*

(a) The heads of Executive agencies shall, to the extent permitted by law, provide the Committee such information with respect to national security telecommunications matters as it may require for the purpose of carrying out its functions. Information supplied to the Committee shall not, to the extent permitted by law, be available for public inspection.

(b) Members of the Committee shall serve without any compensation for their work on the Committee. However, to the extent permitted by law, they shall be entitled to travel expenses, including per diem in lieu of subsistence.

(c) Any expenses of the Committee shall, to the extent permitted by law, be paid from funds available to the Secretary of Homeland Security.

Section 4. General.

(a) Notwithstanding any other Executive Order, the functions of the President under the Federal Advisory Committee Act, as amended (5 U.S.C.App. I), except that of reporting annually to the Congress, which are applicable to the Committee, shall be performed by the Secretary of Homeland Security, in accord with guidelines and procedures established by the Administrator of General Services.

(b) In accordance with the Federal Advisory Committee Act, as amended, the Committee shall terminate on December 31, 1982, unless sooner extended.

Antitrust Division

Office of the Assistant Attorney General Washington, D.C. 20530

June 1, 1983

Lt. Gen. William J. Hilsman
Manger, National Communications System
Washington, D.C. 20305

Dear General Hilsman:

In response to your May 2, 1983, letter to Ronald G. Carr, the Antitrust Division has reviewed the April 18, 1983, draft report of the NSTAC Emergency Response Procedures Working Group on the establishment of a National Coordinating Mechanism. In particular, the Division focused on the proposed functions of the National Coordinating Mechanism (NCM) as set out in Section 6, "Conclusions," of the draft report and Annex B.

The views expressed in this letter are preliminary and respond to your suggestion that we provide general guidance to the Funding and Regulatory Working Group prior its June 2, 1983 meeting.

In summary, we believe the functions of a National Coordinating Mechanism, if carried out along the lines suggested in Chapter 6 and Annex B, pose no significant competitive problems that would rise to the level of a possible Antitrust violation if such activities were carried out in a manner designed to minimize any anticompetitive potential and if the appropriate government agencies retain the responsibility for necessary procurement and regulatory decisionmaking.

As we understand it, the NCM would have four organizational components. Overall policy would be set by a General Forum, "an industry-wide organization with widespread membership" which would meet semi-annually to provide the opportunity for members of the communications industry to discuss National Security-Emergency Preparedness (NS/EP) needs. Subordinate to the General Forum would be two standing committees: (1) the Technical Planning Committee, which would focus on matters involving technical interoperability, (2) the Operations Planning and Policies Committee, which would focus on those involving operating methods and procedures relating to NS/EP. A National Coordinating Center (NCC) would be responsible for day to day planning activities and for responding to NS/EP requirements as they occur. The NCC would consist of an operations center located at a government facility and be staffed with representatives of the National Communications System, and "selected representatives of the industry." Carriers not physically present would remain in electronic contact with the NCC. Lastly, a Secretariat would be responsible for administrative coordination and support.

According to Appendix B, the NCM would appear to have four types of functions. The first, would be to provide a coordination point for dealing with communications emergencies, including service disruptions. This activity includes development of the "watch center" operations of the NCC, technical analysis/damage assessments of service disruptions, and coordination or direction of prompt restoration of telecommunication services. (Items 1, 2, 4, 7.) The second basic function would be to coordinate and assist in the provision of time sensitive NS/EP service requests. (Items 8, 11.) The third category is a broader planning function in which the NCM would assist in the development of technical standards and network planning to meet NS/EP needs and to assist the overall development of each carrier's network so as to insure that NS/EP needs are

taken into consideration. (Items 3, 9, 10.) Finally, the NCM would provide a mechanism to supply the government and, potentially, other carriers with critical information about resources available to meet NS/EP needs or emergency requirements. (Items 5, 6.)

The following discussion of these functions, including the issue of the appropriate scope industry membership in the NCM and its component activities, is based on the descriptions set out in the draft report.

From the description, it would appear that the NCM, although sponsored and supported by the government, would largely function as a joint activity among potentially competing members of the telecommunications industry. The antitrust laws do not prohibit collective activity between competing members of an industry simply because they are competitors. Instead, the question asked by the antitrust laws is whether or not the collective activity at issue has the probable effect of lessening competition in the markets at issue. In the case of the NCM, the proposed essential elements recommended by the Working Group do not appear to do so. Rather, they would enable the industry to provide collectively that which each member of the industry could not provide individually, *i.e.,* a nationwide, interoperable system of independent carrier networks in which the resources of all are available to meet this Nation's NS/EP needs. Consequently, the key focus of any antitrust and competitive analysis is on the methods and procedures by which the essential objectives are implemented.

1. Membership. Under the Sherman Act, if joint facilities established by competing firms become essential to participating effectively in markets served by venture's participants, participation in the activity on reasonable terms by all competing enterprises may be mandated. To the extent that participation in the NCM would confer a competitive advantage therefore, exclusion by industry members of competing firms might be of concern. As we understand the proposal, however, the scope of the NCM and its components would be established by the Government to meet public NS/EP needs, not private interests. In such a circumstance, the decision to limit membership in a particular activity should be made by responsible government agencies, rather than by industry participants, themselves, limiting possible antitrust concerns. In turn, the criteria utilized by the sponsoring government agencies should be designed to promote as broad as possible participation in the group, with membership in any activity restricted only to the minimum extent necessary to achieve the objectives of such an activity, *e.g.,* limiting physical presence at an NCC to numbers that prevent the NCC from becoming an operationally unmanageable undertaking. In this regard, we note that the government, as "the purchaser" of NS/EP services should have every incentive to maximize industry participation, and limit participation, if at all, only to ensure that the benefits of the NCM are maximized.

2. Coordination of Service Disruptions and Similar Emergencies. As we understand it, the goal of this function is to ensure that existing communications requirements can be maintained in the face of disruption of the network of one or more carriers as a result of, *e.g.,* equipment failure, natural disasters, sabotage or war. The goal of the NCM in this activity would not be to process service orders to meet added requirements, but to assure that services already ordered by government agencies and the private sector can be provided in the face of adversity. On the facts as set out above, there would appear to be few, if any, competitive or antitrust issues at stake in this type of activity, to the extent the actual restoration and back-up processes do not have the effect of disadvantaging any particular carrier. Consequently, the procedures involved should minimize any possibility that the services of any carrier will be unreasonably excluded from the backup and restoration process.

3. Coordination of Additional NS/EP Requirements. Under this function, the NCM would assist the government in obtaining a quick, coordinated industry response to time-sensitive NS/EP requirements, such as the provision of additional circuits and equipment to areas hit by a disaster, or for Presidential travel or military mobilization requirements. As we understand it, this activity is different from that just described because it

would result in new government orders for additional services or equipment. Here, the competitive and antitrust risks are greater in that, if appropriate safeguards are not adopted, the NCM could theoretically serve as a mechanism for allocating government orders among competing firms to the detriment of the government's interest. Such an allocation could result, if, for example, firms represented at the NCC decided among themselves who would bid for a particular circuit order when several of them could do so, or if failure to have a representative at the NCC would mean that a particular firm, as a result of procedures agreed on by the carriers present at the NCC, would not have the opportunity to bid on the circuit request.

These theoretically possible competitive problems could be minimized to the extent that the relevant government agencies make the procurement decisions and establish the appropriate bidding processes for emergency telecommunications, with the NCM merely supporting those processes and providing a mechanism coordinating an end-to-end response once the government's procurement decisions were made. What should be avoided, therefore, is the adoption by participating carriers, themselves, of practices that would undercut the ability of government procurement officers to obtain such benefits of competition as procurement regulations envisioned in the circumstances at issue. So long as the NCM merely facilitates actions desired by government agencies in their capacity as a purchaser of communications services, antitrust concerns would be minimized.

4. Industry Standard-Setting and Planning. Standard setting to promote interoperability is widespread across a broad spectrum of American commercial activity, including the communications industry. Under the antitrust laws, such standard-setting processes pose few problems if access to the standard setting bodies are available to competing industry members whose products and services are affected by the standard-setting process and to the extent that reasonable procedures are utilized to assure that the competing firms will have the opportunity to present their views before such standards are collectively adopted.

Nevertheless, both competitive and antitrust issues may be raised to the extent that such standard setting becomes a vehicle to place the products or services of a firm at a competitive disadvantage. Where such actions are taken, it can be alleged that the participants in the standard setting process undertook collective action to eliminate a competitor from the market. Such actions should not give rise to antitrust liability to the extent that the actions in question represented reasoned and reasonable choices and were not undertaken for an exclusionary purpose. In some cases, however, the adoption of standards by collective industry action, *e.g.,* for interoperability or interconnection, may result in a choice that will confer relatively greater competitive benefits on one firm or technology. Consequently, competitive risks would be minimized to the extent that the standards adopted responded to specific NS/EP objectives in a manner that maximized carrier flexibility to meet those standards.

5. Information Sharing. Finally, the proposed NCM envisions that a limited amount of carrier information concerning available NS/EP resources will be provided to the NCC. It is also envisioned that a mechanism will be adopted by which individual carrier actions, such as the introduction of new services or the planning of facility routes, may be scrutinized so that the NS/EP consequences of these carrier activities can be reviewed to enhance NS/EP benefits. The fundamental competitive and antitrust concerns regarding such information plans are to ensure that proprietary carrier information is not involuntarily disclosed to competitors, and that voluntary sharing arrangements do not have the effect of reducing competition among carriers in the introduction of new services and the construction of new facilities. Thus, procedures should be adopted to foreclose potentially anticompetitive information disclosures.

For example, it would appear preferable for each carrier to maintain its own inventory of spare circuits, *etc.,* rather than to create a centralized data base of such information, unless access to such a data base was strictly controlled and limited to the carrier concerned or to government employees. Of course, these concerns are

minimized with respect to information that relates not to the overall commercial capabilities of each carrier, but to purely emergency resources, *e.g.,* mobile facilities or the status of equipment dedicated to NS/EP requirements. In this regard, the operating environment of the NCC should be designed to minimize opportunities for informal and unauthorized access by employees of one carrier to the proprietary information of other carriers.

In the same fashion, the opportunities for disclosure of proprietary information to competing carriers in the process of planning new facilities should also be minimized. For example, it would appear prudent for carriers to obtain information from government employees as to appropriate routings for facilities and to base their actions independently upon such recommendations, rather than for competing carriers to agree on facility routings, particularly where the effect would be to require advance disclosure of construction plans to competitors.

In sum, we believe that the proposals outlined in the draft Working Group report can form an appropriate basis for a National Coordinating Mechanism that will meet government NS/EP requirements while minimizing competitive antitrust risks. The Antitrust Division will continue to work closely with your staff, the NSTAC, and other federal agencies to assure that the NCM is implemented in a manner consistent with both our agencies' legal and policy concerns.

Sincerely,

William F. Baxter
Assistant Attorney General
Antitrust Division

NSTAC Membership

The President's National Security Telecommunications Advisory Committee Membership (as of April 17, 2007)

Mr. Gary D. Forsee, NSTAC Chair
Chairman and CEO
Sprint Nextel Corporation

Mr. Randall L. Stephenson, NSTAC Vice Chair
Chief Operating Officer
AT&T, Incorporated

Mr. F. Duane Ackerman
Senior Executive Consultant
for Communications

Mr. James F. Albaugh
Executive Vice President,
President and Chief Operating Officer
Boeing Integrated Defense Systems
The Boeing Company

Mr. Lawrence T. Babbio, Jr.
Vice Chairman and President, Ret.
Verizon Communications, Incorporated

Mr. Gregory Q. Brown
President and Chief Operating Officer
Motorola, Incorporated

Mr. Daniel J. Carroll, Jr.
President and CEO
Telcordia Technologies, Incorporated

Mr. Kenneth C. Dahlberg
Chairman and CEO
Science Applications International
Corporation

Mr. Van B. Honeycutt
Chairman and CEO
Computer Sciences Corporation (CSC)

Mr. Arthur E. Johnson
Senior Vice President
Corporate Strategic Development
Lockheed Martin Corporation

Mr. Clayton M. Jones
Chairman, President and CEO
Rockwell Collins, Incorporated

Mr. Scott Kriens
Chairman and CEO
Juniper Networks, Incorporated

Mr. Howard L. Lance
Chairman, President and CEO
Harris Corporation

Mr. Craig O. McCaw
Chairman
Teledesic Corporation

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

Mr. Craig J. Mundie
Chief Research and Strategy Officer
Microsoft Corporation

Mr. Richard C. Notebaert
Chairman and CEO
Qwest Communications
International, Incorporated

Mr. Donald J. Obert
Group Executive
Network Computing Group
Bank of America Corporation

Mr. Stratton D. Sclavos
Chairman, President and CEO
VeriSign, Incorporated

Mr. Stanley T. Sigman
President and CEO
AT&T Mobility
CTIA – The Wireless Association

Mr. William H. Swanson
Chairman and CEO
Raytheon Company

Mr. Lawrence A. Weinbach
Chairman
Unisys Corporation

Mr. Joseph R. Wright, Jr.
Chairman
Intelsat, Ltd.

2006-2007 NSTAC Executive Report to the President

Executive Report on the 2007 Meeting of the President's National Security Telecommunications Advisory Committee – April 26, 2007

The President's National Security Telecommunications Advisory Committee (NSTAC) met on April 26, 2007, at the U.S. Chamber of Commerce in Washington, DC. The meeting focused on issues surrounding national security and emergency preparedness (NS/EP) communications in this time of an increasingly global communications environment and increased threats to network security. The NSTAC Principals met with Mr. George Foresman, Under Secretary, National Protection and Programs Directorate (NPPD), and Manager of the National Communications System (NCS), Department of Homeland Security (DHS); Mr. James Schlesinger, Homeland Security Advisory Council; Mr. Robert Jamison, Deputy Under Secretary, NPPD, DHS; Mr. Greg Garcia, Assistant Secretary for Cyber Security and Communications, DHS; Ambassador David Gross, United States Coordinator for International Communications and Information Policy, Department of State; Ms. Linda Haller Sloan, Office of Science and Technology Policy (OSTP); and other senior Government officials and reviewed NSTAC activities over the past cycle during the Open Session. During the Closed Session the NSTAC Principals engaged in discussion with Secretary Michael Chertoff, DHS; Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism; Lieutenant General Charles Croom, Director, Defense Information Systems Agency; Mr. Derek Poarch, Public Safety and Homeland Security Bureau Chief, Federal Communications Commission (FCC); Mr. Tom Bossert, Homeland Security Council; Mr. Richard Russell, OSTP; and a number of senior Administration officials. This Executive Report summarizes those presentations and deliberations. Also attached are the recommendations to the President from NSTAC XXX cycle (Attachment 1) and an attendance list of NSTAC Principals (Attachment 2).

2007 NSTAC Open Session

Call to Order/Opening Remarks.

Mr. Gary Forsee, Sprint Nextel Corporation and NSTAC Chair, called to order the 2007 NSTAC Meeting Open Session on April 26, 2007, at 1:15 p.m. at the U.S. Chamber of Commerce in Washington, DC. Mr. Forsee welcomed members of the NSTAC and congratulated the NSTAC membership on celebrating its 25th anniversary.

Mr. Forsee noted that the NSTAC last met via conference call in January during which time the Principals reviewed and approved the *NSTAC Report on Emergency Communications and Interoperability* and held a discussion on the ongoing work in the area of international communications. He informed the members that as follow-on to the discussions in January, the Open Session will include an update on the second phase of the emergency communications and interoperability work and a discussion on the draft findings and recommendations in the area of international communications. The Open Session will also serve as an opportunity to hear remarks from some of the stakeholders. Mr. Forsee then recognized the senior Government officials participating in the Open Session:

- Mr. Foresman;
- Mr. Jamison;
- Mr. Garcia;
- Ambassador Gross;
- Mr. Poarch;
- Ms. Haller Sloan; and
- Lt. Gen. Croom;

Remarks: Mr. George Foresman.

Mr. Foresman thanked the NSTAC for its immeasurable contributions to addressing national security and emergency preparedness (NS/EP) communications in the current unpredictable risk environment. Mr. Foresman then highlighted some of the activities underway within the Department. Specifically, he noted that the Department continues to go through organizational changes that will ensure its proactive stance in managing the current threat environment and has placed increased focus on prevention and protection of both physical and economic assets. The newly formed Office of Cyber Security and Communications (CS&C), under the leadership of Mr. Garcia, includes the Office of Emergency Communications (OEC), which is a new organizational element designed to support the communications abilities of emergency responders and Government officials in the event of natural disasters, acts of terrorism, or other man made disasters, and to ensure, accelerate, and attain interoperable emergency communications nation-wide. The OEC will expedite the establishment of a nationwide interoperable emergency communications framework and will serve as the focal point for these efforts within DHS. Specifically, the OEC will focus on ensuring the development of a clear vision for interoperability at the Federal, State, and local level. Furthermore, the OEC will look beyond technology issues associated with interoperability and will consider governance and organizational solutions.

Mr. Foresman then thanked the NSTAC for its salient recommendations over the past cycle and addressed recent NCS actions to address the recommendations and noted that many of the recommendations, most specifically those related to wireless priority, have been incorporated into the Department's hurricane preparedness efforts. Mr. Foresman noted that the Government has a job to determine its strategic communications needs, vulnerabilities, and risks. Meanwhile, the NSTAC must continue to add value by providing a broad understanding of the communications market and the future of technology.

Mr. Foresman acknowledged the *NSTAC Report on Telecommunications and Electric Power Interdependencies,* noting that the report placed a very practical face on the infrastructure interdependency. Mr. Foresman assured the Principals that the NCS is currently working on an activity which addresses this interdependency and noted that ultimately the Government will provide a strategic framework which will require industry participation to implement. However, Mr. Foresman stated that at this time the Department is not yet ready to brief on the activity.

Mr. Foresman further reported that the Department continues to work on the recommendations put forth in the *NSTAC Report on Global Infrastructure Resiliency.* However, Mr. Foresman added that the NSTAC could further assist the Government in this area through providing guidance and understanding regarding the global nature of the communications infrastructure. Mr. Foresman remarked that, to many within Government, the degree of interconnectivity of the telecommunications infrastructure is not widely understood and that the private sector can add significant value through educating the Government on these global interdependencies.

Mr. Foresman then announced to the NSTAC Principals that following his resignation, Mr. Jamison will serve as acting Under Secretary for the new Directorate. Mr. Jamison has a strong private sector background and will be a great partner to the NSTAC in its continuing efforts. Mr. Foresman concluded by reminding the members that homeland security goes far beyond gates, guards, and guns and seeks to create societal stability, in part through the robustness of response and recovery methods. Mr. Foresman urged the NSTAC to stay the course even among organizational and administration shifts, continuing in its role as a driver in NS/EP policy.

Remarks: Mr. James Schlesinger.

Mr. James Schlesinger, Homeland Security Advisory Council (HSAC), thanked the Principals for the opportunity to address the NSTAC and noted that the NSTAC truly embodies a successful industry/ Government relationship. Mr. Schlesinger commented on the progress that has been made since the

formation of DHS and noted that as a Nation we must remain prepared for change as we are up against an adaptive enemy. Mr. Schlesinger further noted the importance of the distinction between national security and homeland security, stating that the Department of Defense continues to distinguish between homeland security and homeland defense.

Mr. Schlesinger raised several areas of concern recently identified by the HSAC. First, Mr. Schlesinger reviewed the importance of the national space assets to both the national economy and security, noting that the loss of space assets could significantly cripple the United States both economically and militarily, and encouraged the NSTAC to conduct an evaluation of the impact of the loss of space assets and associated terrestrial assets. Mr. Schlesinger then noted the power of globalization and the Internet in increasing the means of adversaries. Terrorists around the world are actively using the Internet to spread messages, recruit members, and provide a platform for planning attacks. He added that the services these adversaries are using are commonly provided by U.S. based service providers, a point which he noted raises questions regarding the United States' role in thwarting these activities. Mr. Schlesinger suggested that the NSTAC could provide some perspective of this issue. Next, Mr. Schlesinger emphasized that the Nation's power grid is particularly vulnerable and any breakdown of the grid could have a catastrophic impact on other sectors, including the communications sector, and suggested that there needs to be an examination into the vulnerability of power grids. Mr. Schlesinger illustrated that the blackout in the Northeastern United States two years ago was a prime example of the damage that can be caused by a major loss of power, and he further noted that the effects of the threat multiply if attacks occur on several power grids.

Mr. Schlesinger then discussed concerns regarding network security and cyber defense and encouraged the NSTAC Principals to pay particular attention to inside threats. Due to the potential for attacks from within the network, the perimeter defense approach should no longer be the sole strategy for network protection. There must be a process in place to scan new software and hardware, as well as screen the workforce, for potential threats.

Mr. Schlesinger concluded the discussion and suggested that the NSTAC take the following additional steps: (1) consider methods for enhancing workforce screening mechanisms at critical infrastructure facilities; (2) continue to provide Government access to telecommunications call records; (3) explore sector interdependencies and the need for collaboration between the major utility sectors; and (4) further address emergency communications and interoperability challenges through assisting DHS with the implementation of emergency communications and interoperability efforts, defining requirement for more robust cellular technologies, and examining the availability of priority communications services during an overload on the Internet Protocol (IP) network, such as during a pandemic.

Ongoing NSTAC Work.

Mr. Forsee turned the discussions to a review of the NSTAC's ongoing work efforts. He thanked the Industry Executive Subcommittee (IES) members for their significant work over the past cycle. At the beginning of the cycle, there were six existing task forces: (1) the Emergency Communications and Interoperability Task Force (ECITF), (2) the Telecommunications and Electric Power Interdependency Task Force, (3) the National Coordinating Center Task Force, (4) the Research and Development Task Force, (5) the Legislative and Regulatory Task Force, and (6) the NSTAC Outreach Task Force. During the course of the cycle, the TEPITF completed its work and sunset. The NSTAC also established one new task force, the International Task Force (ITF), and a working group, the Global Infrastructure Resiliency Working Group. Mr. Forsee thanked the NSTAC Principals who championed these task forces for their extensive insight and leadership. Mr. Forsee then turned the discussion over to a more thorough review of the work in the areas of emergency communications and interoperability and international communications.

Emergency Communications and Interoperability. Mr. Stanley Sigman, AT&T, Inc. and ECITF Co-Champion, provided the Principals with an update on the activities on the NSTAC's work related to emergency communications and interoperability. He commended Mr. Gregory Brown, Motorola, Inc. and ECITF Co Champion, for his exemplary leadership on this vital topic, and thanked the members for their continued valuable contributions to the work.

Mr. Sigman stated that the NSTAC's initial work in the area of emergency communications and interoperability was designed to identify short-term, urgent actions in anticipation of the 2006 hurricane season. Initial recommendations were presented in the Principal-approved *NSTAC Letter to the President on Emergency Communications and Interoperability.* The NSTAC also completed the *NSTAC Report on Emergency Communications and Interoperability,* refining *The Letter's* recommendations and, per White House request, provided input to the *National Emergency Communications Plan.* Mr. Sigman noted that the report was formally approved by the Principals in January 2007. He informed the Principals that the report has been well received and widely-read, and feedback has been both salient and encouraging as the Committee enters the scoping phase of its future efforts in this area.

Mr. Sigman reported that valuable comments from the Executive Office of the President (EOP) have also been used to frame the current work strategy. In discussions with EOP sponsors, potential issues for future NSTAC consideration were raised, and specific NSTAC assistance was solicited in evaluating how IP-enabled capabilities and technologies might play a role in enhancing the interoperability concerns related to emergency communications. Mr. Sigman noted that in response to this EOP request, current work is focusing on IP interoperability technology solutions. Discussions with Government stakeholders have been initiated to gain cross-agency perspectives on the issue.

In addition, Mr. Sigman informed the Principals that the IES leadership met with Mr. Garcia to review the recommendations in the first report. Discussions included review of the need to evaluate whether Executive Order (E.O.) 12472, *Assignment of NS/EP Telecommunications Functions,* requires updating to reflect those new organizational entities that have been granted legislative authority for responsibilities that complement, but also overlap with existing NS/EP roles within DHS and the NCS as authorized under E.O. 12472. In addition, the IES leadership and Mr. Garcia reviewed the NSTAC's recommendation to enhance the Telecommunications Service Priority program for wireless networks and discussed approaches to further move forward with this recommendation.

In conclusion, Mr. Sigman reported that the NSTAC's continued work in the area of emergency communications and interoperability is well underway, and that focus is being given to addressing issues relevant to national security and scoping an approach to ensure development of a streamlined and immediately actionable deliverable. He noted that such a scoping effort is inherently complex in light of the multiple industry and Government efforts to address a range of emergency communications and interoperability concerns and suggested that as the Committee continues to scope the issue it should ensure that the NSTAC does not duplicate efforts underway in other groups. Mr. Sigman thanked the Principals for their contributions and encouraged additional feedback and comments.

A Principal commented on significant Congressional appropriations targeted at resolving emergency communications and interoperability concerns. He noted that the NSTAC may be able to play a role in supporting the effective coordination and targeting of these resources. Mr. Foresman noted that $1.7 billion in funds has been provided to State and local jurisdictions to improve communications capabilities, but recognized that a Federal Government role is necessarily limited in terms of mandating specific use of such grants. Mr. Foresman noted that a key failure of past approaches was the lack of a single visible point of Government orchestration on the issue. The codification of an effective DHS organizational structure is underway and the new OEC is charged with developing a plan and framework to specifically address this concern.

Mr. Foresman commented that an appropriate supporting role for the NSTAC is to support the overall strategic vision through providing industry's estimate of the communications architecture capabilities three, five, and ten years from now. The Principals agreed that in light of the significant resources being programmed to address emergency communications interoperability concerns, additional focus is required on the part of Government and industry to ensure that today's expenditures do not merely "upgrade" the communications incompatibilities that exist today, particularly at the local level.

International Communications.

Mr. Stratton Sclavos, VeriSign and ITF Champion, provided the NSTAC Principals with an update on the NSTAC's work in the area of international communications and the draft *NSTAC Report on International Communications.* Mr. Sclavos expressed his gratitude for the work of many senior IES members and Government stakeholders in examining the issue. Mr. Sclavos continued noting that the draft report was informed by over 25 subject matter experts, extensive U.S. Government participation, and international industry involvement from the UK and Canada.

Mr. Sclavos outlined the NSTAC's initial scoping regarding international communications, noting that the issue developed out of the discussions at the 2006 NSTAC Meeting. Mr. Sclavos stated that the Committee approached the examination of international communications NS/EP issues by: (1) evaluating current U.S. strategies, policies, and frameworks for international collaboration; (2) preparing recommendations to the President to improve international efforts addressing the response to any disruptions of the global infrastructures upon which NS/EP telecommunication and other critical international operations depend; and (3) determining areas for future study.

Mr. Sclavos stated that the work resulted in four key findings, including: (1) the networks on which NS/EP communications services depend are global; (2) private sector information and communications technology (ICT) operators, both U.S. and non-U.S., operate regularly on a global basis; (3) threats to ICT infrastructures originate from global sources, often beyond the reach of U.S. and allied authorities; and (4) the U.S. Government's international NS/EP communications policy and operational response frameworks are not commensurate with the pace of network globalization and technological convergence. Additionally, the ITF developed draft recommendations to the President in three areas: (1) expand participation to and beyond key allies in policy and strategic processes supporting operational coordination and response mechanisms in order to meet global changes taking place in the international ICT environment; (2) encourage broader international use of public private partnership models as illustrated by sector coordinating councils at the policy level and information sharing and analysis centers and similar bodies at the operational level; and (3) create a process to improve global incident response by including on a reciprocal basis key allied governments, U.S. private-sector infrastructure owners, and key non U.S. companies in appropriate operational coordination and response mechanisms, such as cyber watch and warning organizations.

A member noted that similar to the NSTAC's work related to emergency communications and interoperability, the NSTAC's international work has a broad and complex scope. Mr. Sclavos agreed, noting that the complexities and threat vectors surrounding NS/EP communications in an international environment represent a "boil the ocean type of problem" and these issues can best be addressed by dividing the ensuing examination into two areas—policy and operations. Mr. Foresman asked Mr. Sclavos to further discuss the main policy considerations currently under investigation by the NSTAC. Mr. Sclavos noted that one of the major U.S. policy concerns is finding the best mechanisms for working with international players outside of the trusted circle of allies. Mr. Sclavos also noted that with regard to policy issues, the private sector is primarily concerned with the ability of policies to influence Government responsiveness to international communications incidents and threats. Mr. Foresman requested that the NSTAC provide guidance to the Government identifying the top 3-4 priorities, from a private sector perspective, regarding global communications.

The discussion then turned to the issue of the provisioning of NS/EP services in an international environment. A Principal stressed the necessity of drawing a distinction between the national security and the emergency preparedness components of NS/EP. He added that in terms of domestic issues the national security lens is sufficient, but from a policy perspective countries must communicate far beyond their borders and allied partners, and as such the emergency preparedness component of NS/EP is critical and demands a separate review. Mr. Sclavos concurred and added that many countries still lack the ability to cooperate in the wake of international communications incidents. Specifically, Mr. Sclavos referenced VeriSign's work with Macedonia, and noted that the Macedonia government lacked the ability to respond to cyber fraud and required international aid in order to move forward. Mr. Forsee closed the discussion, noting that the dynamic conversation underscored the breadth and depth of the NSTAC's investigation of international communications.

Remarks: Ambassador David Gross.

Ambassador Gross began his remarks noting that this was his third time participating in the Annual NSTAC Meeting. Ambassador Gross commented that the first time he attended an NSTAC Meeting, international communications issues were not a primary focus and expressed his appreciation to the NSTAC for bringing international communications to the forefront of its agenda. Specifically, Ambassador Gross thanked the NSTAC for its work on the draft *NSTAC Report on International Communications,* and stated that this report underscores the issues surrounding international communications and is a solid first step in identifying solutions.

In moving forward, Ambassador Gross stated that while the breadth of the issues surrounding international communications are vast, there are practical steps that can be taken immediately to address NS/EP concerns. Ambassador Gross encouraged all meeting participants to increase their involvement with two global initiatives. The first, the International Telecommunications Union (ITU) is a global, interagency forum whose core competency centers on telephony related issues. The second, the President's Digital Freedom Initiative (DFI) works in the developing world to enable countries to use telecommunications and Internet technologies for economic, social, and political purposes. Ambassador Gross stressed that both the ITU and the DFI lack the depth of U.S. Government and private sector participation and partnership necessary for the articulation and discussion of emerging international communications issues, including cyber security.

Ambassador Gross stated that three distinct groups of countries currently comprise the international communications space. The first group is made up of close allies and the conversation between these countries is ongoing. The second are the "troublesome" countries with whom dialogue is difficult. The third and largest group of countries falls somewhere in the middle. This group has not yet thought deeply about international communications and it is critical that U.S. Government and industry work with these countries to create enabling environments, such as rule of law. Ambassador Gross stressed the need to bring all countries on-line and added that the international communications community is only as strong as its weakest link. Ambassador Gross concluded his remarks, by encouraging a holistic approach to international communications by both Government and industry.

A Principal thanked Ambassador Gross for his remarks, but questioned whether the ITU was an appropriate venue for increased Government and industry participation, as the ITU has traditionally focused on standardization within the telecommunications infrastructure. Ambassador Gross replied that the ITU is a trusted enterprise for the developing world and that the next generation networks issue is implicit in its continued work. Additionally, Ambassador Gross stated that China, Korea, and Japan currently dominate the ITU discussion and additional U.S. involvement is necessary in order to further comprehend the current situation. Another member concurred with Ambassador Gross' comments, adding that the recent appointment of Dr. Hamadoun Touré as ITU secretary general has further broadened the scope of the ITU, making it an appropriate place for continued

U.S. Government and private sector participation and discussion. Mr. Forsee closed the discussion, thanking Ambassador Gross for his remarks.

Adjournment.

Mr. Forsee thanked the Principals and the Government stakeholders for their participation and adjourned the NSTAC Open Session at 2:40 p.m.

2007 NSTAC Closed Session

Call to Order/Opening Remarks.

Mr. Forsee called to order the 2007 NSTAC Meeting Closed Session at the U.S. Chamber of Commerce in Washington, DC, on April 26, 2006, at 3:00 p.m.

Mr. Forsee explained that the NSTAC Closed Session would provide the NSTAC Principals, along with the senior Government officials in attendance, the opportunity to first hear from some senior Government stakeholders and to then discuss, in an environment closed to the public, potential areas for NSTAC examination related to the global network environment and network security. Before commencing the Closed Session discussion, Mr. Forsee introduced the Government stakeholders who joined the meeting for the session:

- Secretary Chertoff;
- Ms. Townsend;
- Lt. Gen. Croom;
- Mr. Bossert;
- Mr. Russell; and
- Mr. Poarch.

Remarks: Secretary Michael Chertoff.

Secretary Chertoff thanked the members for the opportunity to speak to the NSTAC and noted that the Committee continues to serve as a strong example of a truly valuable industry/Government partnership. The NSTAC's continued success in addressing NS/EP communications is critical to improving the resilient posture of our Nation and advancing our prevention, protection, response, and recovery capabilities. Over the past year, the NSTAC has completed several timely and actionable reports in the areas of global infrastructure resiliency, telecommunications and electric power interdependencies, and emergency communications and interoperability. The Department has reviewed the NSTAC's recommendations and the newly organized CS&C is prepared to implement those recommendations that fall under its purview. CS&C is designed to bridge the needs of the communications and information technology sectors, and as our networks converge into the next generation networks (NGN), the Office will be well-positioned as a focal point for addressing communications challenges. Secretary Chertoff informed the Principals that immediate CS&C priorities include implementation of the Sector Specific Plans, which were developed through public/private sector collaboration. Secretary Chertoff further noted that CS&C includes both the National Cyber Security Division and the United States Computer Emergency Readiness Team, a move which effectively consolidates the Department's cyber functions.

Secretary Chertoff further reviewed recent Departmental structural changes and informed the Principals that the *DHS Appropriations Act of 2007* transformed the organizational structure of the Department to better enable a risk-based approach to security and preparedness. Effective this month, the Act established new leadership positions within DHS and transferred several functions into the Federal Emergency Management Agency (FEMA). Furthermore, the Department made additional modifications that include the stand up of the new NPPD as the focal point for the Department's infrastructure protection efforts. The NPPD includes CS&C, the Office of Infrastructure Protection, and US VISIT as well as two new offices—the Office of Risk Management and Analysis, and the Office of Inter Governmental Programs. Secretary Chertoff announced he appointed Mr. Jamison as the new Deputy Under Secretary for NPPD. Mr. Jamison joins the directorate from the Transportation Security Administration, where he has been a proven leader and has successfully analyzed and driven solutions.

Secretary Chertoff acknowledged recent NSTAC recommendations related to authentication and credentialing and reported that the Department has continued to make progress to address the need for common authentication credentials for first responders. Specifically, Secretary Chertoff reviewed the progress of the Department's First Responder Partnership Initiative designed to provide Federal and non-Federal first responders with a standardized identity management process and a common credential for access to incident areas in the event of an emergency. As part of this initiative, DHS and the Department of Defense recently participated in a demonstration with public and private sector participants to validate the functionality of the First Responder Authentication Credential. More than 50 organizations, in over 20 locations across the United States, including the National Capital Region, actively participated in this demonstration, known as *Winter Storm.*

Secretary Chertoff further reported that the Department is leading an interagency review of both the National Response Plan (NRP) and the National Incident Management System (NIMS), which constitute the Department's core response and recovery elements. The Department formed the NIMS Working Group to ensure that NIMS is best prepared to manage the consequences of domestic incidents and to identify linkages as appropriate. Specifically, the working group identified five key issues for consideration: (1) offering better guidance to clarify roles and responsibilities within the NIMS framework; (2) incorporating the concept of preparedness into the NIMS; (3) refining the NIMS for easier use by stakeholders; (4) identifying the relationships between the NIMS and, Homeland Security Presidential Directive 8, *"National Preparedness,"* the NRP, and other Federal response efforts; and (5) emphasizing NIMS training for emergency management, response personnel, disaster workers, private sector, and non-governmental agencies. The NIMS Working Group has since released the second draft of the NIMS Upgrade for nationwide review and comment.

In conclusion, Secretary Chertoff stated that industry/Government partnerships are more critical than ever in the increasingly complex risk landscape. The NSTAC, in particular, serves as an excellent model for such collaboration and the Secretary thanked the NSTAC for its hard work and valuable recommendations.

Remarks: Ms. Frances Fragos Townsend.

Ms. Townsend commended the NSTAC for its 25 years of service and reported that earlier that morning she met with the President, who expressed his appreciation for the NSTAC's essential guidance on NS/EP issues. Ms. Townsend informed the Principals that the President is intent on ensuring that the NSTAC has access to him and his staff and that the members' time is well spent.

Ms. Townsend reviewed four major NSTAC achievements over the last year. She noted that the *NSTAC Report on Global Infrastructure Resiliency* will have a significant impact on the Nation's ability to preserve the integrity of the undersea cable infrastructure. The *NSTAC Report on Telecommunications and Electric Power Interdependencies* will help the Administration address the development of response capabilities in the event of a long-term outage. In addition, the recommendations in the *NSTAC Report on Emergency Communications and Interoperability* will bring policy makers closer to attaining fully operable and interoperable communications in a wide range of crisis situations. Finally, Ms. Townsend commended the NSTAC for its support to the National Infrastructure Advisory Council report, *Prioritization of Critical Infrastructure for a Pandemic Outbreak in the United States,* which generated valuable recommendations for priority vaccine distribution.

Ms. Townsend noted that the increasingly global and converged network environment has resulted in new challenges and threats for NS/EP communications. As the communications and information technology (IT) sectors are increasingly interdependent, the ability of an adversary to harm the U.S. communications infrastructure by manipulating IT products and accessing U.S. network control spaces is enhanced. To address these threats, Ms. Townsend requested that the NSTAC examine at least two issues in the coming cycle. First, policy makers are uncertain how increased

network congestion during a crisis, such as an influenza pandemic, will affect IP based voice communications. Accordingly, the NSTAC should conduct an examination of the availability of critical IP-based services during times of congestion. Second, due to the communications infrastructure's reliance on global positioning systems (GPS), the NSTAC should initiate a scoping effort regarding the communications infrastructure's dependence on GPS and the impact of a loss of GPS on NS/EP communications.

Ms. Townsend concluded her remarks and noted that she looks forward to another year of working with the Committee, receiving its guidance, and continuing to build on the successes of this partnership.

Remarks: Mr. Derek Poarch.

Mr. Poarch thanked the NSTAC Principals for the opportunity to address them and noted that he is now three weeks into his new position as Chief of the FCC's new Public Safety and Homeland Security Bureau. He informed the members that the Bureau is well positioned to address public safety and homeland security issues in the face of evolving technological challenges. However, Mr. Poarch noted that since many network vulnerabilities exist in the commercial realm, it is essential that industry and Government work together to address vulnerabilities and to restore networks following an event.

Mr. Poarch further highlighted the priorities of the new Bureau and noted that restoration of telecommunications services following a disaster is among the Bureau's top priorities. Mr. Poarch informed the members that the FCC already monitors network outages, coordinates spectrum needs, and serves as a communications information clearinghouse as an Emergency Support Function #2 support agency. During the 2005 hurricane season, FCC engineers assisted affected States with communications resource auditing and the Commission continues to work with FEMA on Gulf Coast recovery efforts and training activities. In addition, the new Bureau has initiated efforts to support a restoration training program and is working to promote the availability of priority service programs. Mr. Poarch reiterated the Commission's commitment to work with the NCS and industry to ensure that emergency scenarios are addressed in a coordinated manner.

Mr. Poarch further informed the members that the FCC recognizes the need for policies that will ensure first responders have access to interoperable and mobile communications systems. To address this need, the FCC is extending its outreach efforts to critical partners in the health care and first responder communities. In addition, Mr. Poarch reported that the FCC recently hosted the First Responders Summit in which participants discussed disaster planning and public safety. The FCC plans to hold other summits based on this format to further its outreach efforts, including one on spectrum policy and management in the 700 Megahertz band. Mr. Poarch concluded by stating that these engagements with partners are essential to formulating a nationwide interoperable communications network.

Global Environment and Network Security Facilitated Issue Discussion.

Mr. Forsee initiated the facilitated discussion regarding NS/EP concerns associated with the increasingly global nature of the communications infrastructure and network security. Before turning the discussion over to the members, Mr. Forsee noted that several key issues surfaced during the Open Session, including the availability of IP based technology during times of network congestion; the far-reaching implications of the NGN evolution; the increasing threat of both cyber and physical attacks on the communications infrastructure; and the necessity of continuing industry-Government partnerships to address the global network environment and associated network security requirements.

Mr. Don Obert, Bank of America Corporation, continued the discussion, providing his perspective on the topic of network security from a global financial services perspective. Mr. Obert began his remarks by emphasizing the interconnectedness between countries and economies worldwide. Mr. Obert highlighted that within the financial industry, global financial systems and their supporting networks and business operations systems must be available 24 hours a day and seven days a week to

support the critical communications requirements of global financial markets. Additionally, many companies, including Bank of America, must ensure continued responsiveness to an expanding global workforce and its increased use of and dependence on global telecommunications services.

To illustrate the financial industry's critical dependence on the underlying communications infrastructure, Mr. Obert noted the increased volume of transactions supported by Fedwire, the U.S.-based global transaction system. The international global payment market is a $74 trillion market and the Fedwire system alone, handles over $1 trillion in global transactions daily. Mr. Obert stressed that reliability and availability of the underlying circuits supporting systems such as Fedwire remains a paramount concern to the financial industry. In addition to physical threats to the infrastructure, the emergence of IP-based technologies increases the threat of cyber attacks. A successful physical or cyber attack on the networks supporting Fedwire or similar critical financial systems would have a devastating impact on global financial markets and economies worldwide.

Mr. Obert also discussed the global effect of emerging markets on the U.S. communications infrastructure. For example, India exports $25 billion in information technology services to the United States every year. United States and foreign international investment in India, $11 billion and $7 billion respectively, are up significantly from previous years. In light of this level of investment and an increased dependence on India for information technology services, a disruption in the supporting communications networks could have major global economic and domestic national security ramifications. In short, Mr. Obert underscored the continued need to address the increased interdependence of systems to support and enable the delivery of IT services worldwide.

In conclusion, Mr. Obert suggested that the scope of any future NSTAC examination regarding network security should be broad enough to address the increasingly international nature of threat vectors. Mr. Obert further suggested that consideration should be given to the pace of development for the necessary NS/EP IP-based network infrastructure features to determine if it is adequate to meet the mission critical functions that will be increasingly reliant on the infrastructure.

Mr. Craig Mundie, Microsoft Corporation, continued the discussion, thanking the NSTAC Principals for the opportunity to address the membership. Mr. Mundie noted the increasingly interconnected nature of today's global society, as well as the complexity of global network security. Mr. Mundie referenced the draft *NSTAC Report on International Communications,* stating that this report underscores the need for the United States to move beyond its trusted circle of allies. He stressed the need for a more rational framework for responding to network security threats. Specifically, such a framework must address complex operational policy issues as well as inter governmental coordination response requirements. Currently, there is no defined protocol to discuss and/or address these challenges effectively and on a non-ad hoc basis. Mr. Mundie stated that hackers are increasingly moving toward targeted attacks with a focus on exploitation of critical information. Use of "social engineering" strategies are also becoming more prevalent. Additionally, new threats are more difficult to police as attacks can originate and terminate from any country, and selectively target the layers of the protocol stack from transport up to application layers. Mr. Mundie illustrated the difficulty of a coordinated international response noting the current limitations of Federal law enforcement jurisdiction to address a cyber event that "hops" outside domestic borders.

Mr. Mundie continued discussing research and development (R&D) gaps as they pertain to network security. Mr. Mundie referenced an attack in December 2006 that penetrated supervisory control and data acquisition systems and showcased the difficulty of policing attacks targeted across the entire supply chain, from end user application software to network management and control system software. Mr. Mundie noted that this policing effort is further complicated as the United States lacks sufficient R&D in the development of reliable and secure core software. Mr. Mundie questioned how best to address software validation and verification. He applauded the NSTAC's related efforts regarding the

NGN, but noted that Government follow-up efforts have been limited and that additional Government leadership could promote more effective methods for cooperation to address the issue. Mr. Mundie recommended that the NSTAC champion the development of policy and operational frameworks to support cyber incident response with an end-goal of providing operational recommendations on how to enhance identity management. Mr. Mundie added that there is a critical requirement to ensure that identity management functions address both human and non human users (for example, human users, computers and applications serving as proxies for human users). Mr. Mundie also noted that the transition to hybrid and full IPv6 environments will present both additional security and mobility benefits and operational and management challenges.

Mr. Mundie concluded his remarks by challenging the NSTAC to reevaluate policies and procedures currently in place to respond to the changing international threat environment. He noted that the current "common criteria" approach to develop reliable and secure products/software is antiquated and is not responsive to the evolving threat. Mr. Mundie raised additional questions for consideration: (1) what level of international coordination is necessary; (2) what would an effective international framework look like; (3) what procurement policies can most effectively address the new cyber threat; and (4) is there an NGN equivalent to the Cold War-era "red phone" to support future national security event response. Mr. Mundie noted that the draft *NSTAC Report on International Communications* begins to answer these questions. In closing, Mr. Mundie emphasized that both industry and Government need to transition from a Cold War threat model (or a passive model of monitoring) to a more proactive model of response.

Mr. Forsee thanked Mr. Obert and Mr. Mundie for their insightful remarks. Mr. Forsee noted that two issues continue to surface and demand further investigation: (1) the resilience and capacity of the IP infrastructure, specifically "last mile" capacity and the ability to support mass-telecommuting in the event of a crisis situation such as a pandemic; and (2) the communications infrastructure dependencies on satellite communications and GPS functions/systems. Mr. Forsee recognized the complexity of these problems, but encouraged the Principals to examine the issues through categorizing and evaluating the component parts.

Mr. Russell noted that the President's Council of Advisors on Science and Technology recently approved a report which provides guidance for spending R&D funds associated with information technology. Mr. Russell further noted that Federal Government involvement in software development R&D, particularly as it relates to networks, has been limited as the software industry has traditionally played a leading role.

Mr. Mundie noted that in their remarks both Mr. James Schlesinger, Homeland Security Advisory Council, and Ms. Townsend addressed the last mile capacity issue with specific reference to the NGN. Mr. Mundie questioned: (1) the plausibility of building last mile capacity to support nationwide telecommuter network access and the inevitable "Mother's Day" network congestion issue that will remain unresolved; (2) effective approaches to establish quality of service in the public network environment versus the corporate/Government network environment; and (3) the potential for a Government Emergency Telecommunications Service-equivalent card for computers and applications. Mr. Mundie suggested that the *NSTAC Report on Next Generation Networks* tackles some of these issues, specifically with regard to last mile capacity. Mr. Bossert reiterated feedback received from Ms. Townsend, stating that the last mile capacity issue should not necessarily be viewed in the context of the NGN, but rather as an issue of prioritization. Mr. Forsee stated that these issues also relate to current discussions on net-neutrality. A Principal suggested that the NSTAC can respond to the issue of satellite and GPS dependencies by revisiting its report on satellite survivability, culling lessons-learned from the document, reviewing recent studies by the Defense Science Board, and incorporating a new GPS satellite component.

Lt. Gen. Croom stressed that many of the issues being discussed point to the need for greater Government leadership, noting that the NSTAC has delivered many

solid recommendations to the Government, but the Government has not always adopted and implemented them, in part because of organizational and jurisdictional barriers. As such, Lt. Gen. Croom encouraged DHS and the National Security Agency (NSA) to work together to develop a point of contact for all NSTAC recommendations. The NSTAC Principals agreed that the current structure to review and vet NSTAC recommendations could be enhanced. Mr. Forsee added that DHS and NSA are aware of the problem, and suggested that within the next 30 days, the NSTAC work in tandem with these agencies to evaluate improvements. The Principals concurred.

The Principals continued to discuss the issues of quality of service, service prioritization, and emergency communications interoperability. A member suggested that the private sector could take more responsibility for developing a standard approach to prioritization for some traffic categories (for example, emergency response traffic). Specifically, the member noted that the provision of quality of service over an IP infrastructure is not a "black and white" issue and that implementation approaches will vary. He suggested that a potential approach is to pursue industry wide agreement on a uniform degradation policy that would enable prioritization of select traffic and consistent network behavior during times of crisis. Such an approach would also avoid unnecessary industry involvement in the associated Government policy debate. Mr. Mundie added that such a degradation policy must be engineered into the network and that such a solution should extend beyond voice traffic to data transactions. The solution would require a hierarchical structure and overarching administration policy. Mr. Forsee added that industry could in effect reverse engineer a solution in response to an established Government policy when it is developed.

Participants also identified additional topics regarding developing practical solutions to support Government communications and response capabilities, including the effective application of Congressionally-appropriated resources to support needed emergency response capabilities, the potential benefits and drawbacks of a national operations center to support existing industry operation centers, and the sharing of industry telecommunications call records to support Government response to events. In closing the facilitated issues discussion, Mr. Forsee thanked the participants for their input and feedback and stated that several of the issues identified deserve additional consideration at the IES or task force level. Mr. Forsee stated that framing the issues in alignment with ongoing Government stakeholder guidance and DHS/NSA activities will support the scoping of future NSTAC initiatives.

Adjournment.

Mr. Forsee thanked the Principals and the Government stakeholders for their participation and adjourned the NSTAC Closed Session at 5:00 p.m.

Attachment 1: Report Recommendations to the President from the 2007 Meeting of the President's National Security Telecommunications Advisory Committee – April 26, 2007

The President's National Security Telecommunications Advisory Committee's (NSTAC) examined national security and emergency preparedness (NS/EP) concerns associated with interdependencies between the telecommunications and electric power sectors. Based on the NSTAC's examinations of technological interdependencies that will affect telecommunications networks in the future, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* direct the appropriate departments and agencies to perform the following:

- Commission a Government funded, cross sector and cross border engineering analysis of the North American telecommunications and electric power infrastructures, with attention given to further international considerations, to determine the interdependencies in long term outage (LTO) situations for both the current and the next generation network environment, and to estimate the attendant costs of mitigation strategies, including the following:
  - Investigating how dependencies and interdependencies will be affected by technology and structural changes in both sectors; and
  - Supporting exercises at the local, State, regional, national, and international level that investigate the dependencies and interdependencies between the two sectors during an LTO.
- Analyze and evaluate current governance procedures applicable to an LTO to determine the appropriate transition from local to national management authority during an LTO. Internet recovery issues (as they relate to the convergence of the telecommunications network) should also be reviewed, but such a review should not be limited to an LTO event.
- To reduce dependencies between the sectors and maintain a minimum level of internal service availability during an LTO, vigorously support selected science and technology applications, including the following:
  - Transformer prototype technology;
  - Power conservation technology for telecommunications; and
  - Fuel cell technology.
- In concert with industry, support the advent and development of cross sector situational analysis tools to facilitate information sharing between industry and Government in advance of, during, and after an LTO.
- As stated in the *NSTAC Report to the President on People and Processes: Current State of Telecommunications and Electric Power Interdependencies,* continue to promote increased collaboration between both the telecommunications and electric power sectors and emergency management authorities at the local, regional, State, national, and international levels to facilitate recovery from an LTO.

The NSTAC examined and identified immediate action that could be taken of behalf of the Federal Government to significantly improve the Nation's emergency communications capabilities. Based on its analysis, the NSTAC recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions:*

- **Expand Use of Deployable Communications Capabilities.** Direct the Department of Homeland Security (DHS) to incorporate into its emergency communications plans and programs rapidly deployable, interoperable, mobile communications solutions that will provide reliable communications to emergency responders in the event of a regional catastrophic failure involving complete or significant loss of communications infrastructure. The President should also direct the DHS to expand and enhance use of the Wireless Priority Service (WPS) program in an area(s) of catastrophic critical infrastructure loss and/or damage through multi carrier WPS end to end solutions that facilitate the rapid restoration of essential wireless network elements.

- **Enhance the Telecommunications Service Priority (TSP) Program for Wireless Networks.** Direct the DHS and other responsible Federal agencies to explore enhancements to the TSP program to accommodate expanded requests from NS/EP users of wireless telecommunications services at critical sites. The President should also direct Federal agencies, and encourage State and local agencies, to fully utilize the existing provisions of TSP and to apply for the enhanced wireless TSP coverage provisions as they are developed for use at their critical sites.

- **Improve NS/EP Policy to Support Emergency Communications.** Modernize existing NS/EP policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities. Specifically, additional Presidential policy guidance is required to:

  - Clearly delineate the NS/EP and emergency communications roles and functions of the National Communications System, the National Cyber Security Division, and the new Office of Emergency Communications, as established by the *DHS Appropriations Act of 2007,* and any other DHS organization, such as the Science and Technology Directorate and the Federal Emergency Management Agency, with a role or responsibility in the area of emergency communications;

  - Preserve and maintain critical NS/EP functions and capabilities that support the national leadership; and

  - Ensure executive oversight across the Federal Government for a fully coordinated, integrated, and interoperable emergency response communications function and capability.

- **Include Critical Elements in the *National Emergency Communications Strategy (NECS)* and the *National Emergency Communications Plan (NECP).*** Incorporate the following critical elements in the development, maintenance, and execution of the *NECS* and associated implementation guidance, and direct the DHS and other responsible Federal agencies to incorporate the elements into the *NECP:*

  - Large scale State and regional shared public safety networks and Federal grants;

  - Yearly benchmarks for achieving defined interoperability objectives;

  - Nationwide outreach to support emergency response communications;

  - Consolidation of operations centers to increase coordination and situational awareness; and

  - Identification of specific private sector emergency communications and interoperability support roles.

- **Address Emergency Communications in the Converged Environment.** To encourage responsive emergency communications capabilities in the converged environment, establish and incorporate the following capability objectives into the *NECS* and associated implementation guidance, and also direct the DHS to incorporate the capability objectives into the *NECP:*

  - Support for a significantly expanded user base;

  - Full leveraging of network assets;

- Internet Protocol based interoperability;
- Assured access for key users through priority schemes or dedicated spectrum;
- National scope with common procedures and interoperable technologies;
- Deployable elements to supplement and bolster operability and interoperability;
- Resilient and disruption–tolerant communications networks;
- Network–centric principles benefiting emergency communications; and
- Enhanced communications features.

The NSTAC examined and identified solutions related to NS/EP concerns associated with global infrastructure resiliency. Those recommendations are available upon request from the Office of the Manager, NCS.

Attachment 2: Attendance of Members at the 2007 Meeting of the President's National Security Telecommunications Advisory Committee

Mr. Gary D. Forsee, NSTAC Chair
Sprint Nextel Corporation

Mr. Randall L. Stephenson, NSTAC Vice Chair
AT&T, Incorporated

Mr. Lawrence T. Babbio, Jr.
Verizon Communications, Incorporated

Mr. Daniel Carroll
Telcordia Technologies, Incorporated

Mr. Kenneth Dahlberg
Science Applications International Corporation

Mr. Scott Kriens
Juniper Networks, Incorporated

Mr. Walter McCormick
United States Telecom Association

Mr. Craig T. Mundie
Microsoft Corporation

Mr. Donald J. Obert
Bank of America Corporation

Mr. Stratton Sclavos
VeriSign, Incorporated

Mr. Stanley Sigman
CTIA—The Wireless Association

Mr. Joseph R. Wright, Jr.
Intelsat, Ltd.

Acronyms

Acronym List

AIN . . . . . Advanced Intelligent Networks
AIP . . . . . Automated Information Processing
ASPR . . . . . Agreements, Standards, Policies, and Regulations
ATIS . . . . . Alliance for Telecommunications Industry Solutions
CCS . . . . . Common Channel Signaling
CIAO . . . . . Critical Infrastructure Assurance Office
CII . . . . . Critical Infrastructure Information
CIP . . . . . Critical Infrastructure Protection
CNS . . . . . Commercial Network Survivability
COP . . . . . Committee of Principals
COR . . . . . Council of Representatives
CSI . . . . . Commercial SATCOM Interconnectivity
CSS . . . . . Commercial Satellite Survivability
CTF . . . . . Convergence Task Force
CWIN . . . . . Cyber Warning Information Network
DARPA . . . . . Defense Advanced Research Projects Agency
DDoS . . . . . Distributed Denial of Service
DHS . . . . . Department of Homeland Security
DOC . . . . . Department of Commerce
DOD . . . . . Department of Defense
DOE . . . . . Department of Energy
DOJ . . . . . Department of Justice
DOS . . . . . Department of State
DPA . . . . . Defense Production Act
E.O. . . . . . Executive Order
EC . . . . . Electronic Commerce
ECC . . . . . Enhanced Call Completion
ECITF . . . . . Emergency Communications and Interoperability Task Force
ELS . . . . . Essential Line Service
EMP . . . . . Electromagnetic Pulse
EPA . . . . . Environmental Protection Agency
ERPWG . . . . . Emergency Response Procedures Working Group
ESP . . . . . National Electric Service Priority
ETSI TIPHON . . . European Telecommunications Standards Institute Telecommunications and Internet Protocol Harmonization over Networks
FCC . . . . . Federal Communications Commission
FNI . . . . . Funding of NSTAC Initiatives
FOIA . . . . . The Freedom of Information Act
FRB . . . . . Federal Reserve Board
FRP . . . . . Federal Response Plan
FRWG . . . . . Funding and Regulatory Working Group
FS . . . . . Financial Services
FSTF . . . . . Financial Services Task Force
GETS . . . . . Government Emergency Telecommunications Service
GII . . . . . Global Information Infrastructure
GSA . . . . . General Services Administration
GTF . . . . . Globalization Task Force
GTISC . . . . . Georgia Tech Information Security Center
HPC . . . . . High Probability of Call Completion
HSPD . . . . . Homeland Security Presidential Directive
I&C . . . . . Information & Communications
IA . . . . . Information Assurance
IAIP . . . . . Information Analysis and Infrastructure Protection
IATF . . . . . Information Assurance Task Force
IAW . . . . . Indications Assessment and Warnings
ID . . . . . Identification
IDSG . . . . . Intrusion Detection Subgroup
IDT . . . . . International Diplomatic Telecommunications
IEPS . . . . . International Emergency Preference Scheme
IES . . . . . Industry Executive Subcommittee
IIG . . . . . Information Infrastructure Group
IIS . . . . . Industry Information Security
IN . . . . . Intelligent Networks
IP . . . . . Internet Protocol
IS/CIP . . . . . Information Sharing/Critical Infrastructure Protection
ISAC . . . . . Information Sharing and Analysis Center
ISATF . . . . . Internet Security/Architecture Task Force
ISEC . . . . . Information Security Exploratory Committee
ISP . . . . . Internet Service Provider
ISSB . . . . . Information Systems Security Board
IT . . . . . Information Technology
ITIC . . . . . Information Technology Industry Council
ITPITF . . . . . Information Technology Progress Impact Task Force
LMBATF . . . . . Last Mile Bandwidth Availability Task Force

LRG . . . . . Legislative and Regulatory Group
LRTF. . . . . Legislative and Regulatory Task Force
LRWG . . . . . Legislative and Regulatory Working Group
LTO. . . . . Long-term Outage
MTT . . . . . Mobile Transportable Telecommunications
NAP . . . . . Network Access Provider
NCC . . . . . National Coordinating Center
NCM. . . . . National Coordinating Mechanism
NCO . . . . . National Coordination Office
NCS . . . . . National Communications System
NCSP . . . . . National Cyber Security Partnership
NERC . . . . . North American Electric Reliability Council
NES . . . . . National Energy Strategy
NG . . . . . Network Group
NGN . . . . . Next Generation Network
NGNTF . . . . . Next Generation Networks Task Force
NII . . . . . National Information Infrastructure
NIPC. . . . . National Infrastructure Protection Center
NIST. . . . . National Institute of Standards and Technology
NLP . . . . . National Level Program
NPTF . . . . . National Plan to Defend Critical Infrastructures Task Force
NRC . . . . . National Research Council
NRIC. . . . . Network Reliability and Interoperability Council
NRP . . . . . National Response Plan
NS/EP. . . . . National Security and Emergency Preparedness
NS/VATF . . . . . Network Security/Vulnerability Assessments Task Force
NSA . . . . . National Security Agency
NSDD . . . . . National Security Decision Directive
NSG . . . . . National Security Group
NSIE. . . . . Network Security Information Exchange
NSSE . . . . . National Special Security Events
NSTAC . . . . . National Security Telecommunications Advisory Committee
NSTF. . . . . Network Security Task Force
NTIA. . . . . National Telecommunications and Information Administration
NTMS . . . . . National Telecommunications Management Structure
NWC. . . . . Naval War College
OAM&P. . . . . Operations, Administration, Maintenance, and Provisioning
OMB . . . . . Office of Management and Budget
OMNCS. . . . . Office of the Manager, National Communications System
OS . . . . . Operating System
OSTP . . . . . Office of Science and Technology Policy
OWG. . . . . Operations Working Group
PAS . . . . . Priority Access Service
PCCIP . . . . . President's Commission on Critical Infrastructure Protection
PCII . . . . . Protected Critical Infrastructure Information
PDD . . . . . Presidential Decision Directive
PN . . . . . Public Network
PO . . . . . Program Office
PSN . . . . . public switched network
PSTN . . . . . Public Switched Telephone Network
PWG. . . . . Plans Working Group
QoS . . . . . Quality of Service
R&D . . . . . Research and Development
R&O . . . . . Report and Order
RDTF . . . . . Research and Development Task Force
RDX . . . . . Research and Development Exchange
RDXTF . . . . . Research and Development Exchange Task Force
REWG. . . . . Resource Enhancements Working Group
RP . . . . . Restoration Priority
SAFETY Act. . . . Support Anti-terrorism by Fostering Effective Technologies Act
SATCOM . . . . . Satellite Communications
SCC . . . . . Sector Coordinating Council
SCOE . . . . . Security Center of Excellence
SME . . . . . Subject Matter Experts
SOP . . . . . Standard Operating Procedure
SRWG. . . . . Security Requirements Working Group
SS7. . . . . Signaling System 7
Stafford Act. . . Robert T. Stafford Disaster Relief and Emergency Assistance Act
STF. . . . . Satellite Task Force
STU. . . . . Secure Telephone Unit
TATF . . . . . Trusted Access Task Force
Telecom Act. . . Telecommunications Act of 1996
TEPITF . . . . . Telecommunications and Electric Power Interdependency Task Force
TESP. . . . . Telecommunications Electric Service Priority
TIM. . . . . Telecommunications Industry Mobilization
TIP . . . . . Telecommunications Infrastructure Providers
TSA. . . . . Transportation Security Administration
TSP. . . . . Telecommunications Service Priority
TSS. . . . . Telecommunications Systems Survivability
USSS . . . . . United States Secret Service
UST. . . . . Underground Storage Tanks
VTF. . . . . Vulnerabilities Task Force

W/LBRDSTF . . . Wireless/Low-Bit-Rate Digital Services Task Force
WPS . . . . . Wireless Priority Service
WSPO . . . . . Wireless Services Program Office
WSTF . . . . . Wireless Services Task Force
WTF . . . . . Wireless Task Force
Y2K . . . . . Year 2000
Y2K Act . . . . . Year 2000 Readiness and Disclosure Act

Office of the Manager
National Communications System
Customer Service Division
Mail Stop 8510
245 Murray Lane
Washington, DC 20528-8510

www.ncs.gov/nstac/nstac.html
nstac1@dhs.gov