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

Issue Review

A Review of NSTAC Issues
Addressed Through NSTAC XXVIII

October 2005

Table of Contents

Table of Contents

Table of Contents (concluded)

Executive Summary

Executive Summary

President Ronald Reagan issued Executive Order (E.O.) 12382 on September 13, 1982, which established the President's National Security Telecommunications Advisory Committee (NSTAC) to provide the President with a unique source of national security and emergency preparedness (NS/EP) communications policy expertise. Impetus for the NSTAC's establishment included 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 includes E.O. 12382, as well as additional NSTAC implementing and governing documentation.

Since its inception, the NSTAC has advised four Presidents on issues pertaining to the reliability and security of communications and their impact on protecting the Nation's critical infrastructures — issues that are vital to America's security and economic interests. Today, members of the communications and information technology industries recognize the NSTAC as a model for industry/Government collaboration. Its record of accomplishments includes substantive recommendations to the President, leading to enhancements of the Nation's NS/EP communications, critical infrastructure policies, and related information systems security posture. Such enhancements in operational programs and policy solutions benefit both industry and Government as security requirements for the communications infrastructure evolve.

During the past 23 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. The NCS coordinates the planning of NS/EP communications to support any crisis or disaster. 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 Telecommunications Information Sharing and Analysis Center (Telecom-ISAC), and the Network Security Information Exchanges (NSIE) process. The NSTAC's perspective and its experiences with a wide range of Federal departments and agencies make it 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 threat environment.

The NCS was officially transferred from the Department of Defense to the Department of Homeland Security (DHS) on March 1, 2003. The NCS capabilities are being leveraged in DHS' Information Analysis and Infrastructure Protection Directorate to enhance the cross-Government and private/public efforts to protect critical infrastructures, while ensuring national level NS/EP functions are fully satisfied. Since June 6, 2002 — when President George W. Bush proposed

Executive Summary (continued)

creating DHS — the NCS and the NSTAC have worked with the Bush Administration to ensure a smooth transition of NCS capabilities and partnerships to DHS.

The NSTAC is composed of up to 30 Presidentially-appointed senior executives representing the communications, information services, electronics, aerospace, and banking industries. Collectively, this group is known as the NSTAC Principals. Appendix B provides a listing of current NSTAC members.

The primary NSTAC working body is the Industry Executive Subcommittee (IES), which consists of representatives appointed by each 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 forms task forces and working groups to address specific issues requiring in-depth analyses. During the NSTAC XXVIII cycle, from May 2004 to May 2005, the IES had the following subordinate task forces:

- **The Trusted Access Task Force** examined vulnerabilities related to industry and Government's background screening and credentialing processes for gaining physical access to critical telecommunications facilities, and provided advice to the President on ways to ensure the physical protection of the infrastructure.

- **The Next Generation Networks Task Force** initiated an examination of how the Government can ensure NS/EP telecommunications requirements continue to be addressed on next generation networks (NGN). In addition, the group proposed substantive near-term recommendations to the President regarding facilitating NS/EP communications over converging networks.

- **The National Coordinating Center Task Force** initiated an examination of the direction and structure of the NCC and how it should continue to partner with Government. In addition, the group also undertook the development of a plan for the implementation of the Communications Sector Coordinating Council (SCC) in response to Homeland Security Presidential Directive 7 (HSPD-7).

- **The Legislative and Regulatory Task Force** continued to monitor and analyze legislative and regulatory activities affecting the NS/EP community. In addition, the group developed recommendations to the President on homeland and national security threats posed by open-source critical infrastructure information publicly posted to the Internet.

- **The Research and Development Task Force** held the NSTAC's sixth Research and Development Exchange (RDX) Workshop in October 2004 that focused on

Executive Summary (concluded)

concerns related to cyber security, physical security, integration, and human factors. The NSTAC's RDX Workshops stimulate and facilitate a dialogue among industry, the Government, and academia on emerging security technology research and development (R&D) issues, and often result in programmatic enhancements to our Nation's NS/EP capabilities. In addition, the group developed a Tested Point Paper for NS/EP research and development purposes, and convened a panel discussion of industry and Government authentication experts to examine how the NSTAC can contribute on this issue.

- **The Telecommunications and Electric Power Interdependency Task Force** initiated an examination of near-term and long-term NS/EP issues associated with the interdependency between the telecommunications and electric power sectors.

Many NSTAC recommendations result in operational activities that enhance NS/EP communications and information systems. For example, the NCC, an industry and Government coordination center for day-to-day operational support to NS/EP communications, began as an NSTAC recommendation. The NCC's mission evolved to include the Telecom-ISAC in 2000. The Telecommunications Service Priority (TSP) System, once an NSTAC issue, is also now an operational system. TSP is the regulatory, administrative, and operational framework that authorizes priority provisioning and restoration of communications services for Federal, State, and local Government users, as well as select non-Governmental users. An NSTAC recommendation also resulted in the establishment of separate NSTAC and Government NSIEs. The NSIEs meet regularly to address the threat of electronic intrusions and software vulnerabilities, as well as mitigation strategies to protect the Nation's critical communications and information systems.

Appendix C contains the NSTAC XXVIII Executive Report to the President, which includes summaries of the May 2005 NSTAC Business and Executive Sessions, as well as task force recommendations made to the President during the NSTAC XXVIII Cycle (May 2004 – May 2005).

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
IAIP/NCS
Mail Stop #8510
Department of Homeland Security
Washington, D.C. 20528-8510
www.ncs.gov/nstac/nstac.html
nstac@dhs.gov

Introduction

Introduction

Purpose

This edition of the President's National Security Telecommunications Advisory Committee (*NSTAC) Issue Review* provides a comprehensive report of issues addressed by the NSTAC from its first meeting in December 1982 to its most recent meeting on May 11, 2005. For each active and previous issue addressed by the NSTAC, the following information is provided 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.

Active Issues

During the NSTAC XXVIII cycle from May 2004 to May 2005, NSTAC task forces addressed issues in the following areas:

- **Trusted Access**
- **Next Generation Networks**
- **National Coordinating Center**
- **Legislation and Regulation**
- **Research and Development**
- **Telecommunications and Electric Power Interdependency**

Previously Addressed Issues

Since its first meeting on December 14, 1982, the NSTAC has addressed a wide range of national security and emergency preparedness communications issues. The Committee's findings have provided the President and members of the administration with industry-based expertise and advice on communications and information systems plans and policies. The *NSTAC Issue Review* records the contributions that industry and Government representatives have made to ensure the security and the emergency response capabilities of the Nation's communications and information infrastructure. A review of the issues previously addressed by the NSTAC provides background information on several Government programs and initiatives that have resulted from NSTAC recommendations.

Active Issues

Active Issues

Trusted Access

Investigation Groups

Vulnerabilities Task Force (VTF)

Trusted Access Task Force (TATF)

Periods of Activity

VTF: May 2002—February 2003

TATF: 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 also recognizes 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. The support of such a vast infrastructure requires a diversified work force, and a large portion of that work force requires physical access to telecommunications components in order to perform routine tasks. The need for physical access by such a wide array of individuals has highlighted a lingering concern that the telecommunications infrastructure is vulnerable to malicious acts. Although most companies protect their key facilities and have rigorous access control policies in place, no standard process exists for vetting telecommunications employees, contractors, and vendors to verify that they are trusted members of the organizations they claim to represent.

In March 2003, the Vulnerabilities Task Force (VTF) issued its *Trusted Access to Telecommunications Facilities Report*, which provided several recommendations to the President on securing access to the Nation's critical telecommunications facilities.

The issue of trusted access was again raised at the President's National Security Telecommunications Advisory Committee (NSTAC) XXVI Meeting in April 2003, this time focusing on the need to improve background check processes to further secure critical telecommunications facilities. Following that meeting, the NSTAC created the Trusted Access Task Force (TATF).

History of NSTAC Actions and Recommendations

The issue of trusted access to critical telecommunications facilities was first addressed by the VTF, which recommended that the President:

- Coordinate with industry and State and local Governments to develop guidance for:
  - Creating national standards and capabilities for national security background checks, screening, and National Crime Information Center reviews;
  - Identifying the criteria for inclusion in background checks; and

  - Identifying who should be subject to background checks.

- Lead the research and development and standards bodies efforts to make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of individuals at critical sites.

- Coordinate with industry to develop a national plan for controlling access at the perimeter of a disaster area, in coordination with State and local Governments. This plan should be incorporated in the *Federal Response Plan*.

- Adopt telecommunications service procurement security policy guidelines that provide positive incentives to those companies that follow Network Reliability and Interoperability Council (NRIC) best practices for access control.

In response to these recommendations, 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 Transportation Security Administration (TSA), may be beneficial for industry in mitigating threats to the telecommunications infrastructure. The TSA program mirrors some of the traits within the airline industry that are similar to the telecommunications industry, including a large number of facilities with varying degrees of security and access requirements, as well as a broad range of employees.

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, Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Department of Homeland Security (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 National Coordinating Center for Telecommunications (NCC) 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 United States Secret Service (USSS) was deemed 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.

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.

Reports Issued

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.

Trusted Access Task Force Membership

Chair
Mr. James Payne, Qwest Communications

Vice Chair
Mr. David Barron, BellSouth Corporation

AT&T Corporation
Mr. Harry Underhill

Lucent Bell Labs
Mr. Karl Rauscher

MCI Incorporated
Ms. Joan Grewe

Microsoft Corporation
Mr. William Cooper

Nortel
Dr. John Edwards

Raytheon Company
Mr. Frank Newell

SBC Communications
Ms. Rosemary Leffler

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Corporation
Mr. Todd Colvin

VeriSign, Inc.
Mr. Justin Somaini

Verizon Communications
Ms. Ernestine Gormsen

Other Trusted Access Task Force Industry Participants

BellSouth Corporation
Mr. Mason Griffin

George Washington University
Dr. Jack Oslund

Global Options, Inc.
Mr. Edward Shubert

Lucent Bell Labs
Mr. Richard Krock

MCI
Mr. Frank Swenson

Qwest Communications
Mr. Gene Carmer

Qwest Communications
Mr. Jon Lofstedt

Qwest Communications
Mr. Thomas Snee

SBC Communications
Ms. Suzy Henderson

Telcordia Technologies
Ms. Louise Tucker

Verizon Communications
Mr. James Bean

Trusted Access Task Force Government Participants

Department of Defense
Mr. Paul Grant

Department of Homeland Security
Mr. Keith Hughes

General Services Administration
Ms. Judith Spencer

Department of Homeland Security/
National Communications System
Mr. Donald Smith

Nuclear Regulatory Commission
Ms. Cheryl Stone

Department of Homeland Security/
Transportation Security Administration
Ms. Pamela Friedman

Department of Homeland Security/
Transportation Security Administration
Special Agent Timothy Upham

Next Generation Networks

Investigation Groups

Convergence Task Force (CTF)

Network Security Vulnerability Assessments Task Force (NS/VATF)

Next Generation Networks Task Force (NGNTF)

Periods of Activity

CTF: June 2000—June 2001

NS/VATF: June 2001—March 2002

NGNTF: May 2004—(present)

Issue Background

The convergence of wireless, wireline, and Internet Protocol (IP) networks into global Next Generation Networks (NGN) is causing a shift in the way that governments and critical infrastructures will meet their needs for NS/EP communications today and in the future. The NSTAC previously examined network convergence issues via its Convergence Task Force (CTF) and Network Security Vulnerability Assessments Task Force (NS/VATF). The CTF Report (June 2001) analyzed the potential security and reliability vulnerabilities of converged networks, while the NS/VATF Report (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. Issues presented by convergence and cyber security also arose during the Financial Services Task Force (FSTF) examination of network resiliency to physical disruptions.

To build on this prior work, the NSTAC Principals agreed at the NSTAC XXVII Meeting that a task force should be created to engage subject matter experts (SMEs) in an examination of NS/EP requirements and emerging threats on the NGN.

Accordingly, the Next Generation Networks Task Force (NGNTF) was created to:

- Agree upon a high-level description of the NGN's expected network environment or ecosystem, and its interdependencies, on which NS/EP applications will rely;
- Identify NS/EP user requirements for the NGN; outline how these user requirements will be met both in a mature NGN and in the transition phase; describe how end-to-end services will be provisioned; and explain how the interfaces and accountability among network participants and network layers will work; and
- Examine relevant user scenarios and expected cyber threats, and recommend optimal strategies to meet NS/EP user requirements.

Members agreed that the task force should also explore international issues, both in terms of NS/EP functions that must be provisioned internationally and international threats to the NGN.

History of NSTAC Actions and Recommendations

As an initial step, the NGNTF assembled a group of SMEs and Government stakeholders in August 2004 to discuss NGN issues. As a result of the meeting,

five fundamental issues were identified as essential to the work of the task force: (1) a description of the NGN; (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. Questions from Government stakeholders also arose regarding how NS/EP communications would be affected by the transition to the NGN. Of particular interest were efforts that could be taken immediately to preserve or enhance NS/EP communications for the future. To address stakeholder requests to explore those issues, the NGNTF formed the Near Term Recommendations Working Group (NTRWG) to examine near-term opportunities for using existing technology to improve the security and availability of NS/EP communications on converging networks. The NTRWG also looked at areas where Government involvement was needed in the near term because of the immediacy of events such as NGN standards and systems development activities that may be proceeding without consideration of NS/EP needs.

Based on the NTRWG's analysis of near-term threats and opportunities, the NSTAC 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: (1) gateways; (2) control systems; and (3) 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.

Working groups were created to address the five additional fundamental areas. The working groups will continue exploring their issues into the next cycle, and their conclusions will form the basis for a final report and recommendations that will be submitted to the President in the fall of 2005.

Reports Issued

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 Membership

Chair
Mr. Philip Reitinger, Microsoft Corporation

Vice Chair
Mr. David Barron, BellSouth Corporation

AT&T Corporation
Mr. Harry Underhill

Bank of America, Inc.
Mr. Roger Callahan

BellSouth Corporation
Ms. Cristin Flynn Goodwin

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Lucent Bell Labs
Mr. Karl Rauscher

MCI
Mr. Roger Higgins

Motorola, Inc.
Mr. Ben LaPointe

Nortel
Dr. John Edwards

Northrop Grumman
Mr. Dennis McCallam

Qwest Communications
Mr. Jon Lofstedt

Raytheon Company
Mr. Frank Newell

SBC Communications
Ms. Rosemary Leffler

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Corporation
Mr. John Stogoski

Telcordia Technologies
Ms. Louise Tucker

United States Telecommunications Association
Mr. Thomas Soroko

VeriSign, Inc.
Mr. Michael Aisenberg

Verizon Communications
Mr. James Bean

Other Next Generation Networks Task Force Industry Participants

Alliance for Telecommunications Industry Solutions
Mr. Tim Jeffries

Bechtel
Mr. Fred Wettling

Cingular Wireless
Mr. Brian Daly

Cingular Wireless
Mr. Peter Musgrove

Cingular Wireless
Mr. DeWayne Sennett

Cingular Wireless
Mr. Richard Tam

Cisco Systems
Ms. Robin Roberts

George Washington University
Dr. Jack Oslund

Global Internetworking
Mr. Gary Hale

Hewlett Packard
Mr. Stephen Squires

Idaho National Engineering and Environmental Lab
Mr. Wayne Austad

Internap
Mr. David Frigeri

Juniper Networks
Mr. Martin Schulman

Lockheed Martin
Dr. Catherine Cherry

Lockheed Martin
Mr. Joseph Cramer

Lockheed Martin
Dr. Al Dayton

Lucent Bell Labs
Ms. Cheryl Blum

Lucent Bell Labs
Mr. Stuart Goldman

Lucent Bell Labs
Mr. Douglas Riley

Lucent Bell Labs
Mr. Robert Thornberry

Microsoft Corporation
Mr. Jerry Cochran

North American Electric Reliability Council
Mr. Louis Leffler

Northrop Grumman
Mr. Scott Freeburn

PricewaterhouseCoopers
Mr. James Craft

Raytheon
Mr. Shawn Anderson

Raytheon
Mr. Robert Connors

SBC Communications
Mr. William Chorley

Securities Industries Automation Corporation
Mr. Andrew Bach

Sprint Corporation
Mr. Timothy Bowe

Sprint Corporation
Ms. Allison Growney

Sprint Corporation
Mr. Brad McManus

Telcordia Technologies
Mr. Robert Lesnewich

Telecommunications Industry Association
Mr. David Thompson

VeriSign, Inc.
Mr. Anthony Rutkowski

Verizon Communications
Mr. Bruce Fleming

Next Generation Networks Task Force
Government Participants

Department of Energy
Mr. John Greenhill

Department of Homeland Security/
National Communications System
Mr. Gary Amato

Department of Homeland Security
Mr. Lew Morrison

Federal Communications Commission
Mr. Greg Cooke

Federal Reserve Board
Mr. Kenneth Buckley

Federal Reserve Board
Mr. Charles Madine

General Services Administration
Mr. Douglas Covert

National Coordinating Center

Investigation Groups

National Center for Telecommunications (NCC) Vision Task Force

NCC Vision Operations Support Group (OSG)

Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF)

National Coordinating Center Task Force (NCCTF)

Periods of Activity

NCC Vision Task Force:
October 15, 1996—April 22, 1997

OSG: April 22, 1997—September 23, 1999

IS/CIPTF: September 23, 1999—
May 16, 2000

NCCTF:
December 14, 2004—Present

Issue Background

Following the divestiture of AT&T in 1982, the Federal Government required a national coordinating mechanism (NCM) to support emergency response efforts for NS/EP telecommunications. Consequently, based on an NSTAC recommendation, the NCC, comprised of industry and Government representatives, was established within the National Communications System (NCS) in 1984.

Since that time, threats to the NS/EP telecommunications infrastructure have changed significantly. In May 1998, the President released Presidential Decision Directive (PDD) 63, 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 also be designated the Telecommunications 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 DOD. Homeland Security Presidential Directive (HSPD) 7, issued in December 2003, succeeded PDD–63, establishing 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 2005, 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 the ISAC.

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 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 approach affect the NCC?

History of NSTAC Actions and Recommendations

In 1997, the NCC Vision Operations Support Group (OSG) worked closely with the NCS member organizations and NCC industry representatives to develop a common framework for assessing the NCC's ongoing role in NS/EP telecommunications. The OSG documented its activities and accomplishments in its report discussed by the Principals at the December 11, 1997, NSTAC XX Meeting.

The NSTAC approved the OSG's report, recommending 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 Subgroup worked closely with the Office of the Manager, NCS (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 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.

At the same time, the OSG's NCM Subgroup met jointly with the Information Infrastructure Group's (IIG) Information Assurance (IA) Policy Subgroup to produce a joint report which 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, Industry Executive Subcommittee (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. 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, 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 required under PDD–63. The NSTAC approved the OSG's September 1998 report 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.
- 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.

During the NSTAC XXII cycle, the OSG concluded that the NCC already performed the primary functions of an ISAC for the telecommunications sector and that the Federal Government should establish it as such.

The NSTAC established and charged the Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force, during cycle XXIII, with developing recommendations leading to significant advances toward the goals of PDD–63, including mechanisms and processes for protected, operational information sharing to achieve these goals and for furthering the role of the NCC as an ISAC for telecommunications and to continue interaction with Government leaders responsible for PDD–63 implementation. In its final report, the IS/CIP Task Force agreed with the conclusion made previously by the OSG during the NSTAC XXII cycle that participation in the ISAC should be expanded during subsequent phases to include a broader spectrum of information and communications industry companies. Participation in the ISAC should include providers and operators of wireless services, Internet services, data transmission services, cable services, and providers of database and gateway services to infrastructure operators. The Federal Government officially established the NCC as the Telecom ISAC in January 2000.

Reports Issued

Operations Support Group Report, December 1997.

IA Policy Subgroup of the Information Infrastructure Group and the NCM 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.

The task force will continue exploring these issues into the next cycle, and its conclusions will form the basis for a final report and recommendations that will be submitted to the President in the fall of 2005.

National Coordinating Center for Telecommunications Task Force Membership

Chair
Mr. James Bean, Verizon Communications

Vice Chair
Mr. John Stogoski, Sprint Corporation

AT&T Corporation
Mr. Harry Underhill

BellSouth Corporation
Ms. Cristin Flynn Goodwin

The Boeing Company
Mr. Robert Steele

Cingular Wireless
Mr. James Bugel

Computer Sciences Corporation
Mr. Guy Copeland

Cellular Telecommunications and Internet Association
Mr. Christopher Guttman-McCabe

Lockheed Martin
Dr. Al Dayton

Lucent Bell Labs
Mr. Richard Krock

MCI Incorporated
Mr. Roger Higgins

Microsoft Corporation
Mr. Philip Reitinger

Nortel
Dr. John Edwards

Raytheon Company
Mr. Frank Newell

Qwest Communications
Mr. Thomas Snee

SBC Communications
Ms. Rosemary Leffler

Science Applications International Corporation
Mr. Henry Kluepfel

United States Telecom Association
Mr. David Kanupke

VeriSign, Inc.
Mr. Michael Aisenberg

Other National Coordinating Center for Telecommunications Task Force Industry Participants

George Washington University
Dr. Jack Oslund

Telecommunications Industry Association
Mr. Daniel Bart

Telecommunications Industry Association
Mr. David Thompson

Qwest Communications
Mr. Jon Lofstedt

Verizon Communications
Ms. Ernestine Gormsen

National Coordinating Center Task Force Government Participants

Department of Homeland Security/
Infrastructure Coordination Division
Ms. Christina Watson

Department of Homeland Security/
National Communications System
Mr. Jeffrey Glick

Department of Homeland Security/
National Communications System
Mr. Donald Smith

Department of Homeland Security/
National Cyber Security Division
Mr. Michael Lombard

Federal Reserve Board
Mr. Charles Madine

General Services Administration
Mr. John Migliaccio

General Services Administration
Mr. Thomas Sellers

Office of Management and Budget
Ms. Kimberly Johnson

Office of Science & Technology Policy
Mr. Mark LeBlanc

Office of Science & Technology Policy
Ms. Linda Haller

Telecommunications and Electric Power Infrastructure Interdependencies

Investigation Groups

Telecommunications Systems Survivability (TSS) Task Force

Energy Task Force

Telecommunications and Electric Power Interdependency Task Force (TEPITF)

Periods of Activity

TSS: March 6, 1986—June 8, 1989

Energy Task Force: August 31, 1988—March 29, 1990

TEPITF: January 15, 2005—Present

Issue Background

For decades, professionals in the telecommunications industry, being cognizant of the interdependencies between the telecommunications and electric power infrastructures, have been concerned with the potential impact on telecommunications network services in the event of a sustained power grid outage, whether due to either natural or man-made events. Two recent events, the long-term power outage in Eastern Canada in January 1998 and the hurricanes that battered Florida and the Gulf Coast during the month of September 2004, again drew attention to the interdependencies between the two sectors and re-energized industry and Government's efforts to find strategies to mitigate against further occurrences.

In addition to the natural threats to the infrastructure, changing trends in network design also raise questions about the continued reliance of the telecommunications sector on electric power sources. With the growth of the NGN, the attendant increase of wireless and mobile technologies, and the dispersion of network elements, the network and the users will increasingly rely on commercial electric service to supply the power needs. In this environment, the telecommunications and electric power sectors will have to increasingly work together to ensure NS/EP services are available to respond to terrorist incidents or natural disasters. While policy currently exists giving the President authority to restore telecommunications services, a commensurate authority does not exist for the electric power sector. The Telecommunications Electric Service Priority (TESP) program is being revitalized by the NCS, and re-characterized as an operational, response driven system. However, since the program is a queuing management system for priority restoration, it does not address other important issues including information sharing, data allocation, and operational and liability issues.

In response to these varied concerns, the NSTAC IES convened a scoping group to determine the need to establish a task force to investigate any NS/EP issues associated with the interdependencies between the telecommunications and electric power sectors. Following development of a report by the scoping group, the IES voted to create the Telecommunications and Electric Power Interdependency Task Force (TEPITF).

History of NSTAC Actions and Recommendations

NSTAC consideration of the interdependencies between the telecommunications and electric power sectors began in 1984 with the NSTAC's response to a Government request for industry's perspective on the options available to industry and Government for improving the Electro Magnetic Pulse (EMP) survivability of the Nation's telecommunications networks.

The NSTAC gave further consideration of the interdependency between the telecommunications and electric power sectors in 1986 with the Telecommunications Systems Survivability (TSS) Task Force which 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.

Following the President's reply, the NSTAC formed the first Energy Task Force and charged it with developing recommendations to mitigate the effects of electric power outages on telecommunications. In 1988, the task force, with participation from the Department of Energy (DOE), the NCS, and the North American Electric Reliability Council (NERC) examined interdependencies between the electric power and telecommunications sectors after a major earthquake.

In October 1991, the NSTAC established a follow-on Energy Task Force charged 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. The NSTAC Principals approved the *Energy Task Force Final Report* in 1993.

In December 1993, DOE began implementing the TESP initiative and made plans to update the critical facilities list, and in 1996, the NCS created a database matching utilities with critical telecommunications facilities. The TESP system fell into disuse in the late 1990's; however, it was revived by the NCS in 2004, based on a foundation of situational awareness. A plan has been set for re-implementation of TESP in 2005.

Interdependency issues recently arose again as a result of extensive power and telecommunications outages during the hurricane season of August and September 2004 in the southeast region of the United States. Mr. F. Duane Ackerman, Chairman and Chief Executive Officer of BellSouth and Chair of the NSTAC, highlighted the concerns in his speech at the Research and Development Exchange (RDX) Workshop in October 2004. Due to the dependence of telecommunications on electric power, Mr. Ackerman noted the need for enhanced and alternative, emergency power technologies. In addition, as the network becomes increasingly distributed, 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.

The TEPITF was created to examine the following issues:

Near-term issues:

- Priority Restoration: Where does the telecommunications network fall in the electric power sector's queue of priority restoration? Who is primarily responsible for restoration of service problems when both sectors or multiple nations, are involved? How do the people who restore service and respond to outages within each sector work together during emergencies? What are the ongoing implications of implementing the TESP program?
- Liability: What, if any, are the liability issues for interdependencies between the two sectors?
- Information Sharing: How much information is currently shared between the two sectors' ISACs? What information should be shared between the two ISACs?
- NSTAC Recommendation follow-up: What actions have been taken by the Executive Branch on previous NSTAC recommendations regarding the energy sector? Which recommendations that have not been acted upon remain relevant?

Long-term issues:

- Decreasing dependency: What, if any, actions can/should the President take to lessen dependency on the commercial power grid during an emergency?
- Industry changes: Have technology-driven changes in the telecommunications sector (e.g., ubiquitous deployment of wireless, terrestrial transition to fiber optic networks, provision of broadband services by the energy sector, distributed network elements, and increased complexities through the introduction of the NGN created new kinds of interdependency vulnerabilities? Are the vulnerabilities simply more of the same, or on a larger scale?
- Science and Technology (S&T) Solutions: What programs or projects underway in the Federal Government research labs represent potential solutions to existing and new interdependency vulnerabilities? What new S&T initiatives should be undertaken?

The task force will continue exploring these issues into the next cycle, and its conclusions will form the basis for a final report and recommendations that will be submitted to the President in the fall of 2005.

Telecommunications and Electric Power Interdependency Task Force Membership

Chair
Dr. John Edwards, Nortel

AT&T Corporation
Mr. Harry Underhill

BellSouth Corporation
Mr. David Barron

BellSouth Corporation
Ms. Cristin Flynn Goodwin

Computer Sciences Corporation
Mr. Guy Copeland

Lucent Bell Labs
Mr. Richard Krock

Motorola, Inc.
Mr. Ben LaPointe

Qwest Communications
Mr. Jon Lofstedt

Raytheon Company
Mr. Frank Newell

SBC Communications
Ms. Rosemary Leffler

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Corporation
Mr. William Hitchcock

Sprint Corporation
Mr. John Quigly

United States Telecommunications Association
Mr. David Kanupke

Other Telecommunications and Electric Power Interdependency Task Force Industry Participants

American Public Power Association
Mr. Michael Hyland

ConEdison
Mr. Peter Hofmann

Edison Electric Institute
Mr. Larry Brown

Edison Electric Institute
Mr. Mark Razeghi

Electric Power Research Institute
Mr. Wade Malcom

George Washington University
Dr. Jack Oslund

Independent Electricity System Operator
Mr. Stuart Brindley

Industry Canada
Mr. John Klurer

Industry Canada
Ms. Maggie Lackey

Industry Canada
Mr. Robert Leafloor

North American Electric Reliability Council
Mr. Louis Leffler

National Rural Electric Cooperative Association
Mr. Barry Lawson

New York Independent System Operator
Ms. Bonnie Bushnell

PEPCO
Mr. Richard Kafka

PEPCO
Mr. George Gacser

Telecommunications and Electric Power Interdependency Task Force Government Participants

Department of Homeland Security/
Office of the General Counsel
Mr. David Delaney

Department of Homeland Security/
National Communications System
Ms. Michele Bruich

Department of Homeland Security/
National Communications System
Mr. Dale Barr

Department of Homeland Security/
National Communications System
Mr. Edward Jacques

Department of Homeland Security/
National Communications System
Mr. Gabriel Martinez

Research & Development 1990-2005

Investigation Groups

Network Security Task Force (NSTF)

Network Security Group (NSG)

Network Group (NG), Intrusion Detection Subgroup (IDS)

Research and Development Exchange Task Force (RDXTF)

Research and Development Task Force (RDTF)

Periods of Activity

NSTF: February 21, 1990—August 26, 1992

NSG: December 1994—April 22, 1997

NG, IDS: April 22, 1997—September 23, 1999

RDXTF: July 18, 2000—July 29, 2003

RDTF: July 29, 2003—Present

Issue Background

Periodically, the NSTAC conducts its 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 NSTAC has traditionally invited 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), Defense Advanced Research Projects Administration (DARPA), and the National Institute of Standards and Technology (NIST). During 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, clear, realistic, actionable recommendations for actions 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, and 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 IES determined that it would again be useful to address network security R&D issues and charged the Network Security Group (NSG) with facilitating 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; (3) identify additional network security R&D activities needed.

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

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. The NG 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 task force's recommendations reinforced prior NSTAC recommendations to examine the need for and feasibility of collaborative R&D approaches for security technology and 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 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 for training more information technology (IT) security professionals, creating large-scale test beds to test security products and solutions, and promoting 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 and 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 NSTAC's fourth RDX Workshop examined issues of transparent security in a converged and distributed network environment and 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 Exchange included the establishment of NSTAC task forces to address standards and best practices for network security.

The NSTAC's 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 event examined trustworthiness from four different perspectives: cyber and software security, physical security, integration issues, and human factors. From this event, the NSTAC 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. The task force finalized recommendations for a joint, collaborative, distributed industry, Government, and academia pilot testbed that could advance the current state of NS/EP and CIP integration activities.

The most recent 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 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 RDTF is currently evaluating whether the NSTAC should conduct an analysis of authentication and identity management security concerns unique to NS/EP telecommunications.

History of NSTAC Actions and Recommendations

Following the 2003 RDX Workshop in Atlanta, Georgia, the NSTAC 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/Proceedings 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 Task Force Membership

Chair
Mr. Guy Copeland, Computer Sciences Corporation

Co – Vice Chair
Dr. John Edwards, Nortel

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

The Boeing Company
Mr. Robert Steele

Lucent Bell Labs
Mr. Kevin Kelly

Motorola, Inc.
Dr. Robert Kubik

Microsoft Corporation
Mr. Theodore Tanner

SBC Communications
Ms. Rosemary Leffler

VeriSign, Inc.
Mr. Michael Aisenberg

Verizon Communications
Mr. James Bean

Other Research and Development Task Force Participants

Georgia Institute of Technology
Dr. Seymour Goodman

Department of Homeland Security/ Science and Technology Directorate
Ms. Annabelle Lee

Office of Science and Technology Policy
Dr. Simon Szykman

Legislation and Regulation 2000-2005

Investigation Groups

Legislative and Regulatory Working Group (LRWG)

Legislative and Regulatory Task Force (LRTF)

Periods of Activity

LRWG: September 23, 1999—February 14, 2001

LRTF: February 15, 2001—Present

Issue Background

Within the evolving telecommunications marketplace and infrastructure, it is important that legislative and regulatory policies progress to ensure continued fulfillment of NS/EP requirements. Therefore, the NSTAC monitors the regulatory environment and various legislative and regulatory activities that could impact NS/EP services, operations, and communications, and also considers areas for which there is a need for legislative and regulatory action. For instance, the apparent lack of Web publishing regulations and guidelines for Federal departments and agencies is of primary concern to the NSTAC. Consequently, the NSTAC focused on analyzing the threat presented by publicly available critical infrastructure information on the Internet and how this threat could be mitigated through the development of Federal Web publishing and access guidelines.

History of NSTAC Actions and Recommendations

At NSTAC XXII, the IES reported its intent to examine the following legislative and regulatory issues:

- Options for eliminating barriers to information sharing for CIP;
- Information sharing for critical infrastructure protection (IS/CIP) legal and regulatory issues pending before Congress; and
- The definition of foreign ownership within the telecommunications industry and how it affects NS/EP communications.

The IES also agreed to continue monitoring the regulatory environment surrounding network convergence for any impact on NS/EP communications. During the NSTAC XXIII cycle, the Legislative and Regulatory Working Group (LRWG) addressed these issues and others at the request of other NSTAC task forces.

The LRWG examined impediments to information exchange, especially critical infrastructure information sharing. The group undertook an in-depth analysis of *The Freedom of Information Act* (FOIA), examining FOIA's potential to hinder industry information sharing with the Government. In accordance with FOIA, the public can request and gain access to records maintained by Government departments and agencies. Such potential disclosure of data deters industry from sharing 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 and potential legal solutions. As a result of their deliberations, the LRWG 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 IS/CIPTF, which addressed the issue in its May 2000 report to NSTAC XXIII.

In addition to analyzing FOIA, the LRWG worked with the DOJ to examine antitrust and liability issues as impediments to information sharing between industry and the Government.

The LRWG also examined foreign ownership regulations and their impact on NS/EP. The group examined domestic regulatory history and analyzed several mergers and acquisitions between domestic and foreign telecommunications carriers. The group found 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, which addressed the issue in its May 2000 report to NSTAC XXIII.

At its February 15, 2001, meeting, the IES approved the transition of the LRWG to a standing body, the Legislative and Regulatory Task Force (LRTF). The LRTF agreed to address the following taskings:

- Examine whether existing legal and regulatory authority is adequate to ensure NS/EP requirements will be met in the converged and NGN environment;
- Identify and address other legal and regulatory issues related to convergence, as appropriate;
- Analyze CIP legal and regulatory issues pending before Congress and the Administration and those, if any, to be recommended for NS/EP implications;
- Consider the legal issues discussed at NSTAC RDX Workshops, including linked or third party liability and new privacy legislation and regulations; and
- Address legal and regulatory issues affecting the other IES task forces at their requests.

During the NSTAC XXIV and XXV cycles, addressing barriers to information sharing such as FOIA, liability, and anti-trust continued to be an important topic. The LRTF monitored pending FOIA legislation from the 106th and 107th Congresses and heard from Congressional staff on the status and outlook of this legislation. The NSTAC also participated in correspondence with the President concerning information sharing legislation. On August 7, 2000, the NSTAC sent a letter to President Bill Clinton asking him to support legislation that would protect critical infrastructure protection information

voluntarily shared with the Government from disclosure under FOIA and limit liability. After 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 by noting 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 Chair encouraged the President to continue to support information sharing legislation.

The LRTF also examined whether the current legal and regulatory environment is adequate to ensure NS/EP services in the converged and NGN environment and produced a report offering an analysis of the issue. The LRTF coordinated with participants in the Government's Convergence Task Force, who discussed the status of the Government's work in the area of network convergence and the assurance of NS/EP communications services. The LRTF concluded in its documentation that until the standards for packet-based services are established and the Government's requirements in the evolving environment are certain, new legislation or regulation is 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 are extremely complex and might require further study. The LRTF shared its analysis with the NSTAC NS/VATF, which incorporated its analysis into the NS/VATF's March 2002 report to NSTAC XXV.

During the NSTAC XXVI cycle, the LRTF examined existing legal penalties for committing Internet attacks to determine whether those penalties should be strengthened or whether additional penalties were needed. The LRTF drafted a report, *Penalties for Internet Attacks and Cyber Crime*, in which the NSTAC concluded sufficient legal authority exists to penalize and deter those who commit cyber crimes. The LRTF also made additional recommendations for pursuing a well-rounded and proactive approach to combating cyber crime. The LRTF recommended the President:

- Increase prosecution of cyber crime at the State level and allot additional funds to the States to better train personnel to combat cyber crime;
- Encourage Congress to ratify the Council of Europe's *Convention on CyberCrime* and implement legislation to reimburse communications service providers for costs incurred in responding to data preservation requests;
- Encourage other nations to adopt policies and procedures to better mitigate and respond to cyber crimes; and
- Encourage companies to implement cyber security best practices.

In addition to addressing existing legal penalties for committing Internet attacks, the LRTF was tasked by the Wireless Task Force to assess the legal and regulatory aspects of the Federal Communications Commission (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, it concluded that revisiting the rules would be a lengthy process and doing so could unintentionally slow the deployment of Wireless Priority Service (WPS). As a result of its 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. The letter also states 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 encourages the Administration to support full and adequate Federal funding for wireless PAS.

The LRTF continued to examine information sharing in the NSTAC XXVI and NSTAC XXVII cycles. During these cycles, Congress passed the *Critical Infrastructure Information Act* (CII Act), which provided additional FOIA and liability protections for companies that voluntarily share critical infrastructure information with DHS. After the CII Act was enacted, the LRTF assessed whether additional information sharing barriers remained and also examined other legal and nonlegal barriers for the purposes of homeland security. During the NSTAC XXVII cycle, the LRTF drafted a report, *Barriers to Information Sharing*, in which it made a series of recommendations for improving the exchange of CII between industry and the Government and for protecting CII that is voluntarily provided to the Government by critical infrastructure owners and operators. The LRTF recommended the President direct the appropriate departments and agencies, in coordination with industry, to:

- Develop a process to resolve multijurisdictional (Federal, State, local) conflicts within the appropriate boundaries of federalism and national, homeland, and economic security;

- Work with Congress to modify the CII Act so that DHS is the clearinghouse and dispenser of CII information;

- Encourage Congress to extend protection of the CII Act to cover departments and agencies other than DHS; and, if other agencies should be designated as such, the NSTAC recommends that they adopt the same rules and procedures as DHS for handling CII; and

- Work diligently with Congress to ensure the CII Act's FOIA exemption and liability provisions remain intact.

During the NSTAC XXVII cycle, the LRTF also 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 LRTF determined that policy conflicts existed, and that they were mainly the result of overlapping and contradictory policies and regulations at the Federal, State, and local levels. On October 16, 2003, the NSTAC

sent a letter to President George W. Bush recommending that he ask the Homeland Security Council, the National Security Council, and Federal departments and executive agencies, including independent agencies, to do the following:

- Evaluate proposed policies and regulations to ensure that homeland security and NS/EP implications have been consolidated;
- Complete a review of existing policies and regulations for potential cross-sector conflicts with homeland security and NS/EP priorities and work with DHS to promptly resolve any identified conflicts; and
- Implement a framework to resolve multijurisdictional (Federal, State, and local) conflicts and, if necessary, recommend an appropriate legislative resolution.

During the NSTAC XXVII cycle, the LRTF began to address 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. During the NSTAC XXVIII cycle, the LRTF completed its analysis and on April 8, 2005, the NSTAC sent a letter to President Bush recommending that:

- The Federal Government develop and adopt Web publishing and access guidelines incorporating provision that protect industry-sensitive critical infrastructure information provided to the Government;
- Federal departments and independent agencies be encouraged to adopt Web publishing and access guidelines; and
- The appropriate departments and agencies be directed to promulgate Web publishing and access guidelines for dealing with sensitive but unclassified critical infrastructure information.

During the NSTAC XXVIII Cycle, the LRTF initiated an examination of the NS/EP telecommunications implications of the implementation of the *Support Anti-terrorism by Fostering Effective Technologies Act*. In addition, the LRTF started an examination of the NS/EP implications of the *Defense Production Act* and the proposed amendments to the Act and Executive Order 12919, *National Defense Industrial Resources Preparedness.*

On an ongoing basis, the LRTF continues to track and monitor the legislative and regulatory activities that could impact NS/EP services, operations, and communications.

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

located within the DHS Information Analysis and Infrastructure Protection Directorate and serves as the clearinghouse and dispenser of CII. The PCII Program will be implemented in three phases. In phase three, the PCII PO will be able to disseminate CII to other Federal, State, and local Governments. However, each receiving entity must first obtain accreditation from the PCII PO and comply with PCII PO requirements and objectives.

Also, in an October 28, 2003, letter to the NSTAC, the Assistant to the President for Homeland Security wrote that the staff of the Executive Office of the President had been asked to convene a meeting with the other White House stakeholders to review the recommendations in the NSTAC's policy conflict letter and "analyze their impact to NS/EP communications."

Reports Issued

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

Legislative and Regulatory Task Force Membership

Chair
Ms. Louise Tucker, Telcordia Technologies

Vice Chair
Mr. Gerald Harvey, Lockheed Martin

AT&T Corporation
Mr. Harry Underhill

BellSouth Corporation
Mr. David Barron

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Lucent Bell Labs
Mr. Michael Garson

MCI Incorporated
Mr. Dennis Guard

Microsoft Corporation
Mr. William Guidera

Nortel
Mr. Raymond Strassburger

Northrop Grumman
Mr. Scott Freber

Qwest Communications
Mr. Jon Lofstedt

Rockwell Collins
Mr. Ken Kato

SBC Communications
Ms. Rosemary Leffler
Sprint Corporation
Mr. Michael Fingerhut

VeriSign, Inc.
Mr. Michael Aisenberg

Verizon Communications
Mr. James Bean

Other Legislative and Regulatory Task Force Industry Participants

AT&T Corporation
Ms. Elizabeth Gastor

BellSouth Corporation
Ms. Cristin Flynn Goodwin

BellSouth Corporation
Ms. Kelly Mauceri

BellSouth Corporation
Mr. Lloyd Nault

Cellular Telecommunications and Internet Association
Mr. Christopher Guttman-McCabe

George Washington University
Dr. Jack Oslund

Lockheed Martin
Ms. Elaine David

Lockheed Martin
Mr. Larry Duncan

Lucent Bell Labs
Mr. Karl Rauscher

Lucent Bell labs
Ms. Selma Munden

MCI Incorporated
Mr. Seth Maiman

Microsoft Corporation
Mr. Scott Forbes

Northrop Grumman
Mr. Larry Blair

Raytheon Company
Mr. Paul Harris

Raytheon Company
Mr. Frank Newell

Science Applications International Corporation
Mr. Henry Kluepfel

Sprint Corporation
Mr. Timothy Bowe

Verizon Communications
Mr. Drew Arena

Verizon Communications
Mr. Michael Hickey

Legislative and Regulatory Task Force Briefers

American Insurance Group
Mr. Ty Sagalow

Booz Allen Hamilton
Mr. Joseph Sifer

Booz Allen Hamilton
Mr. David Sulek

Booz Allen Hamilton
Mr. Winston Wiley

Department of Commerce
Mr. Richard Meyers

Department of Homeland Security
Ms. Wendy Howe

Federal Emergency Management Agency
Mr. Larry Hall

Federal Emergency Management Agency
Mr. Crane Miller

Network Security Information Exchange
Mr. Fred Herr

Telcordia Technologies
Mr. Robert Lesnewich

Legislative and Regulatory Task Force Government Participants

Department of Defense/
Defense Information Systems Agency
Ms. Hillary Morgan

Department of Energy
Mr. John Greenhill

Department of Homeland Security/
Office of the General Counsel
Mr. David Delaney

Department of Homeland Security/
Office of the General Counsel
Mr. Eric Werner

Federal Communications Commission
Mr. Gregory Cooke

Office of Management and Budget
Ms. Kimberly Johnson

Previously Addressed Issues

Previously Addressed Issues

Wireless Services (Including Priority Services)

Investigation Groups

Wireless/Low-Bit-Rate Digital Services Task Force (W/LBRDSTF)

Wireless Services Task Force (WSTF)

Legislative and Regulatory Task Force (LRTF)

Wireless Task Force (WTF)

Periods of Activity

W/LBRDSTF: March 1991—October 1991

WSTF: December 1991—September 1995

LRTF: February 2001—Present

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 Service (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.

Wireless Security

Investigation Group

Wireless Task Force (WTF)

Period of Activity

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. Thus 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.

Physical Security of the Telecommunications Network

Investigation Groups

Industry Executive Subcommittee (IES)
Plans Working Group (PWG)

Vulnerabilities Task Force (VTF)

Periods of Activity

PWG: December 1990—September 1991

VTF: May 2002—February 2003

Issue Background

On December 13, 1990, at NSTAC XII, an NSTAC member questioned the physical security of the PSN, due to issues surfaced by a National Research Council report on the growing vulnerability of the PSN. As a result, the NSTAC tasked the IES to work with the OMNCS to address industry's growing concerns related to physical security of the telecommunications infrastructure. The IES subsequently established the PWG to further investigate the tasking.

In response, the PWG, in conjunction with the OMNCS Office of the Joint Secretariat, prepared a physical security study that examined current industry/Government activities, including results from a questionnaire given to the NCC industry representatives on physical security policy, operational procedures, and methods. The study also documented past NSTAC task force and OMNCS 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 NSTAC and OMNCS 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 PWG concluded that it needed no further NSTAC review at that time. The IES amended and approved the physical security study at the September 5, 1991, IES Meeting.

During the business and executive sessions of the NSTAC XXV Meeting, the NSTAC Principals 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 IES 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 critical sites and equipment are secured 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 issues regarding the security of products and services delivered to critical locations (i.e., chain of control). 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.

History of NSTAC Actions and Recommendations

At the October 3, 1991, NSTAC XIII Meeting, members approved the PWG report, concluding that the physical security issue required no further study at that time. Over a decade later, and in the wake of the attacks of September 11, 2001, the NSTAC Principals again discussed the value of physically protecting the telecommunications assets that comprise the network infrastructure. To mitigate risks associated with concentration of assets, the NSTAC recommended that the President direct the appropriate departments and agencies to fund and undertake the following:

- Work with risk assessment organizations and service providers, to conduct site by site mission critical risk analyses to identify vulnerabilities that could affect NS/EP communications and operations; and provide adequate funding and resources for departments and agencies to identify, mitigate, and remediate vulnerabilities that could affect individual critical mission functions;

- Establish a mechanism to coordinate infrastructure data requests from Federal, State, and local Governments to the information and communications sector;

- Work with industry to develop and implement a cross-functional threat warning system that both carriers and the Government could adopt as part of their internal threat warning and response procedures; and coordinate with industry to develop a process

for sanitizing threat information for distribution; and

- Adopt telecommunications services procurement security policy guidelines that provide incentives to companies that follow best practices established by the NRIC, high levels of security standards, and other recognized business contingency principles.

To mitigate risks associated with trusted access issues, the NSTAC recommended that the President direct the appropriate departments and agencies to:

- Coordinate with industry and State and local Governments to develop guidance for:
  - creating national standards and capabilities for national security background checks, screening, and National Crime Information Center reviews
  - identifying the criteria for inclusion in background checks
  - identifying who should be subject to background checks
- Lead the research and development and standards bodies efforts to make available a standard "tamper-proof," certificate-based picture identification technology to enable the positive identification of individuals at critical sites;
- Coordinate with industry to develop a national plan for controlling access at the perimeter of a disaster area, in coordination with State and local Governments. This plan should be incorporated in the Federal Response Plan; and
- Adopt telecommunications service procurement security policy guidelines that provide positive incentives to those companies that follow NRIC best practices for access control.

Actions Resulting from NSTAC Recommendations

Following the NSTAC XXVI Meeting held on April 30, 2003, the IES created the Trusted Access Task Force (TATF), as a follow-on to the work of the VTF, specifically its Trusted Access Report. The TATF was charged 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. (See the Trusted Access section in the Active Issues section of this NSTAC Issue Review.)

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.

Information Sharing/Critical Infrastructure Protection

Investigation Groups

Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF)

National Plan to Defend Critical Infrastructures Task Force (NPTF)

Periods of Activity

IS/CIPTF: September 1999—March 2002

NPTF: June 20, 2001—September 20, 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.

Last Mile Bandwidth Availability

Investigation Group

Last Mile Bandwidth Availability Task Force (LMBATF)

Period of Activity

LMBATF: January 18, 2001—March 6, 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.

Report Issued

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

Network Convergence

Investigation Groups

Information Technology Progress Impact Task Force (ITPITF)

Convergence Task Force (CTF)

Network Security Vulnerability Assessments Task Force (NS/VATF)

Periods of Activity

ITPITF: September 1999—June 2000

CTF: June 2000—June 2001

NS/VATF: June 2001—March 2002

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 NSTAC recognizes that industry and Government must strive to identify and remedy associated network vulnerabilities to ensure sustained critical communications capabilities of the 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 IES created the ITPITF to examine the potential implications of Internet Protocol (IP) network and public switched network (PSN) convergence on existing NS/EP services (e.g., GETS and 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 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.

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.

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 created the Next Generation Networks Task Force (NGNTF), to conduct an examination of NS/EP requirements and emerging threats on the NGN. (See the Next Generation Networks section in the Active Issues section of this *NSTAC Issue Review*.)

Reports Issued:

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.

Response to September 11, 2001, Terrorist Attacks

Investigation Group

September 11 "Lessons Learned" Ad Hoc Group

Period of Activity

October 15, 2001—December 3, 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.

Report Issued:

NSTAC Letter to the President,
December 17, 2001.

Information Assurance

Investigation Groups

Information Assurance Task Force (IATF)

Information Infrastructure Group (IIG)

Financial Services Task Force (FSTF)

Periods of Activity

IATF: May 15, 1995—April 22, 1997

IIG: April 22, 1997—September 23, 1999

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.

Legislation and Regulation 1994-1999

Investigation Groups

Funding and Regulatory Working Group (FRWG)

Legislative and Regulatory Group (LRG)

Periods of Activity

FRWG: December 1982—December 1994

LRG: December 1994—September 1999

Issue Background

At its inaugural meeting in December 1982, the NSTAC established the FRWG to examine funding alternatives and regulatory issues for candidate enhancements to NS/EP telecommunications. In 1984, the FRWG formed the Funding of NSTAC Initiatives Task Force to investigate approaches to NSTAC funding mechanisms. The FRWG reconvened in 1990 to review the NSTAC funding methodology. The FRWG remained active until 1994 addressing issues such as enhanced call completion, underground storage tanks, and telecommunications service priority carrier liability. The NSTAC IES later changed the name of the FRWG to the LRG per the December 1994 *Industry Executive Subcommittee Guidelines.* The LRG did not become active until January 1997 following the passage of the landmark Telecommunications Act of 1996. The IES reconstituted the LRG as the Legislative and Regulatory Working Group (LRWG) following the IES reorganization in September 1999. The IES established the LRWG as a permanent working group, which received taskings from the IES when task forces require clarification or analysis on legislative or regulatory matters affecting a specific issue.

As the first major overhaul of telecommunications policy since 1934, the *Telecommunications Act of 1996* (Telecom Act) redefined competition and regulation in virtually every sector of the communications industry. In response to passage of the Telecom Act and the evolving telecommunications environment, the IES charged the group to examine legislative, regulatory, and judicial actions that potentially impact NS/EP telecommunications.

In its charge to the LRG, the IES placed particular emphasis on monitoring implementation of the Telecom Act. In addressing this charge, the group 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.

The group found the Telecom Act did not alter carrier responsibilities for the provision of NS/EP services. However, the group determined that continued change in the regulatory and industry structure warranted increased educational outreach efforts for new entrants and existing carriers regarding their mandatory and voluntary obligations.

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, and presented those findings in

its December 1997 report to NSTAC XX. The LRG 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.

In response to this finding, the IES charged the LRG to examine options for enhancing communication on NS/EP matters among industry, the 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; and documented the intergovernmental relationships between the FCC, the National Communications System, and the Office of Science and Technology Policy regarding NS/EP responsibilities. Discussions with FCC officials prompted the LRG to work jointly with the Network Group's Widespread Outage Subgroup to develop procedural guidelines to help telecommunications carriers resolve issues with the FCC when critical emergency telecommunications services needed to be restored in a timely manner.

In July 1997, the 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 LRG 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 LRG assessed what actions it should take to ensure that industry and Government consider NS/EP requirements during the planning process. In its report to NSTAC XX, the group presented its findings and recommended that the IES continue to assess the development of the NRIC recommendations regarding National Services.

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 a paper to NSTAC XXI in September 1998 geared to facilitating public awareness of selected NS/EP-critical telecommunications functions and capabilities. The 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.

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 IES charged the LRG to review the PCCIP's recommendations for potential legislative and regulatory implications for NS/EP telecommunications. Addressing this charge, the LRG also conducted a preliminary analysis of PDD 63, *Critical Infrastructure Protection*, which built on the PCCIP's recommendations. The President issued PDD-63 on May 22, 1998, and outlined a national policy to eliminate vulnerabilities in the Nation's critical infrastructures. Given the LRG's findings, the IES decided to undertake a more detailed assessment of the planned implementation of PDD-63.

Following NSTAC XXI and in response to information sharing policy outlined in PDD-63, the IES tasked the LRG with identifying and assessing 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 IES in assessing critical information sharing issues, particularly those associated with the implementation of PDD-63. To better understand the information sharing environment and the entities involved in the process, the LRG developed a report illustrating the entities with whom telecommunications companies shared outage and intrusion information and reviewing potential legal barriers that could inhibit the information sharing process.

In addition to evaluating the landscape of outage and intrusion information sharing, the IES tasked the LRG to examine relevant Y2K issues, particularly the success of the *Year 2000 Readiness and Disclosure Act* (Y2K Act) in being a catalyst to information sharing within industry. 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 IES forwarded a summary of the LRG's findings in February 1999.

The IES also 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 CPAS, (now referred to as Wireless Priority Service).

The LRG learned that due to a number of factors, the NCS was addressing a new approach for providing wireless priority access based on channel reservation rather than the technology originally proposed for CPAS.

The LRG also 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.

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.

Industry/Government Information Sharing and Response

Investigation Groups

National Coordinating Center for Telecommunications (NCC) Vision Task Force

Operations Support Group (OSG)

Information Sharing/Critical Infrastructure Protection (IS/CIPTF) Task Force

Periods of Activity

NCC Vision Task Force:
October 15, 1996—April 22, 1997

OSG: April 22, 1997—September 23, 1999

IS/CIPTF: September 23, 1999—
May 16, 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 for Telecommunications Task Force (NCCTF) to examine the future mission and role of the NCC. Future editions of the NSTAC *Issue Review* will summarize the activities and deliberations of the NCCTF once the group completes its report with Presidential recommendations.

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.

Globalization

Investigation Groups

National Information Infrastructure (NII) Task Force

Operations Support Group (OSG)

Information Infrastructure Group (IIG)

Globalization Task Force (GTF)

Periods of Activity

NII: August 2, 1993—March 18, 1997

OSG: April 22, 1997—September 23, 1999

IIG: April 22, 1997—September 23, 1999

GTF: September 23, 1999—May 16, 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.

National Information Infrastructure

Investigation Group

National Information Infrastructure (NII) Task Force

Period of Activity

August 2, 1993—March 18, 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.

Common Channel Signaling

Investigation Groups

Common Channel Signaling (CCS) Task Force

NS/EP Panel

Periods of Activity

CCS Task Force: April 28, 1993—January 31, 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.

Report Issued

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

Obtaining Critical Telecommunications Facility Protection During a Civil Disturbance

Investigation Group

NS/EP Panel

Period of Activity

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.

Energy

Investigation Groups

Energy Task Force

NS/EP Panel

Periods of Activity

Energy Task Force: August 31, 1988—March 29, 1990

Energy Task Force: October 3, 1991—May 27, 1993

NS/EP Panel: March 8, 1994—October 5, 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 Groups

Industry Executive Subcommittee (IES) Funding and Regulatory Working Group (FRWG)

Enhanced Call Completion (ECC) Task Force

ECC Ad Hoc Group

Periods of Activity

IES FRWG (Assured access): June 7, 1990—September 1990

ECC Task Force: December 13, 1990—July 17, 1992

ECC Ad Hoc Group: July 17, 1992—August 2, 1993

IES FRWG (Regulatory aspect of call-by-call preferential treatment): July—December 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.

Underground Storage Tanks

Investigation Group

Industry Executive Subcommittee Funding and Regulatory Working Group (FRWG)

Period of Activity

April 12, 1990—March 1, 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.

Report Issued

Energy Task Force Final Report,
February 1990.

International National Security and Emergency Preparedness Telecommunications

Investigation Group

Ad Hoc Group of the Industry Executive Subcommittee (IES) Plans Working Group (PWG)

Period of Activity

July 25, 1990—March 1, 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.

Report Issued

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

Telecommunications Systems Survivability

Investigation Group

Telecommunications Systems Survivability (TSS) Task Force

Period of Activity

March 6, 1986—June 8, 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.

Telecommunications Service Priority

Investigation Group

Telecommunications Service Priority (TSP) Task Force

Period of Activity

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

Industry Executive Subcommittee (IES) Funding and Regulatory Working Group (FRWG)

Period of Activity

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.

Intelligent Networks

Investigation Group

Intelligent Networks (IN) Task Force

Period of Activity

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.

National Research Council Report

Investigation Group

National Research Council (NRC) Report Task Force

***Period of Activity*:**

August 18, 1989—March 29, 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.

Report Issued

NRC Report Task Force Final Report,
March 1990.

Commercial Satellite Survivability

Investigation Groups

Commercial Satellite Survivability (CSS) Task Force

Satellite Task Force (STF)

Periods of Activity

CSS: December 1982—April 1984
June 1988—March 1990

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.

Industry Information Security

Investigation Group

Industry Information Security (IIS) Task Force

Period of Activity

August 19, 1986—September 22, 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.

National Telecommunications Management Structure

Investigation Group

National Telecommunications Management Structure (NTMS) Task Force

Period of Activity

August 19, 1986—June 8, 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.

Report Issued

NTMS Implementation Concept (Final), November 1987.

Telecommunications Industry Mobilization

Investigation Group

Telecommunications Industry Mobilization (TIM) Task Force

Period of Activity
June 7, 1985—June 8, 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.

Commercial Network Survivability

Investigation Group

Commercial Network Survivability (CNS) Task Force

Period of Activity

February 29, 1984—October 9, 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.

Funding of NSTAC Initiatives

Investigation Group

Funding of NSTAC Initiatives (FNI) Task Force

Period of Activity

April 3, 1984—December 12, 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. The IES renamed the FRWG the Legislative and Regulatory Group in accordance with the December 1994 *IES Guidelines*.

Report Issued

NSTAC Funding Methodology, October 25, 1984.

Electromagnetic Pulse

Investigation Group

Electromagnetic Pulse (EMP) Task Force

***Period of Activity*:**

September 27, 1983—October 9, 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.

International Diplomatic Telecommunications

Investigation Group

International Diplomatic Telecommunications (IDT) Task Force

Period of Activity

September 27, 1983—December 12, 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.

Automated Information Processing

Investigation Group

Automated Information Processing (AIP) Task Force

Period of Activity

December 14, 1982—December 12, 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.

National Coordinating Mechanism

Investigating Group

National Coordinating Mechanism (NCM) Task Force

Period of Activity

December 14, 1982—November 15, 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. The status of the NCC is reported at each Industry Executive Subcommittee meeting. (See the Industry/ Government Coordination and Response section in this *NSTAC Issue Review* for a fuller discussion of more recent NCC actions.)

Reports Issued

NCM Task Force Report, May 16, 1983.

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

Research & Development

Investigation Groups

Network Security Task Force (NSTF)

Network Security Group (NSG)

Network Group (NG), Intrusion Detection Subgroup (IDSG)

Research and Development Exchange Task Force (RDXTF)

Research and Development Task Force (RDTF)

Period of Activity

NSTF: February 21, 1990—August 26, 1992

NSG: December 1994—April 1997

NG, IDS: April 22, 1997—
September 23, 1999

RDXTF: July 18, 2000—July 29, 2003

RDTF: July 29, 2003—Present

Issue Background

Periodically, the NSTAC conducts a Research and Development Exchange (RDX) Workshop. The broad purpose of the Workshop is to stimulate and facilitate a dialogue among industry, the Government, and academia on emerging security technology R&D activities that have the potential to affect the NS/EP posture of the Nation, whether positively or negatively. To ensure inclusion of all stakeholders in the R&D community, the NSTAC has traditionally invited 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 OSTP, Defense Advanced Research Projects Administration (DARPA), and the NIST. During 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, clear, realistic, and actionable recommendations for actions by key stakeholders and decision makers.

The roots of the RDX Workshop date back to 1990, when the growing number of hacker incidents led to the formation of the NSTAC's NSTF. The task force's purpose was to assess the threats to, and vulnerabilities of, the public switched telephone network; and 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 the Government already had R&D efforts under way in all of those areas.

NSTAC R&D activities gained momentum in March 1996, when the NSTAC's IES determined that it would again be useful to address network security R&D issues and

charged the NSG with facilitating a seminar for industry and Government participants to discuss network security R&D activities and issues. The purpose of the seminar was threefold: (1) encourage a common understanding of network security problems affecting NS/EP telecommunications; (2) identify R&D activities in progress to address those problems; and (3) define additional network security R&D activities needed.

The NSG specified four areas of interest for further investigation—authentication, intrusion detection, integrity, and access control—and 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 R&D center. The NSTAC limited industry representation to NSTAC member companies.

In 1997, in response to a number of stimuli, including the recommendations from the 1996 RDX Workshop, the Network Group's (formerly the NSG) IDSG conducted a study of intrusion detection technology R&D and analyzed it in terms of meeting NS/EP requirements. The IDSG 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, the Government, and academia. The task force's recommendations reinforced previous NSTAC recommendations to examine the need for, and feasibility of, collaborative R&D approaches for security technology. Those recommendations 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 for training more information technology (IT) security professionals, creating large-scale testbeds to test security products and solutions, and promoting 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, as well as three recommendations for future NSTAC consideration, including the need to "conduct another R&D Exchange [Workshop] 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 NSTAC RDX Workshop also provided the model for all future workshops.

At the University of Tulsa in September 2000, participants at the NSTAC's fourth RDX Workshop examined issues of transparent security in a converged and distributed network environment and 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 next generation network. Findings and recommendations from the Workshop included the establishment of NSTAC task forces to address standards and best practices for network security.

The NSTAC's fifth RDX Workshop—held in March 2003 at the Georgia Technology 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 event examined trustworthiness from four different perspectives: cyber and software security, physical security, integration issues, and human factors. From this event, the NSTAC 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. The task force formulated recommendations for a joint industry, Government, and academia large-scale pilot testbed that could advance the current state of NS/EP integration activities.

The NSTAC's sixth and most recent workshop was held in Monterey, California in October 2004. Please see the Research and Development section in the Active Issues section of this NSTAC *Issue Review*.

History of NSTAC Actions and Recommendations

Following the 2003 RDX Workshop in Atlanta, Georgia, the NSTAC 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. In addition, the RDTF provided its *NS/EP Definition Discussion Paper* to the Executive Office of the President to utilize in ongoing discussions on NS/EP communications.

Reports/Proceedings 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.

Financial Services

Investigation Group

Financial Services Task Force (FSTF)

Period of Activity

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 is expected to be completed by the end of 2005.

Report Issued

Financial Services Task Force Report, April 2004.

Network Security

Investigation Groups

Internet Security/Architecture Task Force (ISATF)

Operations, Administration, Maintenance, and Provisioning (OAM&P) Standard Working Group

Periods of Activity

ISATF: April 2002—April 2003

OAM&P Working Group: February 2003—August 2003

Issue Background

During the NSTAC XXVI cycle (March 2002–April 2003), the IES created the Internet Security/Architecture Task Force (ISATF) to study such issues as identifying pervasive software/protocols and defining the "edge" elements 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. This initial list of security requirements was developed as a consensus document and submitted as a contribution to the ATIS Committee T1–Telecommunications, Working Group T1M1.5 Operations, Administration, Maintenance, and Provisioning (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

Following the NSTAC XXV Meeting on March 13, 2002, the IES turned to 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 IES created the ISATF to provide 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 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 alerting and warning systems to continue 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. Thirdly, the task force emphasized that significant barriers to information sharing exist, such as the 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, a streamlined method for disseminating expeditiously corrected information to the telecommunications and Internet service provider (ISP) communities is not utilized.

The ISATF 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 to coordinate with industry, a process for warnings, 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 (NAP), backbone, and ISP communities;

- Fund efforts related to identifying and mitigating vulnerabilities in the most critical protocols or software relied upon within key sectors of the Nation's infrastructure; and

- Promote and support legislation to address FOIA, antitrust, and liability concerns regarding information shared by industry for the purposes of CIP.

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

During the NSTAC XXV Meeting, concern was also expressed 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 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 be placed 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.

The ISTAF recommended to the President that:

- The Government should continue its work to identify the critical NS/EP 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 up-to-date; 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 implementations are inconsistent across the various telecommunications equipment and software providers. In addition, service providers are specifying similar but different 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 are introduced; and threats in the public network now 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 (i.e., 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. Separate and apart from the T1.276-2003 requirements, the current standard assumes that effective hardware and software controls provided by the operating system (OS) protect the data and resources being managed.
In addition, the OAM&P Standard Working Group recommended to the President that:

- The 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 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

DHS created the Information Analysis and Infrastructure Protection Directorate to identify and assess intelligence information concerning threats to the United States, issue warnings, and take preventative and protective action against those threats. The watch center capabilities of several Federal Government agencies were also consolidated within DHS.

The Homeland Security Act of 2002 included a provision (section 214) 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, GSA recently 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

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.

NSTAC Implementing and Governing Documentation

Executive Order 12382
President's National Security Telecommunications Advisory Committee

Source:

The provisions of Executive Order 12382 of Sept. 13, 1982, appear at 47 FR 40531, 3 CFR, 1982 Comp., p. 208, unless otherwise noted.

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.

Sec. 2

Functions.

(a) The Committee shall provide to the President, among other things, information and advice from the perspective of the telecommunications industry with respect to the implementation of Presidential Directive 53 (PD/NCS-53), National Security Telecommunications Policy.

(b) The Committee shall provide information and advice to the President 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 PD/NCS-53, National Security Telecommunications Policy.

(e) The Committee shall periodically report on matters in this Section to the President and to the Secretary of Defense in his capacity as Executive Agent for the National Communications System.

Sec. 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 Defense.

Sec. 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 Defense, 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.

Ronald Reagan
The White House,
September 13, 1982.

[Filed with the Office of the Federal Register, 4:39 p.m., September 13, 1982.]

Charter of the President's National Security Telecommunications Advisory Committee

I. Official Designation. Under Executive Order 12382, dated September 13, 1982, and Executive Order 13225, dated September 30, 2001, 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. I).

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 *mutatis mutandis* 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 which 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.

IV. Official to Whom the Committee Reports.

A. The Committee will report in writing to the President of the United States, through the Assistant to the President for National Security Affairs, and to the Secretary of Defense, in his capacity as Executive Agent for the National Communications System.

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 $2.4 million, including travel expenses, per diem, contractor support, and staff support.

C. The Secretary of Defense, in his 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 11.5 staff years, excluding contract support.

VI. Meetings and Termination.

A. The Committee will meet approximately every 9 months at
the call of the Chair. Subcommittees will meet as necessary for their assigned responsibilities.

B. Under Executive Order 13225, dated September 30, 2001, the Committee will terminate on September 30, 2003, 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. This charter will be considered approved as of this date; copies will be filed with the Administrator of General Services and the Library of Congress under the provisions of the Federal Advisory Committee Act as amended
(5 U.S.C., App. I).

National Security Telecommunications Advisory Committee Bylaws

Adopted: July 20, 1983
Amended: June 8, 1989
Amended: January 12, 1995
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 III, 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.

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 <u>if</u> 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.

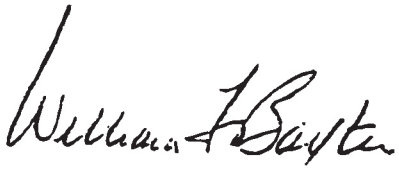
5. Information Sharing. Finally, the proposed NCM envisions that a limited amount of carrier information concerning available NS/EP resources will be provided to the NCC. It is also envisioned that a mechanism will be adopted by which individual carrier actions, such as the introduction of new services 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 (NSTAC) Membership (as of May 11, 2005)

Mr. F. Duane Ackerman, NSTAC Chair	Chairman and CEO BellSouth Corporation
Ms. Patricia F. Russo, NSTAC Vice Chair	Chairman and CEO Lucent Technologies
Mr. James F. Albaugh	President and CEO Integrated Defense Systems The Boeing Company
Mr. Lawrence T. Babbio, Jr.	Vice Chairman and President Verizon Communications
Mr. Gregory Brown	President and CEO Commercial, Government, and Industrial Solutions Sector Motorola, Inc.
Mr. Kenneth C. Dahlberg	President and CEO Science Applications International Corporation (SAIC)
Mr. Gary D. Forsee	Chairman and CEO, Sprint Corporation
Mr. William J. Hannigan	President, AT&T
Mr. Van B. Honeycutt	Chairman and CEO Computer Sciences Corporation (CSC)
Mr. Clayton M. Jones	Chairman, President and CEO Rockwell Collins, Inc.
Mr. Craig O. McCaw	Chairman, Teledesic Corporation
Mr. Craig J. Mundie	Senior Vice President and CTO Microsoft Corporation

Mr. Richard C. Notebaert	Chairman and CEO, Qwest Communications
Mr. Donald J. Obert	Group Executive, Network Computing Group Bank of America, Inc.
Mr. G. William Ruhl	CEO, D&E Telephone Company United States Telecom Association (USTA)
Dr. Hector de J. Ruiz	President and CEO Advanced Micro Devices, Inc. (AMD)
Mr. Stratton Sclavos	Chairman and CEO, VeriSign, Inc.
Mr. Stanley Sigman	President and CEO, Cingular Wireless Cellular Telecommunications & Internet Association (CTIA)
Ms. Susan Spradley	President, Wireline Networks Nortel
Mr. Randall L. Stephenson	Chief Operating Officer SBC
Mr. William H. Swanson	Chairman and CEO, Raytheon Company
Mr. Lawrence A. Weinbach	Chairman and CEO, Unisys Corporation
Mr. Joseph R. Wright	President and CEO PanAmSat Corporation
Position Vacant	Electronic Data Systems (EDS)
Position Vacant	Lockheed Martin Corporation
Position Vacant	MCI, Inc.
Position Vacant	Northrop Grumman Corporation

NSTAC XXVIII Executive Report to the President

Executive Report on the 28th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVIII) May 11, 2005

The President's National Security Telecommunications Advisory Committee (NSTAC) held its 28th meeting (NSTAC XXVIII) on May 11, 2005, at the United States (U.S.) Chamber of Commerce in Washington, DC. The meeting, which centered around the theme "Protecting the Nation's Telecommunications Infrastructure: Prevention, Response, and Restoration in a New Era" focused on issues surrounding national security and emergency preparedness (NS/EP) communications in this time of heightened security within industry and the Government, specifically, the Department of Homeland Security (DHS), the Department of Defense (DOD), the Federal Communications Commission (FCC), the Executive Office of the President (EOP), and the Congress. The NSTAC Principals met with Representative Christopher Cox (R-CA) during the Executive Breakfast; reviewed NSTAC activities over the past cycle and met with Mr. Robert Stephan, Assistant Secretary for Infrastructure Protection and Manager of the National Communications System (NCS), DHS, Chairman Kevin Martin, FCC, Lieutenant General Harry D. Raduege, Jr., Director of the Defense Information Systems Agency (DISA), DOD, and other senior Administration officials during the Business Session; met with Vice President Richard Cheney and other senior Administrative leaders; met with Secretary Michael Chertoff, DHS, during the Executive Luncheon; and engaged in discussion with Ms. Frances Fragos Townsend, Assistant to the President for Homeland Security and Counterterrorism, and Dr. John Marburger, Director of the Office of Science and Technology Policy (OSTP), and a number of senior Administration officials during the Executive Session. This Executive Report summarizes those presentations and deliberations. Also attached are the recommendations to the President from NSTAC XXVIII (Attachment 1) and an attendance list of NSTAC Principals (Attachment 2).

NSTAC XXVIII EXECUTIVE BREAKFAST

Call to Order/Opening Remarks.

Mr. F. Duane Ackerman, BellSouth and NSTAC Chair, called to order the 28th NSTAC Executive Breakfast on May 11, 2005, at 8:00 a.m. at the U.S. Chamber of Commerce in Washington, DC.

Mr. Ackerman introduced Representative Cox, the first Chairman of the House Committee on Homeland Security.

Representative Christopher Cox's Remarks.

Representative Cox noted that with the fall of Communism and the attacks of September 11, 2001, on the U.S., the Nation's security challenges differ

greatly from those posed during the Cold War era. He thanked the NSTAC Principals for the work they do to secure the telecommunications networks which includes not only physical protection of assets but also cyber defense.

Representative Cox observed that DHS' primary goal is to focus on prevention which will be considerably aided by the Nation's strong technological advantage in information and telecommunications technologies. He cautioned, however, that the U.S. must continue to outperform other countries in this area, as well as, non-state actors, who received a considerable number of tools and technologies with the dissolution of the Union of the Soviet Socialist Republics in 1991. He challenged industry to work with the Government to continue to leverage our considerable population numbers, technological advantage, and civic desire to live freely to counter terrorist attacks by building resiliency and redundancy into the basic architecture of the telecommunications network.

Representative Cox acknowledged that DHS faces considerable challenges in its efforts to continue to enhance homeland security technology and to make the Nation safer. However, he expressed confidence that these are challenges the Nation can meet and surpass.

Representative Cox announced that the House of Representatives has made significant advancements in its treatment of homeland security issues, consolidating jurisdiction for these issues within the House Committee on Homeland Security. He reported that Congress will also deliberate on two pieces of important legislation during the following week — DHS grant reform and the annual DHS authorization bill.

In response to a question from a Principal, on partisan treatment of homeland security issues by Congress, Representative Cox remarked that Congress is comprised of competing individuals who will naturally disagree about how issues should be handled; however, he acknowledged that all Congressman have a desire to ensure the protection of the Nation from terrorist attack which leads to less partisan politics than on other concerns facing the body.

A Principal inquired as to the integration challenges faced by DHS. Representative Cox responded that former Secretary of Homeland Security Thomas Ridge had the formidable task of integrating 22 Federal departments and agencies into one organization while simultaneously instituting mission change for many with strong legacy traditions. He noted that successful integration of the Department will include developing a common culture and suggested that standardizing the information technology across the Department will be a worthy first step.

In response to a question from a Principal on cybersecurity, Representative Cox stated that cyber issues should receive considerable emphasis in the work of DHS and noted that Congress is currently reviewing legislation that would elevate responsibility for cyber issues within DHS to the Assistant Secretary level.

Representative Cox responded to a question regarding oversight of the power grid by the House Committee on Homeland Security by noting that the Energy and Commerce

Committee had usual jurisdiction over matters concerning the power grid. The House Committee on Homeland Security only investigates power grid concerns when they involve intentional destruction. He also noted that the Homeland Security Advisory System will continue to exist but will be improved as necessary moving forward.

Closing Remarks/Adjournment.

Mr. Ackerman thanked the Principals and Representative Cox for their participation and adjourned the Executive Breakfast at 8:45 a.m.

NSTAC XXVIII BUSINESS SESSION

Call to Order/Opening Remarks.

Mr. Ackerman called to order the 28th NSTAC Business Session on May 11, 2005, at 9:00 a.m. at the U.S. Chamber of Commerce in Washington, DC. He welcomed members of the NSTAC and recognized the senior Government officials participating in the Business Session:

- Lieutenant General Raduege;
- Chairman Martin;
- Mr. Stephan;
- Ms. Kimberly Johnson, Office of Management and Budget;
- Mr. Mark LeBlanc, OSTP;
- Ms. Cheryl Peace, Homeland Security Council (HSC);
- Colonel Gregory Rattray, National Security Council (NSC);
- Mr. Michael Gallagher, National Telecommunications and Information Administration;
- Mr. Alfonso Martinez-Fonts, DHS; and
- Mr. Andrew Purdy, DHS.

Mr. Ackerman encouraged the NSTAC Principals to think through the "how's" and the "why's" as they approach a multitude of issues associated with emerging technologies and threats, focusing on outcomes and not process. Mr. Ackerman stressed the urgency and importance of the work of the NSTAC and reminded the Principals that national security and economic security are directly related. He also highlighted the importance of continuing to build the partnership between industry and Government. Ms. Patricia Russo, Lucent Technologies and NSTAC Vice Chair, echoed Mr. Ackerman's opening remarks and highlighted Secretary Chertoff's and Representative Cox's remarks from the Reception and the Executive Breakfast, respectively, on the importance of the NSTAC in the homeland security environment and the value of the partnership between industry and Government.

Opening Remarks: Mr. Robert Stephan.

Mr. Ackerman introduced Mr. Stephan, who thanked the NSTAC Principals for the opportunity to address them and for their dedication to NS/EP matters. Mr. Stephan praised both the NCS and the NSTAC for their invaluable work throughout the Cold War, and more recently in the war on terrorism. Mr. Stephan thanked the NSTAC for its input to the new National Incident Management System (NIMS) and the National Response Plan (NRP). He explained that these two documents provide the Nation with its first all-hazards incident management approach spanning prevention, protection, response, and recovery. Without the NSTAC's input regarding the telecommunications and coordination aspects of the NIMS and the NRP, Mr. Stephan noted that they would not be the comprehensive documents that they are today.

Mr. Stephan informed the Principals that during his first two and a-half weeks as the Assistant Secretary for Infrastructure Protection, he focused his efforts on assessing the current state of the Nation's critical infrastructure protection (CIP) efforts. He explained that during its first two years of existence, DHS focused primarily

on the internal matters of establishing a new department. Unlike the DOD's Northern Command (NORTHCOM), which was established in autumn 2002 and given a full year to become operational, DHS, and the Information Analysis and Infrastructure Protection Directorate in particular, were not given adequate time to establish operations and were held accountable by the American public immediately. During these initial years, tactical and operational decisions had to be made without proper grounding in policy and strategy. According to the Assistant Secretary, now that most of the internal functions are operational, the Office of Infrastructure Protection can begin to focus its attention on its true mission of reducing the vulnerabilities of the Nation's critical infrastructure. Mr. Stephan noted that immediate work must occur within the Office of Infrastructure Protection to reduce the vulnerabilities of the Nation's interconnected and interdependent infrastructures and key assets, and to perfect timely and efficient incident response mechanisms. Mr. Stephan informed the Principals that to achieve these goals, there are three challenges to be considered: (1) the nature of the enemy which is unlike any enemy our Nation has faced before; (2) the risk posed by vulnerabilities in our infrastructures that can effectively be used against our Nation if defensive mechanisms are not in place; and (3) the need for effective command and control mechanisms to protect our infrastructures. Given the fact that 85 percent of the Nation's critical infrastructure is privately owned and operated, he acknowledged that the methods of protecting critical assets are not uniform and require a great deal of work moving forward. He noted that the public-private partnership is key to the success of the Nation's infrastructure protection efforts.

Mr. Stephan emphasized that the key focus of CIP efforts moving forward will center on strategic planning. To achieve this strategic focus, Mr. Stephan noted that the National Infrastructure Protection Plan (NIPP) will be used as the strategic backbone of the work of the Office of Infrastructure Protection. However, the document, currently in the interim stage, and the processes it details will require a great deal of revision, specifically additional input from industry, before it can become the focal point of infrastructure protection efforts. Mr. Stephan highlighted the need for the future revised plan to embrace a risk-management based approach and to also include the following: (1) clearly defined roles and responsibilities for the private sector and Federal, State, local and tribal Governments; (2) protective standards and guidelines for each infrastructure sector; and (3) a review of resource requirements that would be updated annually.

Mr. Stephan noted the important role of industry in revising the NIPP. He emphasized that because threats are continually evolving, industry and the Government must work together to develop processes that can adapt to emerging threats. Mr. Stephan specifically asked for industry and the NSTAC's help to accomplish the following: (1) refine the NIPP so it may be used as the strategic backbone for the public-private partnership; (2) provide business models for strategic planning to accomplish a risk-management based approach; (3) identify the ways and means to enhance the strategic partnership between industry and Government; (4) determine the end state for CIP to best utilize public and private financial resources; (5) develop performance metrics for measuring CIP progress; and (6) consider the future interplay of the National

Infrastructure Coordinating Center (NICC) with the National Coordinating Center for Telecommunications (NCC), including the possibility for "one-stop-shopping" for critical infrastructure protection.

In closing, Mr. Stephan said the Nation cannot declare victory in the war on terror until all terrorist organizations throughout the world are eliminated. Until then, the Nation must remain vigilant and anticipate a constantly changing threat environment. Mr. Ackerman thanked Mr. Stephan and presented him with a commemorative coin as a token of the NSTAC's appreciation for his continued support.

STAKEHOLDER INPUT FOR NSTAC.

Chairman Kevin Martin.

Mr. Ackerman introduced FCC Chairman Kevin Martin and thanked him for speaking before the NSTAC. Mr. Ackerman remarked that Chairman Martin is not only the Chairman of the FCC, but also Defense Commissioner, responsible for NS/EP, defense, and homeland security functions. He also oversees the Network Reliability and Interoperability Council, an organization crucial to helping protect the Nation's critical infrastructures. Mr. Ackerman noted that Chairman Martin previously worked at the White House as Special Assistant to the President for Economic Policy and assumed his current position on March 18, 2005.

Chairman Martin thanked the NSTAC for its efforts to protect the country's critical infrastructures and acknowledged that the FCC is looking forward to continuing to work with the NSTAC to protect NS/EP communications. He recognized that new technology is emerging, creating new infrastructures, and altering the economic landscape of the country. As the economic environment changes, the FCC wants to ensure that a competitive market continues to protect NS/EP communications amid the development of new technology. Chairman Martin encouraged the NSTAC to be forward-thinking in its work and consider the challenges posed by convergence and the next generation networks (NGN). He noted that the FCC also has a role in shaping NS/EP communications and public safety, while also encouraging new services, without imposing heavy regulation. The public and private sectors must cooperate with each other and use creativity in moving forward to ensure NS/EP communications. For example, priority services capabilities are increasing due to the creativity and cooperation of the public and private sectors.

Chairman Martin cited efforts on which the FCC is focusing to improve public safety and NS/EP communications. The Commission is working to transfer spectrum to State and local Governments, and to date, 170 licenses have been granted. In addition to the transfer of spectrum, the FCC is committed to eliminating interference in the 800 megahertz band to guarantee that public safety officials can communicate effectively. He complimented the NCC's efforts and acknowledged that the NCC provides a unique forum and plays a critical role in restoring the telecommunications infrastructure in times of national emergency. Chairman Martin noted that the challenge in moving forward is fostering creative solutions to complex challenges. He further noted that the public and private sectors employed a creative approach in an unexpected situation to ensure communications on September 11, 2001, as restoration began immediately through the activation of switches in surrounding areas.

In moving forward, Chairman Martin cited areas where he believes the NSTAC and the FCC should focus. Specifically, he suggested that the NSTAC focus on: (1) improving priority communications programs; (2) exploring ways to improve diversity and redundancy; and (3) reviewing current FCC rules to help the Commission identify how to improve and extend existing homeland security initiatives. He reiterated the importance of the ability to communicate during crises and the ability to ensure that the telecommunications infrastructure can withstand any future emergency situation.

Mr. Ackerman thanked Chairman Martin for his remarks and inquired about the Commission's efforts to ensure that the FCC's reporting requirements do not compromise national security. Chairman Martin recognized the companies' concern and acknowledged that the FCC is doing its best to ensure that information collected is handled with the greatest sensitivity.

Lieutenant General Harry Raduege, Jr.

Mr. Ackerman introduced Lieutenant General Raduege, who highlighted NS/EP communications challenges and lessons learned from his unique perspective as the former Manager of the NCS and the current Director of DISA. Specifically, he noted that many national emergencies have reinforced that communications is the first priority, before even food and water, in emergency response situations. For this reason, it is essential that communications systems remain operational in a disaster situation and cannot be easily disabled. Lieutenant General Raduege commended the NSTAC for its past recommendations that resulted in many of the current communications priority services programs. Specifically, he highlighted the importance of assured communications and praised the effectiveness of the Government Emergency Telecommunications Service, the Telecommunications Service Priority program, and the Wireless Priority Service program.

Lieutenant General Raduege reminded the Principals that information sharing and public-private collaboration continue to be a priority at DOD, and emphasized the need to leverage information sharing activities to transition from reactive to proactive approaches to infrastructure protection. In addition, he highlighted DOD's need for assured connectivity in even the most remote locations to support operations in places such as Afghanistan. In particular, he emphasized that the demand for assured bandwidth capabilities for command and control operations are increasing.

Lieutenant General Raduege informed the Principals that several communications challenges will need to be addressed through technological advancement, human networking, and cultural adjustment. Specifically, as DOD moves to a system of net-centric operations, new methods for disseminating information will emerge and new security issues, such as the need for trusted software, will arise. As an initial step, DOD has adopted a new information sharing philosophy of "need to share" to replace the old "need to know" philosophy. In addition, preparation for the transition from Internet Protocol Version 4 to Version 6, including carefully orchestrating requirements, will be essential. During this transition, networks must be controlled and managed as effectively as weapons systems; and network management and information assurance tools must be utilized to protect the networks against cyber

hacking. He noted that cyber terrorism is effectively an "information network dirty bomb" that could dramatically compromise economic security and the American way of life. Lieutenant General Raduege highlighted the importance of human networking within the communications and homeland security community and commended the members of the NSTAC for their assistance on September 11, 2001, noting that the relationships fostered by the NSTAC membership proved to be of utmost importance at that time. In addition, he noted that the NCC and the various Information Sharing and Analysis Centers (ISACs) play a critical role in human networking and information sharing. He noted that DOD is seeking measures to improve its relationship with the ISACs.

Finally, he emphasized the importance of developing a culture of collaboration and information sharing. Teamwork must permeate organizations in both the public and private sectors, and walls must be broken down in favor of information sharing to improve the Nation's NS/EP posture.

Lieutenant General Raduege continued by describing four components essential to meeting the desired communications "end-state," which requires focused attention and collaboration among industry, DOD, and NCS: net-centric operations, nontraditional services, information sharing and collaboration, and improved NS/EP capabilities. He noted that providing net-centric operational capabilities for war fighting, business, and intelligence is a critical area of concern for DOD. DOD is working to build communities of interest that coalesce around these particular areas to ensure that the transition is effective.

He again raised the challenge of ensuring that both wireline and wireless communications services are available to users in remote areas. The technological revolution has placed a premium on connectivity, and users traveling between major population centers expect to have wireless service, despite limited infrastructure. He also emphasized the need for recognizing operational realities and promoting information sharing and collaboration between responsible users with appropriate security credentials. Improving NS/EP communications capabilities is a quest shared by DOD, NCS, and the NSTAC.

A Principal inquired regarding the progress of the Global Information Grid Bandwidth Expansion (GIG-BE) project since its deployment. Lieutenant General Raduege informed the Principals that the program is designed to purchase and deploy bandwidth to 90 worldwide locations to improve national security intelligence, surveillance and reconnaissance, command and control, and information sharing. He reported that bandwidth with a 10 gigabyte capacity has been deployed to the first 10 military sites through diverse paths with two points of presence. He expects all 90 locations to be functional by the end of September 2005. He thanked those companies that participated for their critical support to the GIG-BE program. He noted, however, that providing the transport for communications capabilities is merely the first step in the process. Achieving the capability to provide the most remote tactical user with access to shared databases over a web-based net-centric environment will continue to demand focused attention and a collection of public and private sector resources. Specifically, the goal of a net-centric

environment cannot be achieved until all the necessary bandwidth is installed, including bandwidth in remote locations.

A Principal asked Lieutenant General Raduege to consider how the NCC should reorganize in response to the 21st century environment and how the NCC should interface with DOD. Lieutenant General Raduege stated that the Joint Task Force Global Network Operations (JTF GNO) Command Center, DISA, and the NCC must maintain and improve connectivity. He noted that with the opening of the new JTF GNO Command Center, it will be important to look for new avenues for collaboration with the NCC. He acknowledged that while the physical presence of the NCC at DISA may no longer be possible, the ability to virtually communicate and seamlessly share information remains critical. He remarked that it is important for the NCC to adopt a posture of readiness, rather than a reactionary posture, to manage emergency events. He also emphasized the importance of strengthening these vital partnerships in the future. In closing, Mr. Ackerman presented Lieutenant General Raduege with a plaque to recognize his years of dedicated service and support to the NSTAC.

Facilitated Discussion.

Mr. Ackerman called on the NSTAC task force champions to provide a review of the task force activities during the NSTAC XXVIII Cycle. Mr. Ackerman encouraged the Champions to offer their insight on the challenges and accomplishments of their respective task forces throughout the discussion.

Mr. Richard Notebaert, Qwest Communications and Trusted Access Task Force (TATF) Champion, stated that the TATF was established to address concerns regarding the need for background checks of individuals who work with the telecommunications infrastructure. The TATF was specifically tasked with considering background screening and credentialing processes for gaining physical access to critical telecommunications facilities. The task force concluded that no standard process exists for the private sector to ensure that personnel accessing critical telecommunications facilities do not pose a threat to NS/EP communications. To address the apparent need for a screening process, the TATF examined the Transportation Security Administration's (TSA) background check procedures and considered how the TSA process might be applied to the telecommunications sector. Mr. Notebaert reported that the task force completed the *Screening, Credentialing, and Perimeter Access Controls Report,* which provides the President with several recommendations on the implementation of standard background screening processes for industry to be coordinated in partnership with DHS and modeled after the TSA procedures. In addition, Mr. Notebaert commented that the TATF Report also included recommendations regarding access at the perimeter of National Special Security Events (NSSEs) and informed the Principals that the Government has been extremely receptive to these recommendations and has already implemented them during recent NSSEs.

Mr. Craig Mundie, Microsoft Corporation and Next Generation Networks Task Force (NGNTF) Champion, stated that the NGNTF was established as a result

of discussion during the NSTAC XXVII Meeting to address how the Government could ensure NS/EP telecommunications requirements continue to be managed on the NGN. To address these issues, the task force created six working groups: (1) Near Term Recommendations Working Group (NTRWG); (2) NGN Description Working Group (NDWG); (3) Scenarios and User Requirements Working Group (SURWG); (4) End-to-End Services Working Group (ESWG); (5) Vulnerabilities and Threat Modeling Working Group (VTMWG); and (6) Incident Management Working Group (IMWG). Mr. Mundie reported that the NGNTF recently completed the *Near Term Recommendations Report* which was approved by the Principals and forwarded to the White House. The activities of the NTRWG have been completed; the NDWG and the SURWG have developed a high-level description of the NGN and several user scenarios respectively; and the activities of the ESWG, VTMWG, and IMWG have been initiated and are expected to be completed in fall 2005. Mr. Mundie thanked the Principals for providing subject matter experts from their organizations to support the NGNTF and acknowledged the involvement of non-NSTAC member companies, noting that the input from this broader group greatly enriched the dialogue. Mr. Gregory Brown, Motorola, praised the NGNTF for its thoughtful and comprehensive work to date. He noted that the integration of public and private networks will be key to the future of the NGN, and encouraged the NGNTF to include the thousands of private networks in its study.

Mr. Lawrence Babbio, Verizon Communications and NCC Task Force (NCCTF) Champion, stated that the NCCTF was established following the October 21, 2004, NSTAC Principals' Conference Call to examine the direction and structure of the NCC and to explore how it should continue to partner with Government in consideration of the NCC's role as a part of DHS. The tasking originated from the need for the NCC to reexamine its structure, organization, and mission in the evolving homeland and national security environment. Some of the challenges the NCCTF hopes to address include facilitating more information sharing between the NCC and other organizations and expanding its membership and partnerships to ensure the key players within the telecommunications infrastructure are well represented. Mr. Stephan commented that DHS' Infrastructure Coordination Division has established the NICC and noted that the NCCTF should consider how the NCC and the NICC will interact in the future and how the NCC might leverage the expertise of the other sector groups represented in the NICC.

Ms. Russo reported that the Research and Development Task Force (RDTF) held its sixth very successful Research and Development Exchange (RDX) Workshop in Monterey, California, in October 2004, and is currently initiating planning for a seventh workshop in 2006. She noted that the 2004 Workshop gathered more than 100 of the Nation's most knowledgeable telecommunications experts from industry, Government, and academia to discuss the trustworthiness of the telecommunications network. The task force recently published its 2004 RDX Workshop Proceedings document, which outlines five major findings, including the need for interoperable identity management and authentication systems as well as the need to examine

the interdependencies between critical infrastructures, especially those between the telecommunications and electric power infrastructures. Ms. Russo informed the group that the interdependency issue has been assumed by the Telecommunications and Electric Power Interdependency Task Force (TEPITF) and that the issue of authentication and identity management will be discussed in greater detail during the NSTAC Executive Session. Ms. Russo also reported that the task force finalized its Testbed Paper, which was the result of discussions held at both the 2003 and 2004 Workshops regarding the need to develop a testbed for NS/EP communications purposes. The paper sites examples of existing working collaborative testbeds and recommends that a testbed workshop be convened and, based on the outcome of the workshop, a Government organization be provided the appropriate funding to assume the leadership of an NS/EP communications testbed. Ms. Russo stated that the paper was approved by the Industry Executive Subcommittee (IES) and now required Principal approval. The NSTAC members unanimously approved the Testbed Paper.

Ms. Susan Spradley, Nortel and TEPITF Champion, reported that the TEPITF was established on February 17, 2005, at the IES Working Session to investigate near-term and long-term NS/EP issues associated with the interdependency between the telecommunications and electric power sectors. Ms. Spradley noted that although the NSTAC examined issues related to the interdependency of the telecommunications and electric power sectors before the September 11, 2001, terrorist attacks, the previous examinations focused primarily on telecommunications and did not take a balanced approach to the issue. In addition, she noted that the technology environment has advanced since the previous NSTAC deliberations and emerging technologies are increasing the telecommunications sector's reliance on electric power. Moving forward, the task force plans to examine past NSTAC work regarding telecommunications and electric power interdependency and to consider the electric power requirements of the NGN. To date, the task force has held an initial meeting and established its overall focus. Ms. Spradley commented that the task force participants reflect a good cross representation of both the telecommunications and electric power industries.

Mr. Ackerman, Legislative and Regulatory Task Force (LRTF) Champion, reported that throughout the past cycle, the LRTF continued to analyze legislative and regulatory issues relevant to NS/EP telecommunications. Specifically, the LRTF developed a letter and detailed addendum to the President recommending that the Federal Government develop and adopt Web publishing and access guidelines, that Federal independent agencies be encouraged to adopt Web publishing and access guidelines, and that the appropriate departments and agencies be directed to promulgate Web publishing and access guidelines for handing sensitive but unclassified critical infrastructure information. In addition, Mr. Ackerman encouraged the Principals to take a proactive approach to reducing critical infrastructure information available on the Internet.

Closing Remarks/Adjournment.

Mr. Ackerman recognized the IES members for all of their efforts during the cycle, specifically naming Mr. David Barron, BellSouth and IES Working Session Chair, and Mr. Karl Rauscher, Lucent and IES

Working Session Vice Chair, as well as the task force chairs. He thanked the Principals and speakers for their participation in the morning's proceedings. Mr. Ackerman adjourned the NSTAC Business Session at 10:30 a.m.

NSTAC XXVIII EXECUTIVE LUNCHEON

Call to Order/Opening Remarks.

Mr. Ackerman called to order the 28th NSTAC Executive Luncheon on May 11, 2005, at 12:45 p.m. at the U.S. Chamber of Commerce in Washington, DC.

Mr. Ackerman introduced Secretary Chertoff, noting that he was sworn in as the head of the DHS on February 15, 2005.

Secretary Michael Chertoff's Remarks.

Secretary Chertoff thanked the NSTAC Principals for their vital, long-term effort to address CIP NS/EP telecommunications issues on behalf of the President of the U.S. He recognized the significant recommendations that the NSTAC sent to the President as part of its Cycle XXVIII activities and reported that the Department is already working with the EOP to consider how to implement them.

Secretary Chertoff observed that the Principals' evacuation from the White House complex while meeting with Vice President Cheney symbolizes the tension that exists across the Nation, but specifically in Washington DC, wherein Americans must undertake normal business processes while also remaining vigilant for abnormal behavior that could signal an imminent terrorist attack. He acknowledged that one of the Department's largest challenges lies in fostering prosperity and freedom while also achieving greater invulnerability. He also stated that he is acutely aware of the need to improve the two way information flow between industry and Government which requires a more collaborative strategy instead of the top down command and control model utilized in the past.

Secretary Chertoff reviewed the Department's overall strategy and philosophy for the "second stage review" currently underway by DHS leadership. He praised former Secretary Ridge's great strides in integrating 22 separate departments and agencies to form DHS in such a short period of time, noting that many within the Federal Government did not consider the DOD to be a success until the passage of the *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, 40 years after its establishment.

Secretary Chertoff acknowledged that DHS must continue to make internal structural adjustments as necessary to ensure that it achieves its mission as a whole. As a result, DHS leadership is currently performing a gap assessment to better understand the results the Department needs to achieve, to identify any shortfalls in current efforts to meet that mission, and to determine where realignments may be necessary. He remarked that this process will ultimately ensure that the Department has clearly identified accountability and responsibility in each of its components which will successfully lead it to its desired outcomes — prevention, protection, preparation, and response.

Secretary Chertoff emphasized that the Department will follow a risk management approach to CIP. He recognized that this approach does accept a certain amount of risk to the Nation and could be unpopular in smaller towns where significant Federal spending is unlikely to occur. He declared that the Federal Government cannot replace the private sector's responsibility to protect

its own assets and asked industry to continue to work with Government to share the responsibility.

Secretary Chertoff thanked the Principals for the important work the NSTAC conducted during its Cycle XXVIII activities. He specifically identified the work of the TATF as essential given the very public recent data incursions suffered by ChoicePoint and other businesses. In addition, he noted the value of the TEPITF and the NGNTF.

In response to a question from a Principal, Secretary Chertoff responded that DHS' responsibilities overlap both domestically and internationally with those of DOD and the two organizations work very closely through mechanisms such as NORTHCOM and the North American Aerospace Defense Command. He stated that the major challenge experienced between DHS and DOD is ensuring that the communications between the two departments is seamless and real-time.

Secretary Chertoff responded to a question on the impact of intelligence reform on DHS by noting that different groups within the Federal Government have different perspectives on how best to conduct information sharing related to intelligence activities. He noted that the key challenge exists around developing an information-sharing architecture that shares the broadest amount of data possible with those who need to know while limiting the depth of data mining allowed to protect privacy rights.

Seven Revolutions Briefing.

Mr. Jay Farrar and Mr. Sam Brannen, Center for Strategic and International Studies (CSIS), provided a briefing to the Principals on the seven key trends that CSIS estimates will impact the future and transform human interaction. The seven trends fall under the categories of population, resource management, technological innovation, technology, integration, conflict, and governance.

Closing Remarks/Adjournment.

Mr. Ackerman thanked the Principals and speakers for their participation and adjourned the Executive Luncheon at 1:45 p.m.

NSTAC XXVIII EXECUTIVE SESSION

Opening Remarks.

Mr. Ackerman called to order the 28th NSTAC Executive Session at the U.S. Chamber of Commerce in Washington, DC, on May 11, 2005, at 1:15 p.m.

Mr. Ackerman explained that the NSTAC Executive Session provides the NSTAC Principals, along with the senior Government officials in attendance, the opportunity to discuss the challenges before the NSTAC with the highest levels of industry and the Government. Before commencing the substance of the Executive Session, Mr. Ackerman introduced the Government stakeholders who joined the meeting for the Executive Session:

- Ms. Townsend;
- Dr. Marburger;
- Mr. Kenneth Rapuano, HSC;
- Dr. Linton Wells, Acting Assistant Secretary for National Information Infrastructure, DOD;
- Ambassador David Gross, U.S. Coordinator for International Communications and Information Policy in the Bureau of Economic and Business Affairs, Department of State (DOS); and
- Mr. Stephen Malphrus, Federal Reserve Board (FRB).

Certificate Presentation.

Mr. Ackerman introduced Ms. Townsend and noted that in addition to her role as Assistant to the President for Homeland Security and Counterterrorism, Ms. Townsend chairs the HSC.
Ms. Townsend thanked the Principals for their continued service to the President. She emphasized that the White House considers every threat very seriously and noted that in a time of crisis, the first concern at the White House is to establish and maintain communication with the President, the Vice President, and the Chief of Staff, and to establish situational awareness. The activity that the Principals witnessed earlier in the morning at the White House was a reminder that the Government considers every threat very seriously and that the threats continue to be real. For these reasons, the NSTAC's advice related to emergency preparedness and communications systems is very important.

Ms. Townsend then moved to the podium and presented certificates recognizing and honoring the participation of the new NSTAC Principals. Ms. Townsend called the following Principals forward to receive their certificates:

- Mr. Babbio;
- Mr. Brown;
- Mr. Kenneth Dahlberg, Science Applications International Corporation;
- Mr. William J. Hannigan, AT&T Corporation;
- Mr. Stanley Sigman, Cellular Telecommunications & Internet Association;
- Mr. Randall L. Stephenson, SBC Communications; and
- Mr. Joseph R. Wright, Jr., PanAmSat Holding Corporation.

The new Principals rose and accepted their certificates.

Homeland Security Council Remarks. Ms. Townsend highlighted the White House's current efforts to address continuity of communications and reaffirmed the importance of information sharing between industry and the Government. She noted that during a crisis, continuity of communications is critical. To address Federal continuity of communications needs, the White House requested that each Federal department and agency identify its national emergency essential functions. Specifically, the departments and agencies were asked to identify the functions of greatest importance in an emergency situation for continuity of communications. Each department and agency was asked to prioritize those functions and identify those they would need to best support the President. The information gathered from the various departments and agencies suggested that although different functions would be required in different emergency scenarios, communications is essential in every scenario.

In addition, Ms. Townsend stressed the importance of information sharing between industry and the Government to best prepare for threats before a crisis unfolds. She noted that the President has identified information sharing as a priority issue and indicated that industry and the Federal Government need to develop a better understanding of the information each requires from the other. Ms. Townsend emphasized that information sharing should encompass the entire scope of available and important data. She noted that DHS has been a leader in facilitating increased information sharing with State and local Governments; however, she acknowledged that more needs to be done in the area of information sharing with industry. A Principal suggested that due to technological advances, the traditional modes of information sharing are changing, and technology should be leveraged to help facilitate improved information sharing. Ms. Townsend remarked that the White House could benefit from industry input on the increased use of technology for information sharing purposes.

Office of Science and Technology Policy Remarks.

Mr. Ackerman introduced Dr. Marburger, noting that he is the Director of OSTP as well as the science advisor to the President. Dr. Marburger praised the NSTAC and its member companies for its many years of valuable insight, which he said is indispensable to the Administration's overall strategy for NS/EP telecommunications. He noted that OSTP provides science and technology support to the President and policy offices in the EOP as well as coordination among all Federal departments and agencies with science and technology missions. Consequently, OSTP also has significant responsibility for NS/EP related communications activities. Dr. Marburger echoed Ms. Townsend's earlier sentiments, stating that communications is a key component of national security, which the Government takes very seriously. Dr. Marburger affirmed the value of the NSTAC for its pointed telecommunications expertise, specifically related to the identification of vulnerabilities and opportunities to improve national security through enhanced communications services.

Dr. Marburger observed that the NSTAC's current examination of the future role of

the NCC and the impact of the transition to the NGN on NS/EP communications is of significant importance to OSTP. He remarked that since its creation in 1984, the NCC has remained a central component of the Government's effort to ensure communications services are assured in any type of crisis. Working collaboratively with Government, the NCC tracks network outages and degradation, quickly relays relevant information to the appropriate agencies, and conducts real-time assessments to provide complete situational awareness. Dr. Marburger commented that OSTP also greatly appreciates the NCC's participation in Government sponsored training exercises, such as TOPOFF, which is very important in helping the Government make decisions about necessary improvements to communications support to ensure the most reliable communications capabilities are available to the President and senior Government leadership, especially during national crises.

Dr. Marburger thanked the NSTAC on behalf of the White House for its forward thinking assessment of the possible effects of the emergence of the NGN on NS/EP telecommunications services. He observed that while technological advancements in communications have enabled ubiquitous interconnectivity, they have also generated an increasing number of vulnerabilities that the science and technology community does not yet fully understand. Dr. Marburger commended the Committee for its *Near Term Recommendations Report,* which provided the Government with a good foundation for beginning its efforts to address NGN transition issues, and mentioned that he looks forward to its future recommendations for improving security and trust in this new environment.

In closing his remarks, Dr. Marburger announced that he is establishing a new Task Force on Effective Warnings that he believes would be of interest to the NSTAC. He commented that as part of its daily responsibilities, OSTP heads an interagency coordination process under the aegis of the National Science and Technology Council (NSTC). In July 2003, the NSTC's Committee on the Environment and Natural Resources' Subcommittee on Disaster Reduction published a report entitled *Reducing Disaster Vulnerability Through Science and Technology.* The report identified possible warning mechanisms that could be leveraged to alert the public about oncoming natural disasters and recognized the value of specific technologies, including the National Oceanic and Atmospheric Association (NOAA) weather radio. Since September 11, 2001, however, Dr. Marburger noted that OSTP has defined the term "disaster" to include not just natural disasters but also deliberate actions undertaken by human beings to cause harm, and therefore, must investigate manmade actions more fully.

Consequently, DHS, NOAA, and the FCC as well as a number of other departments and agencies have agreed to coordinate their efforts with OSTP to improve public warning mechanisms for all disasters through NSTC's Task Force on Effective Warnings. He explained that the task force will not duplicate any ongoing DHS efforts in this area, but will seek instead to implement the recommendations from the Subcommittee on Disaster Reduction's report. The result will be the creation of a broad planning and implementation framework to integrate all warnings under a single set of systems and protocols that will ultimately provide a context for improving

and sustaining effective national warnings for natural and manmade disasters. The task force's efforts will include examining existing and planned warning systems, conducting outreach programs, and making final recommendations to ensure effective warnings. Dr. Marburger revealed that he has asked Brigadier General John J. Kelly, Jr., Deputy Under Secretary of Commerce for Oceans and Atmosphere, NOAA; and Mr. Stephan to co-chair the task force; and he specifically requested input from the NSTAC in the task force's future deliberations.

Dr. Marburger thanked Mr. Ackerman and the NSTAC Principals for their leadership on the NSTAC. A Principal asked Dr. Marburger to provide his perspective on how the U.S. is performing with respect to the global race for recognized leadership in the communications and information technology markets. Dr. Marburger responded that the quest for leadership in these two markets, which includes the need for significant investment in research and development (R&D), is a very serious issue due to the globalization of the economy and the businesses that compose that economy. He noted that despite visa restrictions, there is a tremendous flux of people, goods, and services across borders around the world, which is changing business models and quickening the pace at which the data the Nation uses to benchmark its progress against that of other nations becomes outdated and ineffective as a framework to interpret market trends. He acknowledged that the tools the Government uses to guide policy making in this arena are "blunt" in effecting change, but Dr. Marburger reassured the Principals that the Administration is committed to the notion that R&D is absolutely essential for both national and economic security and is not reluctant to allocate funding to maintain leadership in this area. Mr. Ackerman thanked Dr. Marburger for taking the time to meet with the Principals to share this insight.

Discussion of Future NSTAC Issues.

Mr. Ackerman facilitated the discussion of future NSTAC issues for consideration and invited the NSTAC Principal/Champion for each issue to lead the discussion.

Next Generation Networks.

Mr. Mundie led a discussion of potential issues that may warrant additional guidance or work from the NSTAC's NGNTF. Specifically, Mr. Mundie raised the following issues for consideration by the Principals: (1) provisioning of NS/EP communications during the transition period to the NGN; (2) vulnerabilities and issues of security and resiliency unique to the NGN; and (3) international incident management and policy coordination. Mr. Mundie noted that although the NSTAC's *Near Term Recommendations Report* provides early guidance, the report does not address the process by which the transition from the public switched telephone network (PSTN) to the NGN should be managed and suggested that additional work in this area be considered by the NGNTF. In addition, Mr. Mundie noted that the unique nature of the NGN raises concerns regarding different vulnerabilities and elements of security in an interconnected NGN environment. Specifically, he stated that in the NGN environment, challenges will exist regarding managing trusted access to the network and much of the success of NS/EP communications in the NGN era will depend on highly sophisticated and secure identity

management capabilities above and beyond what is required on the PSTN. Finally, Mr. Mundie remarked on the incident management and policy coordination concerns related to the international nature of the NGN and noted that with the transition, it will become increasingly important for world leaders to be able to communicate over the NGN.

A Principal provided additional comments on international issues associated with NS/EP communications over the NGN. The member informed the Principals that there is a significant threat to the Nation's cyber infrastructure from abroad. In a one month time period, approximately 400 billion network connections are made worldwide; and one–two percent of these connections are malicious. In addition the e-commerce industry is currently a $400 billion industry, and six percent of e-commerce business is fraudulent, with 50 percent of this fraudulent activity originating from outside the U.S. The Principal further noted that 60 percent of phishing sites are established outside of the U.S., and about 250 million security events occur on U.S. networks each day, of which 20 percent of these attacks originate outside the country. Specifically, the Principal suggested that recommendations be formed regarding both a multinational incident response to such security events and international technological cooperation. A member inquired regarding those countries with which the U.S. should cooperate. Although Ambassador Gross did not indicate specific countries with which the Nation should coordinate its efforts, he informed the Principals that DOS is taking a proactive and flexible approach with regard to the NGN and maintains that the U.S. needs to be the international leader in this area. However, to meet this goal, cooperation and input from industry are required to help the Government understand the projected network architecture. He further emphasized that since international standards bodies, which are primarily industry driven, will play a significant role in determining the network architecture, it is critical that industry communicate international standards development with Government. In addition, DOS is currently examining concerns related to the legal aspects of information exchange with other nations.

A Principal inquired regarding the preferred methods for industry to communicate essential network information with Ambassador Gross. Ambassador Gross noted that industry information could be shared with him through a variety of channels, including informal personal phone calls and the Advisory Committee on International Communications and Information Policy. He emphasized that industry should not wait for formal processes to communicate and encouraged the NSTAC members to pursue informal means of communication when appropriate.

Lieutenant General Raduege informed the Principals that DISA coordinates a number of special communications needs for DOS. Specifically, since 1963, DISA has worked to connect special data and voice networks with 111 nations. Although these networks originally just included traditional telephone lines, the demand for special bandwidth connections has increased.

On the basis of the discussions, Mr. Mundie suggested that the NGNTF scope the following issues: (1) provisioning of NS/ EP communications during the transition period to the NGN; (2) trusted access concerns unique to the NGN; and

(3) global integration of networks and international incident management and policy coordination.

Dr. Wells further informed the NSTAC members that DOD is reaching maturity on end-to-end systems engineering efforts on the GIG. He noted that he was recently in Norfolk, Virginia, at the U.S. Joint Forces Command (USJFCOM) and learned that the USJFCOM has rolled out Everything over Internet Protocol (EoIP). Dr. Wells mentioned that he has personally spoken with several of the NSTAC Principals about their companies' assistance to the USJFCOM EoIP efforts, and he has invited any other interested members who would like to provide assistance to contact him. In addition, he informed the group that OSTP recently released the Networks Information Technology R&D Annex to the President's budget, which provides a total of $2.16 billion government-wide for R&D initiatives. Only $300 million of this total is allocated for DOD Federal networks R&D. Dr. Wells suggested that these funding allocations indicate that opportunities exist to leverage R&D funding outside of DOD.

National Coordinating Center for Telecommunications.

Mr. Babbio, Champion of the NCCTF, reported that as work continues to investigate the future role of the NCC, the task force has become increasingly aware of the numerous Government and industry bodies the Center must interface with to accomplish its mission. He noted the likelihood that the missions of these various groups minimally overlap, and he suggested that the task force has the opportunity to develop an inventory of the groups and broadly investigate their planning and operational processes and cross functional data sharing activities to identify any interdependencies and redundancies. He commented that the task force will focus on this aspect of the NCC's future role over the next 6 months.

A Principal remarked that resolving any mission redundancies is critical in determining how the NCC should operate in the future, especially since the member companies must continually reassess where finite resources are spent. Lieutenant General Raduege praised the work of the NCC and the trust its member companies placed in the Government to maintain a database containing industry's proprietary network data. He observed that the Government's effort to respond to the attacks on September 11, 2001, was made easier due to the fact that it had access to information outlining New York City's telecommunications network connectivity and choke points.

Telecommunications and Electric Power Interdependency.

Ms. Spradley reported that the task force held its first meeting in late April 2005 with very good representation from both the telecommunications and electric power sectors. She remarked that the task force plans to divide its tasking between two timeframes—near-term and long-term concerns. In the near term, the group will reevaluate past NSTAC interdependency recommendations in light of the activities of September 11, 2001, and work with DHS to determine whether rejuvenation of the Telecommunications Electric Service Priority program would provide a solid first step in addressing the sectors' concerns. In the long term, the task force will examine

communications structures between the sectors at the local and regional levels to determine where telecommunications providers require additional power assistance, and where power companies require additional telecommunications services. Ms. Spradley commented that this investigation is very important given the expected increased power needs of the telecommunications industry due to the evolution of the NGN and wireless technologies. She noted that the task force will not just investigate recovery aspects but will also consider research into power saving options.

Mr. Ackerman thanked her for her work to date on the issues, stating that physical and financial security are directly dependent on the sectors' abilities to manage their interdependencies and to limit outages in service.

Authentication.

Ms. Russo informed the Principals that as a result of the discussion at the 2004 RDX Workshop, authentication emerged as a critical issue meriting further consideration by the NSTAC. The RDTF convened a panel discussion, with representatives from various sectors, to promote a clearer understanding of the current state of affairs and assess R&D implications. At this time, the RDTF is seeking the Principals' guidance regarding future NSTAC attention to the issue. Ms. Russo emphasized that in the context of the NGN, it is currently relatively easy to "spoof" an identity on the Internet and that, in fact, companies exist that provide identity spoofing services. She emphasized that there is a clear need for significant work with regard to authentication and identity management over the NGN.

Ms. Russo acknowledged that industry has already initiated a lot of work with regard to general identity management issues. However, work still needs to be done to distinguish and identify the unique NS/EP requirements of identity management. Although this issue relates to the work of the NGNTF, Ms. Russo suggested that the RDTF continue to examine NS/EP issues related to authentication and identity management over the NGN and report back to the Principals. The IES member leading the RDTF efforts informed the Principals that the members of the RDTF are aware of current industry efforts with regard to identity management. He emphasized that there is still a need to identify the special requirements for the NS/EP environment as the authentication scheme for a crisis situation may need to change, with little warning, at the time of a crisis to either provide more or less stringent access requirements. A Principal suggested that the RDTF also consider Federated approaches to authentication and identity management services.

General Discussion.

A Principal raised concerns regarding the effective use of satellite communications for continuity of operations planning. Although the Nation responded well to the September 11, 2001, terrorist attacks, the wireline networks in Manhattan were unavailable, and the wireless networks were heavily congested. To help ensure continuity of operations, he suggested that commercial satellites be considered as an important part of the Nation's response capabilities moving forward. He noted that commercial satellites stay in place for seven–ten days, cannot be easily attacked, and are currently only about

80 percent utilized. For these reasons, satellites could provide a good alternative form of communication during a crisis. He informed the Principals that he has prepared a white paper discussing this issue, which he will submit to the IES. He suggested that the IES form a scoping group to consider this paper and determine whether a task force should be formed to address increased utilization of the Nation's domestic satellite communications capabilities for continuity of operations purposes.

A Principal reminded the Principals of the ongoing work of the Alliance for Telecommunications Industry Solutions' (ATIS) National Diversity Assurance Initiative and turned to Mr. Francis Dramis, BellSouth Corporation, to provide the Principals with an update on the ATIS initiative. Mr. Dramis noted that the initiative, which is halfway to completion, is designed to develop an understanding of and definition of the capabilities of diversity assessment and assurance for the financial services sector; to develop an understanding of the framework and processes that would be required to develop a diversity assessment and assurance model across multiple service providers; and to identify and develop recommended requirements for providing diversity assessment and assurance. At the inception of the study, the FRB identified 11 circuits to be tested and inspected on a continuous basis with the intention that at the end of the year, a report on diversity assurance requirements would be developed based on the results of these tests and inspections. Mr. Dramis informed the Principals that the requirements are currently being determined for a system to track the results of the tests. As soon as the system is in place, the results will be shared with the NSTAC Principals. Mr. Malphrus thanked the NSTAC for its continuing support of the initiative.

Adjournment.

Mr. Ackerman reviewed the day's discussions. He reminded the Principals that many of the Government stakeholders emphasized that the threat to our Nation and our Nation's infrastructures is real and that both industry and Government share responsibility in preparing for and mitigating the threat. He further noted that there is significant interdependence between industry and Government and that the NSTAC must remain responsive to the Government's needs. Mr. Ackerman informed the Principals that the summary of the meeting discussions will be sent to the Principals, and he encouraged them to continue to provide input on the issues for consideration and the prioritization of these issues. Mr. Ackerman expressed his appreciation to the NSTAC Principals and the senior Government officials for their active participation in both the Business and Executive Sessions and noted that he looks forward to their continued participation on the next Principals' Conference Call. Mr. Ackerman adjourned the NSTAC XXVIII Executive Session at 3:15 p.m.

Attachment 1
Report Recommendations to the President from the 28th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVIII) May 11, 2005

The President's National Security Telecommunications Advisory Committee (NSTAC) Trusted Access Task Force (TATF) worked with Department of Homeland Security (DHS) representatives to coordinate with industry and State and local Governments to develop guidance for: (1) creating national standards and capabilities for national security background checks, screening, and National Crime Information Center reviews; (2) identifying the criteria for inclusion in background checks; and (3) identifying who should be subject to background checks. The task force was also tasked to analyze the data gathered during the aforementioned task and apply it to the concept of a national background check process. In addition, the TATF was tasked to address an industry response to better securing National Special Security Events.

Based on the TATF analysis, the NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* and other existing authority, 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 Transportation Security Administration (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 the Network Reliability and Interoperability Council 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 National Coordinating Center for Telecommunications (NCC) Information Sharing and Analysis Center (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 United States (U.S.) Secret Service.

- 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.

The NSTAC's Next Generation Networks Task Force (NGNTF) examined near term opportunities for using existing technology to improve security and availability of national security and emergency preparedness (NS/EP) communications on converging networks. Based on its examinations, the NGNTF of 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—

- Use existing and appropriate cross-government coordination mechanisms to track and coordinate cross-agency next generation networks (NGN) activities and investment;

- Explore the use of Government (civilian and Department of Defense) 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: (1) gateways; (2) control

systems; and (3) 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 Legislative and Regulatory Task Force (LRTF) of the NSTAC examined NS/EP issues associated with open source critical infrastructure information. The NSTAC member companies were encouraged to undertake their own reviews and to consider adopting Web publishing and access guidelines. Similarly, to raise the Government's awareness and to limit the public access to sensitive infrastructure information, the NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472*, Assignment of National Security and Emergency Preparedness Telecommunications Functions,* and other existing authority, that—

- The Federal Government develop and adopt Web publishing and access guidelines incorporating provisions that protect industry-sensitive critical infrastructure information provided to the Government.

- Federal departments and agencies be encouraged to adopt Web publishing and access guidelines.

- The appropriate departments and agencies be directed to promulgate Web publishing and access guidelines for dealing with sensitive but unclassified critical infrastructure information.

At its fifth Research and Development Exchange (RDX) Workshop in March 2003, the NSTAC realized the need for a large-scale testbed to be used as an environment in which to test NS/EP systems ("systems" herein meaning telecommunications, networking and related information technology systems) and critical infrastructure dependencies on such systems. In October 2004, the NSTAC held its sixth RDX Workshop in Monterey, California. Participants again emphasized the critical importance of supporting research and development (R&D) initiatives addressing emerging communications technologies through modeling, simulation, and testbeds.

To meet the needs of the NS/EP community, a joint, collaborative industry, Government, and academia pilot testbed could advance the current state of NS/EP integration activities. As the potential benefits of such a testbed touch so many departments and agencies, effective implementation will require oversight and direction from the Executive Office of the President. Accordingly, the task force recommends that the Government —

- Convene a Government sponsored NS/EP Testbed Workshop, hosted by an appropriate technical organization (e.g., National Institute of Standards and Technology), and attended by

appropriate, representative stakeholders from industry, Government, and academia to:

- Validate the need for and value of a national, joint, collaborative, large-scale, distributed testbed with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection and recovery dependencies;
- Develop a small set of alternative approaches for the envisioned testbed that consider organization, membership, and operation and management, including startup, growth and continuing operations and the respective roles of Government, academia and industry participants;
- Determine whether the envisioned testbed should ultimately transition entirely to the private sector and, if it should, recommend under what conditions that could occur; and
- Estimate startup and recurring costs for the envisioned testbed, including direct Government funding and indirect financial support (e.g., research grants).

- Dependent on affirmation and supporting recommendations from the NS/EP Testbed Workshop, task and fund an appropriate government organization with the mission to establish a national, joint, collaborative, large-scale, distributed testbed program with a primary focus on emerging technology impacts on priority NS/EP services and related critical infrastructure protection dependencies, including:
  - Identifying candidate member facilities, collaborating with participating members to develop methods to interconnect member facilities, generally administering test procedures, and monitoring the results;
  - Operating, to the extent feasible, on a fee-for-service and non-attribution basis, thereby encouragi ng participation by industry compo nents;
  - Prioritizing NS/EP and critical infrastructure use of the overall testbed facilities and allowing for secondary use for other collaborative testing purposes; and
  - Accounting for intellectual property rights and technology ownership.

Attachment 2
Attendance of Members at the 28th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVIII)
May 11, 2005

Mr. F. Duane Ackerman, Chair	BellSouth Corporation
Ms. Patricia F. Russo, Vice Chair	Lucent Technologies
Mr. James F. Albaugh	The Boeing Company
Mr. Lawrence T. Babbio, Jr.	Verizon Communications
Mr. Gregory Q. Brown	Motorola, Inc.
Mr. Kenneth Dahlberg	Science Applications International Corporation
Mr. Gary D. Forsee	Sprint Corporation
Mr. William J. Hannigan	AT&T Corporation
Mr. Clayton M. Jones	Rockwell Collins, Inc.
Mr. Craig O. McCaw	Teledesic Corporation
Mr. Craig T. Mundie	Microsoft Corporation
Mr. Richard C. Notebaert	Qwest Communications
Mr. Donald J. Obert	Bank of America, Inc.
Mr. G. William Ruhl	U.S. Telecom Association
Mr. Stratton Sclavos	VeriSign, Inc.
Mr. Stanley Sigman	Cellular Telecommunications & Internet Association
Ms. Susan Spradley	Nortel
Mr. Randall L. Stephenson	SBC Communications
Mr. William H. Swanson	Raytheon Company
Mr. Lawrence A. Weinbach	Unisys
Mr. Joseph R. Wright, Jr.	PanAmSat Holding Corporation

Acronyms

Acronyms

AIN ..... Advanced Intelligent Networks

AIP ..... Automated Information Processing

ATIS ..... Alliance for Telecommunications Industry Solutions

CCS ..... Common Channel Signaling

CIAO ..... Critical Infrastructure Assurance Office

CII Act ..... *Critical Infrastructure Information Act of 2002*

CIP ..... Critical Infrastructure Protection

CNS ..... Commercial Network Survivability

COP ..... Committee of Principals

COR ..... Council of Representatives

CPAS ..... Cellular Priority Access Service

CSI ..... Commercial SATCOM Interconnectivity

CSS ..... Commercial Satellite Survivability

CTF ..... Convergence Task Force

CWG ..... Convergence Working Group

CWIN ..... Cyber Warning Information Network

DARPA ..... Defense Advanced Research Projects Agency

DDoS ..... Distributed Denial of Service

DHS ..... Department of Homeland Security

DOD ..... Department of Defense

DOE ..... Department of Energy

DOJ ..... Department of Justice

DOS ..... Department of State

EC ..... Electronic Commerce

ECC ..... Enhanced Call Completion

EISISG ..... Embedded Interoperable Security Issue Scoping Group

ELS ..... Essential Line Service

EMP ..... Electromagnetic Pulse

E.O. ..... Executive Order

EPA ..... Environmental Protection Agency

ERPWG ..... Emergency Response Procedures Working Group

ESF ..... Emergency Support Function

ESP ..... National Electric Service Priority Program in Support of Telecommunications

ETSI ..... European Telecommunications Standards Institute

FCC ..... Federal Communications Commission

FNI ..... Funding of NSTAC Initiatives

FOIA ..... *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

GNSS ..... Government Network Security Subgroup

GSA..... General Services Administration

GTISC ..... Georgia Technology Information Security Center

GTF ..... Globalization Task Force

HPC..... High Probability of Call Completion

IA..... Information Assurance

IAIP..... Information Analysis and Infrastructure Protection

IATF ..... Information Assurance Task Force

IAW ..... Indicators, Assessment, and Warnings

I&C ..... Information and Communications

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

IP ..... Internet Protocol

ISAC ..... Information Sharing and Analysis Center

ISATF ..... Internet Security Architecture Task Force

IS/CIP..... Information Sharing for Critical Infrastructure Protection

IS/CIPTF ..... Information Sharing Critical Infrastructure Protection 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

MTT ..... Mobile Transportable Telecommunications

NAP..... Network Access Provider

NCC ..... National Coordinating Center

NCM ..... National Coordinating Mechanism

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 NS/EP Telecommunications Program

NOAHG ..... NSTAC Outreach Ad Hoc Group

NOTF ..... NSTAC Outreach Task Force

NPTF..... National Plan to Defend Critical Infrastructures Task Force

NRC ..... National Research Council

NRIC..... Network Reliability and Interoperability Council

NSA..... National Security Agency

NSDD..... National Security Decision Directive

NS/EP..... National Security and Emergency Preparedness

NSG ..... Network Security Group

NSIE..... Network Security Information Exchange

NSSC ..... Network Security Steering Committee

NSSOG ..... Network Security Standards Oversight Group

NSTAC..... The President's National Security Telecommunications Advisory Committee

NSTF..... Network Security Task Force

NS/VATF..... Network Security/ Vulnerability Assessment Task Force

NTIA..... National Telecommunications and Information Administration

NTMS ..... National Telecommunications Management Structure

NWC ..... Naval War College

OAM&P ..... Operations, Administration, Maintenance, and Provisioning

OCS ..... Office of Cyberspace Security

OMNCS ..... Office of the Manager, National Communications System

OS ..... Operating System

OSG ..... Operations Support Group

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

PSTF ..... Protecting Systems Task Force

PWG ..... Plans Working Group

QoS ..... Quality of Service

R&D ..... Research and Development

RDTF ..... Research and Development Task Force

RDX ..... Research and Development Exchange

RDXTF ..... Research and Development Exchange Task Force

REWG ..... Resource Enhancements Working Group

R&O ..... Report and Order

RP ..... Restoration Priority

SATCOM ..... Satellite Communications

SCOE ..... Security Center of Excellence

SRWG ..... Security Requirements Working Group

SS7 ..... Signaling System 7

STF ..... Satellite Task Force

STU ..... Secure Telephone Unit

Telecom-ISAC .... Telecommunications Information Sharing and Analysis Center

TEPITF ..... Telecommunications and Electric Power Interdependency Task Force

TESP ..... Telecommunications Electric Service Priority

TIM ..... Telecommunications Industry Mobilization

TIPHON ..... Telecommunications and Internet Protocol Harmonization Over Networks

TSP ..... Telecommunications Service Priority

TSS	Telecommunications Systems Survivability
UST	Underground Storage Tank
USTA	United States Telecom Association
VTF	Vulnerabilities Task Force
W/LBRDSTF	Wireless/Low-Bit-Rate Digital Services Task Force
WOS	Widespread Outage Subgroup
WPS	Wireless Priority Service
WSPO	Wireless Services Program Office
WSTF	Wireless Services Task Force
WTF	Wireless Task Force
Y2K	Year 2000