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

Issue Review

A Review of NSTAC Issues Addressed Through NSTAC XXVII

August 2004

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 its 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. Enhancements in the form of operational programs and policy solutions benefit both industry and the Government as the security requirements for the communications infrastructure evolve.

During the past 22 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: it facilitates industry involvement with both the defense and civil agencies comprising the NCS; and it regularly sustains interaction between industry and the NCS member departments and agencies through the National Coordinating Center for Telecommunications (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 the NSTAC a key strategic resource for the President and his national security and homeland security teams in their efforts to protect our Nation's critical infrastructures in today's dynamic and evolving environment.

The NCS was officially transferred from the Department of Defense to the Department of Homeland Security (DHS) on March 1, 2003.

Executive Summary (continued)

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 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 XXVII cycle, from May 2003 to May 2004, the IES formed the following task forces and working groups:

- **The Financial Services Task Force** examined vulnerabilities related to the financial services sector's dependence on the telecommunications infrastructure, analyzed issues regarding network resiliency that could impact the financial services sector, and provided advice to the President on methods to help ensure resilient services.

- **The Satellite Task Force** examined the use of commercial satellites in NS/EP missions, vulnerabilities, and mitigation techniques. In addition, the group proposed recommendations to the President for enhancing the security of the commercial satellite infrastructure and the robustness of NS/EP communications.

- **The Legislative and Regulatory Task Force** examined national policies and regulatory issues that conflict with NS/EP missions. In addition, the group developed recommendations to the President on barriers to information sharing under the *Critical Infrastructure Information Act of 2002*.

- **The Research and Development (R&D) Task Force** developed a proceedings document following the NSTAC's fifth Research and Development Exchange (RDX) Workshop, held in March 2003, that identified major findings regarding the trustworthiness of NS/EP telecommunications and information systems.

Executive Summary (concluded)

The NSTAC's RDX Workshops stimulate and facilitate a dialogue among industry, the Government, and academia on emerging security technology R&D issues, and often result in programmatic enhancements to our Nation's NS/EP capabilities. In addition, the group produced papers on both an NS/EP definition and the possible development of a pilot testbed for NS/EP research and development purposes.

- **The Operations, Administration, Maintenance, and Provisioning (OAM&P) Working Group** examined the standard on OAM&P baseline security requirements for the management plane and provided recommendations to the President on the adoption and use of the OAM&P Telecommunications Standard by the Federal Government and other critical infrastructures.

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 XXVII Executive Report to the President, which includes summaries of the May 2004 NSTAC Business and Executive Sessions, as well as task force recommendations made to the President during the NSTAC XXVII Cycle (May 2003–May 2004).

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
P.O. Box 4502
Arlington, Virginia 22204-4502
(703) 607-6211
www.ncs.gov/nstac/nstac.html
nstac@ncs.gov

Introduction

Introduction

Purpose

This edition of the *NSTAC Issue Review* provides a comprehensive report of issues addressed by the President's National Security Telecommunications Advisory Committee (NSTAC) from its first meeting in December 1982 to its most recent meeting on May 19, 2004. 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 XXVII cycle from May 2003 to May 2004, NSTAC task forces addressed issues in the following areas:

- Financial Services
- Satellite Security
- Legislation and Regulation
- Research and Development
- Network Security

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 administration members 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

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 Industry Executive Subcommittee (IES) of the President's National Security Telecommunications Advisory Committee (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 Financial Services Task Force (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 national security and emergency preparedness (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' 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 sector-wide 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.
- 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.

Report Issued

- *Financial Services Task Force Report,* April 2004.

Financial Services Task Force Membership

Chair
Mr. William Sweeney,
Electronic Data Systems Corporation

Co-Vice Chair
Mr. Roger Callahan, Bank of America, Inc.

Co-Vice Chair
Ms. Cristin Flynn, BellSouth Corporation

AT&T
Mr. Harry Underhill

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

Lucent Technologies
Mr. Karl Rauscher

MCI, Inc.
Ms. Joan Grewe

Microsoft Corporation
Mr. Joel Greenberg

Nortel Networks Limited
Dr. Jack Edwards

Northrop Grumman Corporation
Mr. William Gravell

Qwest Communications
Mr. Thomas Snee

Raytheon Company
Ms. Heather Kowalski

Science Applications
International Corporation
Mr. Hank Kluepfel

SBC Communications, Inc.
Ms. Rosemary Leffler

Sprint Corporation
Mr. John Stogoski

United States Telecom Association
Mr. David Kanupke

VeriSign, Inc.
Mr. Michael Aisenberg

Verizon Communications
Ms. Ernie Gormsen

Other Financial Services Task Force Industry Participants

BellSouth Corporation
Mr. David Barron

BellSouth Corporation
Mr. Shawn Cochran

BellSouth Corporation
Mr. Doug Langley

BITS
Mr. John Carlson

BITS
Ms. Heather Wyson

Electronic Data Systems Corporation
Ms. Liesyl Franz

The George Mason University
Dr. Kevin McCrohan

The George Washington University
Dr. Jack Oslund

Qwest Communications
Mr. Jon Lofstedt

Raytheon Company
Mr. James Craft

SBC Communications, inc.
Ms. Suzy Henderson

Securities Industries
Automation Corporation
Mr. Andrew Bach

Sprint Corporation
Mr. Todd Colvin

Sprint Corporation
Ms. Laura Harper

Verizon Communications
Mr. Lowell Thomas

Financial Services Task Force Government Participants

U.S. Department of Homeland Security
Mr. Darrell Mak

U.S. General Services Administration
Mr. Tom Sellers

Federal Communications Commission
Mr. Ken Moran

Federal Reserve Board
Mr. Ken Buckley

Federal Reserve Board
Mr. Chuck Madine

Satellite Security

Investigation Group

Satellite Task Force (STF)

Period of Activity

September 2003–March 2004

Issue Background

The terrorist attacks on September 11, 2001, caused unprecedented disruption to communications and marked a dramatic surge in the use of national security and emergency preparedness (NS/EP) services. The attacks also raised security concerns about the protection of the Nation's vital telecommunications systems against threats. Currently, a Federal program does not exist to ensure NS/EP communications via commercial satellite systems and services. Previous security issues regarding NS/EP satellite programs focused on providing an alternative means of communications under nuclear attacks.

In January 2003, the Director, National Security Space Architect, requested that the President's National Security Telecommunications Advisory Committee (NSTAC) consider embarking on a study of infrastructure protection measures for commercial satellite communications (SATCOM) systems. In response, the NSTAC's Industry Executive Subcommittee (IES) formed the Satellite Task Force (STF) to analyze and assess commercial 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.

History of NSTAC Actions and Recommendations

The STF study complements past NSTAC work in the area of commercial satellite survivability (CSS), such as the studies the NSTAC conducted in the 1980s on satellite vulnerabilities. (See the Commercial Satellite Survivability section in the Previously Addressed Issues of this *NSTAC Issue Review.*) The NSTAC IES CSS Task Force assisted the National Communications System (NCS) by reviewing proposed objectives and implementation initiatives of the commercial SATCOM interconnectivity architecture. 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 National Communications System
- Draft a task force report with findings and Presidential recommendations.

The STF engaged broad and active participation from representatives of NSTAC member companies, non-NSTAC commercial satellite owners and operators, commercial satellite trade associations, Government agencies, and technical experts.

The task force examined all types of commercial SATCOM systems, which include fixed satellite service, broadcast satellite service, mobile satellite service, and satellite digital audio radio service. To understand the vulnerabilities of SATCOM systems, the STF compared the severity of potential threats against the degree of susceptibility of key elements in these services, including the radio frequency links, ground segment, cyber segment, and space segment.

The STF conducted two surveys to gain an understanding of how Federal agencies use commercial SATCOM systems and services for NS/EP, as well as to document vulnerabilities of infrastructure. The STF surveyed 14 Federal departments and agencies on their use of commercial satellites and services, backup communications plans, and anticipated communications requirements. The Satellite Industry Association surveyed its member satellite operators to provide voluntary self-assessments of the industry's vulnerabilities and mitigation techniques currently used.

The Government survey revealed that agencies do not fully optimize or protect the satellite infrastructure. Civil agencies have a shortage of in-house technical expertise that can integrate satellite communications into their network architectures, and agency procurement processes do not allow them to compete effectively for commercial SATCOM capacity. The industry survey revealed that the satellite industry has already taken steps to ensure that the security of the infrastructure adequately protects its commercial business interests.

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 and 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;
- 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.

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

Report Issued

Satellite Task Force Report, March 2004.

Satellite Task Force Membership

Co-Chair
Mr. Bob Britton,
Lockheed Martin Corporation

Co-Chair
Mr. William Reiner, The Boeing Company

Vice Chair
Mr. Peter Hadinger,
Northrop Grumman Corporation

BellSouth Corporation
Mr. Shawn Cochran

MCI, Inc.
Ms. Joan Grewe

Motorola, Inc.
Mr. Ben LaPointe

Qwest Communications
Mr. Jon Lofstedt

Raytheon Company
Mr. Alan Goldey

Rockwell Collins, Inc.
Mr. Ken Kato

Science Applications
International Corporation
Mr. Hank Kluepfel

SBC Communications, Inc.
Ms. Rosemary Leffler

Other Satellite Task Force Industry and Nongovernmental Participants

The Aerospace Corporation
Mr. Richard Buenneke

The Boeing Company
Mr. Robert Steele

The George Washington University
Dr. Jack Oslund

Hughes Network Systems, Inc.
Mr. Amir Dehdasty

Inmarsat Limited
Mr. Jack Deasy

Inmarsat Limited
Mr. Robert Demers

Intelsat
Mr. Joe Jankowski

Intelsat
Mr. Michael Kelley

Lockheed Martin Corporation
Mr. Steve Adelmann

Lockheed Martin Corporation
Dr. Al Dayton

Loral Space & Communications Ltd.
Mr. Bob Berry

Loral Space & Communications Ltd.
Mr. D. D'Ambrosio

Loral Space & Communications Ltd.
Mr. John Stern

The MITRE Corporation
Dr. Edward Jacques

Mobile Satellite Ventures
Mr. Carson Agnew

Mobile Satellite Ventures
Mr. Brian Deobald

PanAmSat G2 Satellite Solutions
Mr. Don Brown

Satellite Industry Association
Mr. David Cavossa

Satellite Industry Association
Mr. Richard Dalbello

SES Americom
Ms. Leslie Blaker

Spacenet Inc.
Mr. Pat Fagan

Verestar, Inc.
Ms. Kay Sears

Satellite Task Force Government Participants

Defense Information Systems Agency
Mr. Richard Bourdon

Defense Information Systems Agency
Ms. Hillary Morgan

U.S. Department of Transportation
Ms. Hollace Twining

Federal Communications Commission
Ms. Linda Haller*

U.S. General Services Administration
Ms. Sabrina Crane

U.S. General Services Administration
Mr. Thomas Sellers

National Communications System
Mr. Dale Barr

National Communications System
Mr. Tom Falvey

National Communications System
Mr. Gabriel Martinez

National Security Space Architect
Lieutenant Commander R. Bronson Armstrong

Office of Science and Technology Policy
Mr. Mark LeBlanc

U.S. Strategic Command
Major Robert Licciardi

U.S. Strategic Command
Mr. Steven Shirley

Satellite Task Force Briefers

The Aerospace Corporation
Mr. Michael Ware

The Electromagnetic Pulse Commission
Dr. Michael Frankel

U.S. General Services Administration
Mr. David Jarrell

Institute of Defense Analyses
Dr. Edward Conrad

National Intelligence Council
Mr. John Gass

National Security Agency
Mr. Ronald Kidwell

Office of the Undersecretary of the Air Force
Lieutenant Colonel Timothy Deaver

* Ms. Haller provided only technical expertise to the STF efforts.

Legislation and Regulation, 2000–2004

Investigation Groups

Legislative and Regulatory Working Group (LRWG)

Legislative and Regulatory Task Force (LRTF)

Period 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 national security and emergency preparedness (NS/EP) requirements. Therefore, the President's National Security Telecommunications Advisory Committee (NSTAC) monitors the regulatory environment and various legislative and regulatory activities that could impact NS/EP services, operations, and communications. For instance, barriers to information sharing among industry and the Government within the critical infrastructure protection (CIP) arena are of primary concern. Consequently, the NSTAC focused on analyzing Congressional activities aimed at removing information sharing barriers related to the *Freedom of Information Act* (FOIA).

Furthermore, advances in network technologies and the convergence of packet and circuit switched networks challenge industry and the Government to maintain a secure, reliable network infrastructure in support of NS/EP activities; and the NSTAC seeks to ensure the regulatory environment supports this objective. Also, in conjunction with the establishment of the Department of Homeland Security (DHS) and the passage of the *Critical Infrastructure Information Act of 2002* (CII Act), the NSTAC examined homeland security policies relating to the protection of critical physical and cyber infrastructures that support NS/EP communications.

History of NSTAC Actions and Recommendations

At NSTAC XXII, the Industry Executive Subcommittee (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
- 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 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 Information Sharing/Critical Infrastructure Protection Task Force, 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 tasks:

- Examine whether existing legal and regulatory authority is adequate to ensure NS/EP requirements will be met in the converged and next generation network (NGN) environment
- Identify and address other legal and regulatory issues related to convergence, as appropriate
- Analyze IS/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 Research and Development Exchanges, including linked or third party liability and new privacy legislation and regulations

- Address legal and regulatory issues affecting the other IES task forces at their request.

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 Network Security/Vulnerability Assessment Task Force (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 Cyber Crime* 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
- 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 rule-making, 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 of 2002* (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 multi-jurisdictional (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.
- 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
- Implement a framework to resolve multi-jurisdictional (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 politically 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 will continue to evaluate the national and homeland security implications of critical infrastructure data that is openly accessible on the Web sites of Federal departments and agencies. It also will continue to review Federal departments' and agencies' policies and practices for posting critical infrastructure information to the Internet.

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

Legislative and Regulatory Task Force Membership

Chair
Ms. Louise Tucker,
Telcordia Technologies, Inc.*

Vice Chair
Mr. Gerald Harvey,
Lockheed Martin Corporation

AT&T
Mr. Harry Underhill

BellSouth Corporation
Mr. David Barron

The Boeing Company
Mr. Robert Steele

Computer Sciences Corporation
Mr. Guy Copeland

MCI, Inc.
Mr. Dennis Guard

Microsoft Corporation
Mr. Bill Guidera

* Telcordia Technologies, Inc. is a wholly owned subsidiary of SAIC, which is a member of the NSTAC.

Nortel Networks Limited
Mr. Ray Strassburger

Northrop Grumman Corporation
Mr. Tim Nagle

Qwest Communications
Mr. Jon Lofstedt

Rockwell Collins, Inc.
Mr. Ken Kato

SBC Communications, Inc.
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

Bank of America, Inc.
Mr. John Huffstutler

BellSouth Corporation
Ms. Cristin Flynn

BellSouth Corporation
Mr. Lloyd Nault

Cellular Telecommunications
& Internet Association
Ms. Kathryn Condello

The George Washington University
Dr. Jack Oslund

Lockheed Martin Corporation
Mr. Larry Duncan

Microsoft Corporation
Mr. Scott Forbes

Qwest Communications
Mr. Tom Snee

Science Applications
International Corporation
Mr. Hank Kluepfel

Sprint Corporation
Mr. John Stagowski

United States
Telecommunications Association
Mr. David Kanupke

Verizon Communications
Ms. Ernie Gormsen

Verizon Communications
Mr. Lowell Thomas

Legislative and Regulatory Task Force Briefers

BellSouth Corporation
Mr. Doug Langley

Federal Communications Commission
Mr. Jim Dailey

Legislative and Regulatory Task Force Government Participants

Defense Information Systems Agency
Ms. Hillary Morgan

U.S. Department of Energy
Mr. John Greenhill

Research & Development (R&D)

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 President's National Security Telecommunications Advisory Committee (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 research and development (R&D) activities that have the potential to affect the national security and emergency preparedness (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 Office of Science and Technology Policy (OSTP), the 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, 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 Network Security Task Force (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 Industry Executive Subcommittee (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 and most recent 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.

Currently, the RDTF is preparing for its next scheduled RDX Workshop in October 2004 in Monterrey, California. The 2004 RDX Workshop will reconsider the issues addressed at the fifth RDX Workshop in Atlanta, Georgia, examining progress made in the areas identified.

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

Research and Development Task Force Membership

Chair
Mr. Guy Copeland,
Computer Sciences Corporation

Co-Vice Chair
Dr. Jack Edwards, Nortel Networks Limited

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

The Boeing Company
Mr. Robert Steele

Lockheed Martin Corporation
Mr. Gerald Harvey

Lucent Technologies
Mr. Frank Cantarelli

Motorola, Inc.
Mr. Ben La Pointe

Microsoft Corporation
Mr. Theodore Tanner

Qwest Communications
Mr. Jon Loftstedt

Raytheon Company
Mr. Frank Newell

SBC Communications, Inc.
Ms. Rosemary Leffler

VeriSign, Inc.
Mr. Mark Kosters

Verizon Communications
Mr. James Bean

Other Research and Development Task Force Participants

U.S. Department of Homeland Security,
Science and Technology Directorate
Dr. Simon Szykman

Georgia Institute of Technology
Dr. Seymour Goodman

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 Industry Executive Subcommittee (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 Network Security Information Exchange (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 Alliance for Telecommunications Industry Solutions (ATIS) Committee T1—Telecommunications, Working Group T1M1.5 OAM&P Architecture, Interface and Protocols for consideration as a standard.

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

During the NSTAC XXVII cycle (May 2003–May 2004), the IES created the Operations, Administration, Maintenance, and Provisioning (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 remedy vulnerabilities in pervasive software/protocols, define the "edge" elements of the Internet, and determine ways that the NSTAC could integrate its efforts to define and monitor significant critical infrastructures supporting the Internet with other industry activities.

In its *First Steps in Identifying and Remediating Vulnerabilities in Pervasive Software/Protocols* report, the ISATF analyzed five stages relevant to identifying and remediating vulnerabilities in pervasive software and protocols: prevention, detection, information sharing, analysis, and correction. In the area of prevention, the task force advocated aggressive public-private research and development activities and cited the need to develop adequate 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. Third, the task force emphasized that significant barriers to information sharing exist, such as the *Freedom of Information Act* (FOIA) and liability concerns, and advocated the creation of legislation that would ease the sharing of critical information. The ISATF also concluded that the analysis functions within industry that detect and publish vulnerabilities appear to be adequate, but the Government may find some benefit in better leveraging available synergies by consolidating Government-funded analysis centers where appropriate.

Finally, the task force observed that while many organizations are successfully correcting and remediating vulnerabilities, 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

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

- 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 National Institute of Standards and Technology (NIST) review the T1.276-2003 standard. If a review finds a conflict between the T1.276-2003 standard and existing Federal Information Processing Standards and NIST publications, NIST should make these conflicts known to the appropriate standards bodies.
- Federal departments and agencies be encouraged to use the T1.276-2003 standard in requests for proposals, as appropriate.
- Through the Department of Homeland Security (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.

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

Operations, Administration, Maintenance, and Provisioning Standard Working Group Membership

Chair
Dr. Jack Edwards, Nortel Networks Limited

Cellular Telecommunications
& Internet Association
Ms. Kathryn Condello

Lucent Technologies
Ms. Anne Frantzen

Microsoft Corporation
Mr. Philip Reitinger

Raytheon Company
Mr. Vernon Joyner

SBC Communications, Inc.
Mr. Jonathan Boynton

Science Applications
International Corporation
Mr. Hank Kluepfel

Other Operations, Administration, Maintenance, and Provisioning Standard Working Group Participants

Cellular Telecommunications
& Internet Association
Mr. Rick Kemper

National Institute of Standards
and Technology
Mr. Rick Kuhn

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

- 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 ongoing 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 rule making, 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, D.C., 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 (GSM) 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 (CDMA) 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, 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 national security and emergency preparedness (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 President's National Security Telecommunications Advisory Committee (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 Industry Executive Subcommittee (IES) formed the Wireless Task Force (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 National Institute of Standards and Technology (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
- Establish policies regarding the public availability and dissemination of Federal critical infrastructure information (such as the policies on Internet availability of Federal Communications Commission and the Federal Aviation Administration databases of tower locations).

At a December 2, 2002, IES task force 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 Recommendation

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 Telecommunications Resources

Investigation Group

Vulnerabilities Task Force (VTF)

Period of Activity

May 2002–February 2003

Issue Background

Following the business and executive sessions of the President's National Security Telecommunications Advisory Committee (NSTAC) XXV Meeting, the NSTAC Industry Executive Subcommittee 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 national security and emergency preparedness (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

In order to mitigate risks associated with concentration of assets, the NSTAC recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, 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
- Adopt telecommunications services procurement security policy guidelines that provide incentives to companies that follow best practices established by the Network Reliability and Interoperability Council, high levels of security standards, and other recognized business contingency principles.

In order to mitigate risks associated with trusted access issues, the NSTAC recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, 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*

- Adopt telecommunications service procurement security policy guidelines that provide positive incentives to those companies that follow Network Reliability and Interoperability Council 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. Future editions of the *NSTAC Issue Review* will summarize the activities and deliberations of the TATF once the group completes its report with Presidential recommendations.

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.

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 Industry Executive Subcommittee (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, the U.S. National Telecommunications and Information Administration (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, National Communications System (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 Industry Executive Subcommittee 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" provisions 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 Telecommunications Service Priority (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 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
- 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.

- 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 Industry Executive Subcommittee (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., Government Emergency Telecommunications Service [GETS] and Telecommunications Service Priority [TSP]) and to prepare for a Research and Development (R&D) Exchange Symposium focusing on network convergence issues.

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

In addition, the ITPITF analyzed potential implications of convergence on TSP services.

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

The ITPITF also examined evolving network technologies and capabilities that could support NS/EP functional requirements in both converged networks and the NGN. The ITPITF concluded that QoS and other new NGN capabilities would require some enhancement to best satisfy specific NS/EP requirements.

Based on the ITPITF's May 2000 report to NSTAC XXIII, the NSTAC recommended that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 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
- 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 and 29, 2000, the President's NSTAC co-sponsored its fourth R&D Exchange. 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 R&D Exchange 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.

- 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 R&D Exchange 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

- 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 of 1996*

- Conduct another R&D Exchange 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
- Utilize the Telecommunications Information Sharing and Analysis Center (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
- 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 National Communications System (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.

Recent and Planned Activities

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
- 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 Network Security and Information Exchanges' (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
- 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

- Develop policies and procedures to support the use of personal area network devices while reducing their risk of compromise.

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 National Coordinating Center for Telecommunications (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 11, 2001, attacks. Subsequently, in response to a request from the Special Advisor to the President for Cyberspace Security, the NSTAC formed the September 11, 2001 "Lessons Learned" Ad Hoc Group to provide an industry perspective on lessons learned in responding to the September 11, 2001, 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 Telecommunications Information Sharing and Analysis Center (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.

Information Assurance

Investigation Groups

Information Assurance Task Force (IATF)

Information Infrastructure Group (IIG)

Periods of Activity

IATF: May 15, 1995–April 22, 1997

IIG: April 22, 1997–September 23, 1999

Issue Background

At NSTAC XVII, 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 information assurance (IA) issues. At the May 15, 1995, Industry Executive Subcommittee (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 critical infrastructure protection (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—Presidential Decision Directive (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
- 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

- 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

- 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 Executive Order 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

- 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 Department of Justice (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 Information Sharing and Analysis Centers (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 Group

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 Industry Executive Subcommittee (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 tasking 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 Federal Communications Commission (FCC), and other relevant Government organizations. To that end, the LRG investigated the role of the FCC Defense Commissioner; investigated the need for an NS/EP industry advisory body to the FCC; 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 Network Reliability and Interoperability Council (NRIC) provided the FCC with a series of recommendations aimed at improving the planning process for National Services and deployable telecommunications services intended or required on a national or regional basis.

The 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 Presidential Decision Directive (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 Year 2000 (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 Cellular Priority Access Service (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 Industry Executive Subcommittee (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 Presidential Decision Directive (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 Information Sharing and Analysis Center (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 National Communications System (NCS) member organizations and NCC industry representatives to develop a common framework for assessing the NCC's ongoing role. The subgroup validated the original ten 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 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-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 Information Assurance (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

- 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.

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 Industry Executive Subcommittee (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

- 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 Legislative and Regulatory Working Group (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, Industry Executive Subcommittee (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, Office of Science and Technology Policy (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
- 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 NSTAC XVI 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 Global Information Infrastructure (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 has 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, Industry Executive Subcommittee (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 inter-connected carriers
- Evaluate the risk to NS/EP user telecommunications
- If significant risk existed, examine procedural or technological alternatives for mitigating it
- 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. Department of Justice (DOJ) and Department of Defense 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 National Coordinating Center for Telecommunications (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), National Communications System (NCS), and the North American Electric Reliability Council (NERC) participated in the Energy Task Force.

The NSTAC Industry Executive Subcommittee (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
- 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 seven-day electric power outage

- 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

- 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 research and development (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

- 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.

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 Office of the Manager, National Communications System (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 Government Emergency Telecommunications Service (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 Federal Communications Commission (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 the other Energy Task Force recommendations.

- 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
- 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, National Communications System (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 Industry Executive Subcommittee (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 Office of the Manager, National Communications Systems (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 Operations Working Group (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 Industry Executive Subcommittee (IES) established the TSP Task Force on February 21, 1985, to advise and assist the Office of the Manager, National Communications System (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 National Communications System (NCS) Council of Representatives TSP Subcommittee and the TSP Task Force drafted and approved the charter in February 1990, and the Department of Defense (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 Council of Representatives 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 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 two-and-a-half-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
- 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.

Physical Security of the Public Switched Network

Investigation Group

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

Period of Activity

December 1990–September 1991

Issue Background

On December 13, 1990, at NSTAC XII, an NSTAC member questioned the physical security of the public switched network (PSN), because the issue resurfaced in the National Research Council report on the growing vulnerability of the PSN. Several task forces had previously addressed physical security. In March 1990, the NSTAC's *National Research Council Report Task Force Final Report* addressed the physical security issue and stated that industry agreed there were PSN vulnerabilities, but disagreed that there was a growing trend. The NSTAC tasked the IES to work with the Office of the Manager, National Communications System (OMNCS) to address this issue. The IES subsequently assigned the PWG the task of assisting the OMNCS. The PWG examined the physical security issue to determine if the NSTAC should review further.

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 National Coordinating Center for Telecommunications 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 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.

History of NSTAC Actions and Recommendations

At the October 3, 1991, NSTAC XIII meeting, members approved the PWG report conclusion that the physical security issue required no further study.

Report Issued

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

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 Industry Executive Subcommittee (IES) with continuing the intelligent network effort on an interim basis pending review by the IES Plans Working Group (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 Office of the Manager, National Communications System (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 Operations Working Group (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
- Develop and implement a strategy for influencing the direction of AIN standards.

The AIN Program Office awarded a five-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 Industry Executive Subcommittee (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
- 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 Federal Communications Commission (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, D.C., 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 Group

Commercial Satellite Survivability (CSS) Task Force

Periods of Activity

December 1982–April 1984

June 1988–March 1990

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 Industry Executive Subcommittee (IES) reactivated the CSS Task Force to review the proposed objectives and implementation initiatives of the Commercial 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.

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 public switched network (PSN) via direct connection at an access tandem

- 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.

During NSTAC Cycle XXVII (May 2003–May 2004), the NSTAC revisited issues related to NS/EP dependence on commercial satellites with a study focused on commercial satellite vulnerabilities. (See the Satellite Security section in the Active Issues section of this *NSTAC Issue Review.*)

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.

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.

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 Industry Executive Subcommittee (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 ten 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 National Security Agency (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 Office of the Manager, National Communications System (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 Council of Representatives 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 Office of the Manager, National Communications System (OMNCS) developed the *NS/EP Telecommunications Plan of Action* to implement relevant portions of Executive Order 12472 and National Security Decision Directives 47 and 97. The plan, approved by the National Communications System (NCS) Committee of Principals 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
- 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 three-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 Industry Executive Subcommittee (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
- Government participation in standards organizations.

The President endorsed those initiatives, and the Office of the Manager, National Communications System (OMNCS) undertook a CNS program. On November 6, 1987, the NSTAC approved the Telecommunications Systems Survivability (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 public switched network (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 Funding and Regulatory Working Group (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 Industry Executive Subcommittee (IES) to:

- Adopt the methodology developed by the FNI Task Force
- Issue the funding methodology as guidance to all existing and future task forces
- 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
- 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 Telecommunications Systems Survivability (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
- 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 Office of the Manager, National Communications System (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 public switched network (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 Industry Executive Subcommittee (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
- 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 two 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
- Provide the necessary funding and develop incentives for AIP survivability enhancements.

The Telecommunications Systems Survivability (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 National Coordinating Center for Telecommunications (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 Telecommunications System Survivability (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 National Communications System (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.

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.

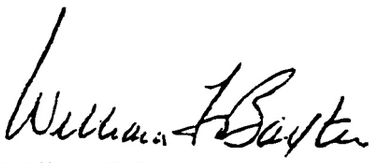
For example, it would appear preferable for each carrier to maintain its own inventory of spare circuits, etc., rather than to create a centralized data base of such information, unless access to such a data base was strictly controlled and limited to the carrier concerned or to government employees. 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 19, 2004)

Dr. Vance D. Coffman, NSTAC Chair	Chairman and CEO Lockheed Martin Corporation
Mr. F. Duane Ackerman, NSTAC Vice Chair	Chairman, President, and CEO BellSouth Corporation
Mr. James F. Albaugh	President and CEO Integrated Defense Systems The Boeing Company
Dr. J. Robert Beyster	Chairman and CEO Science Applications International Corporation (SAIC)
Mr. Gregory Brown*	President and CEO Commercial, Government, and Industrial Solutions Sector Motorola, Inc.
Mr. Gary D. Forsee	Chairman and CEO, Sprint Corporation
Mr. Van B. Honeycutt	Chairman and CEO Computer Sciences Corporation (CSC)
Mr. Clayton M. Jones	President and CEO, Rockwell Collins, Inc.
Mr. Craig O. McCaw	Chairman, Teledesic Corporation
Mr. Craig J. Mundie	Senior Vice President, Microsoft Corporation
Mr. Richard C. Notebaert	Chairman and CEO, Qwest Communications

* Membership pending White House approval (as of May 19, 2004).

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)
Ms. Patricia F. Russo	Chairman and CEO, Lucent Technologies
Mr. Stratton Sclavos	Chairman and CEO, VeriSign, Inc.
Mr. Stanley Sigman*	President and CEO, Cingular Wireless
Ms. Susan Spradley	President, Wireline Networks Nortel Networks Limited
Mr. William H. Swanson	Chairman and CEO, Raytheon Company
Mr. Lawrence A. Weinbach	Chairman and CEO, Unisys Corporation
Mr. Edward E. Whitacre, Jr.	Chairman and CEO SBC Communications, Inc.
Position Vacant	AT&T
Position Vacant	Electronic Data Systems Corporation (EDS)
Position Vacant	MCI, Inc.
Position Vacant	Northrop Grumman Corporation
Position Vacant	Verizon Communications

* Membership pending White House approval (as of May 19, 2004).

NSTAC XXVII Executive Report to the President

Executive Report on the 27th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVII) May 19, 2004

The President's National Security Telecommunications Advisory Committee (NSTAC) held its 27th meeting (NSTAC XXVII) on May 19, 2004, at the U.S. Chamber of Commerce in Washington, D.C. The meeting, which centered around the theme "Advising the President on Critical Telecommunications: Partnership 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 State (DOS), the Federal Communications Commission (FCC), and the executive and legislative branches. The NSTAC Principals met with former Virginia Governor James S. Gilmore III during the Executive Breakfast; reviewed NSTAC activities over the past cycle, received several briefings, and met with Secretary of State Colin Powell and other senior Administration officials during the Business Session; engaged in discussion with Representative Joseph Barton (R-TX) and a number of senior Administration officials during the Executive Session; met with Chairman Michael Powell, FCC, during the Executive Luncheon; and met with President George W. Bush and other senior Administration leaders.

This Executive Report summarizes those presentations and deliberations. Also attached are the recommendations to the President from NSTAC XXVII (Attachment 1) and an attendance list of NSTAC Principals (Attachment 2).

NSTAC XXVII Business Session

Opening Remarks.

Dr. Vance Coffman, Chairman and Chief Executive Officer (CEO), Lockheed Martin and NSTAC Chair, called to order the 27th NSTAC Business Session on May 19, 2004, at 8:15 a.m. at the U.S. Chamber of Commerce in Washington, D.C. Dr. Coffman noted that the day would serve as his last meeting as the NSTAC Chair, and that at the end of the day's proceedings, Mr. F. Duane Ackerman, BellSouth, the current NSTAC Vice Chair, would be assuming the Chairmanship.

Introduction of Key Government Officials and NSTAC Principals.

Dr. Coffman then recognized the senior Government officials participating in the meeting:

- Mr. Robert Liscouski, Assistant Secretary for Infrastructure Protection, Information Analysis and Infrastructure Protection (IAIP) Directorate, DHS;

- Dr. John Marburger, Director of the President's Office of Science and Technology Policy (OSTP);
- Dr. Charles McQueary, Under Secretary for Science and Technology, DHS;
- Lieutenant General Patrick Hughes, U.S. Army (Ret.), Assistant for Homeland Security for Information Analysis; and
- Secretary of State Colin Powell, DOS.

Dr. Coffman then recognized the following NSTAC Principals recently appointed by President George W. Bush: Mr. Gary Forsee, Sprint, and Mr. William Swanson, Raytheon.

Dr. Coffman additionally recognized two individuals who have been recently nominated to serve on the NSTAC and are awaiting final approval by the President: Mr. Greg Brown, Motorola, and Mr. Stanley Sigman, Cellular Telecommunications and Internet Association.

Dr. Coffman then reviewed the agenda for the day, outlining the presentations that would be given by Government stakeholders. Before delivering his "Cycle in Review," Dr. Coffman thanked all NSTAC Principals who served as Champions for key NSTAC issues over the past year, as well as those who volunteered to lead the development of key NSTAC issues through the next cycle.

NSTAC XXVII Cycle in Review.

Dr. Coffman presented the "Cycle in Review," which outlined the activities of the NSTAC during the XXVII cycle.

This review included an overview of the Financial Services Task Force (FSTF), the Satellite Task Force (STF), the Operations, Administration, Maintenance, and Provisioning (OAM&P) Working Group, the Trusted Access Task Force (TATF), the Legislative and Regulatory Task Force (LRTF), the NSTAC Outreach Task Force (NOTF), the Research and Development Task Force (RDTF), and the Cyber Scoping Group (CSG).

Dr. Coffman opened his presentation with an overview of the work and accomplishments of the FSTF. Continuing its tasking from NSTAC Cycle XXVI, the FSTF explored the physical aspects of the financial services sector concerns for resiliency and redundancy capabilities of the telecommunications infrastructure. The FSTF issued a report to the President that provided seven key recommendations and a strong assessment of the additional measures needed to ensure the resiliency and reliability of critical NS/EP circuits.

Dr. Coffman then presented the work of the STF during the past cycle. He noted the STF examined the use of commercial satellites in national NS/EP missions, vulnerabilities, and mitigation techniques. The STF coordinated with many non-NSTAC companies and Government agencies, and proposed recommendations to the President for enhancing the security of the commercial satellite infrastructure and the robustness of NS/EP communications. The STF report identified 22 findings, and highlighted the need for the Government to improve the management of its commercial satellite communications (SATCOM).

The report also provided three recommendations to the President regarding the need for a national policy on the provisioning and management of commercial SATCOM services, funding to support the implementation of commercial SATCOM NS/EP, and the appointment of commercial satellite service providers and associations to represent the SATCOM industry on the NSTAC.

Dr. Coffman then discussed the work of the OAM&P Working Group. This working group was established as a follow-on to the spring 2003 Network Security Information Exchange. In the report submitted to the President, the group recommended the adoption and use of the OAM&P Telecommunications Standard by the Federal Government and other critical infrastructures. The group also developed policy guidance related to the standard on OAM&P Baseline Security Requirements for the Management Plane to promote awareness and implementation of the standard.

The TATF was the next subject addressed by Dr. Coffman. He stated that the TATF is examining ways to implement a national security background check program. The TATF is also examining various Government and private sector background check processes and credentialing to better capture concerns with the current system. The group is expected to submit its report to the President during NSTAC Cycle XXVIII, and will continue to address the development of a national plan for controlling access at the perimeter of a disaster area and the adoption of telecommunications service procurement security policy guidelines.

Dr. Coffman noted that the participants would hear more on this issue during the Executive Session from Mr. Richard Notebaert, Qwest.

Dr. Coffman then addressed the work of the LRTF. This task force has continued to advise the President on national policies and regulatory issues that conflict with NS/EP missions. The LRTF drafted, and the NSTAC submitted, a letter to the President, which included recommendations on this issue. In addition, the LRTF drafted, and the NSTAC submitted, a report to the President, which included recommendations on barriers to information sharing under the *Critical Infrastructure Information Act of 2002*. The group is currently examining issues regarding open-source critical infrastructure data. Dr. Coffman encouraged the member companies to conduct internal reviews of the information posted to their respective Web sites. He noted that the LRTF would continue its activities through the next NSTAC cycle.

Next, Dr. Coffman discussed the NOTF and its work to solicit feedback and input on NSTAC products and outreach initiatives, and promote the adoption of NSTAC recommendations. To accomplish these goals, the task force arranged meetings with key Government stakeholders from the OSTP, the Homeland Security Council (HSC), the Office of Management and Budget (OMB), and the National Security Council (NSC). The task force also developed and delivered an NSTAC orientation briefing to members of the Industry Executive Subcommittee (IES) and is currently planning an IES off-site meeting scheduled for September 15–17, 2004, at the Kingsmill resort in Williamsburg, Virginia.

Dr. Coffman continued his briefing with an overview of the RDTF. This task force developed an official proceedings document as a follow-up to the 2003 Research and Development Exchange (RDX) and formed actionable plans to address the findings. The task force also developed a paper addressing the definition of NS/EP and examined the development of a pilot testbed for NS/EP research and development purposes. Dr. Coffman then discussed the scheduling of the 2004 NSTAC RDX for October/November on the West Coast and noted that the task force will continue its activities through the next NSTAC cycle.

Dr. Coffman then reviewed the activities of the most recently established group, the Cyber Scoping Group (CSG). The CSG examined and prioritized issues associated with cyber-related infrastructure interdependencies. Specifically, the group examined Voice over Internet Protocol (VoIP) and network convergence issues, software quality, and cyber attack vulnerabilities. Dr. Coffman noted that the group would hear more on those issues during the Executive Session from Mr. Craig Mundie, Microsoft.

Lastly, Dr. Coffman discussed opportunities pursued by the NSTAC to collaborate with the National Infrastructure Advisory Council (NIAC). The NSTAC provided input to the NIAC's draft "Report on Cross Sector Interdependencies and Risk Assessment Guidance."

An NSTAC ad hoc group convened and produced a report suggesting that the NIAC report also consider separately examining each sector with regard to its own circumstances and that a higher degree of interdependency in a sector may both necessitate and lead to a higher degree of coordination.

In conclusion, Dr. Coffman acknowledged and thanked the IES members for their hard work and also thanked the attendees for their participation in the NSTAC XXVII Meeting.

IAIP Six-Month Outlook.

Dr. Coffman introduced Assistant Secretary Liscouski, who thanked the NSTAC Principals and IES members for the opportunity to speak with them and for their hard work. Mr. Liscouski recognized the NSTAC as a richly talented body from which DHS welcomes input and looks forward to continued partnership. In the past 14 months, DHS has worked diligently to address the tactical and strategic challenges arising from building the new Department and the work laid out in *The National Strategy for Homeland Security*, *The National Strategy to Secure Cyberspace*, and *The National Strategy for the Physical Protection of the Critical Infrastructure and Key Assets*. Mr. Liscouski recognized the critical importance of input from the private sector to identify and protect the Nation's critical infrastructures—80 percent of which is owned by the private sector—and noted that DHS is diligently pursuing that goal.

Looking ahead, Mr. Liscouski described the IAIP Directorate's priorities for critical infrastructure protection over the next six months.

Mr. Liscouski characterized that period as posing increased risk of potential terrorist activity, noting high-profile events such as the political conventions, the summer Olympics, and the Presidential election. He said that IAIP is working on a plan to identify and validate potential targets, and noted that DHS formed an interagency working group to examine security priorities for the upcoming events. Mr. Liscouski said the bombings in Madrid, Spain, on March 11, 2004, highlighted remaining vulnerabilities and the terrorists' enduring desire to cause mass casualties, disrupt the democratic political process, and erode the public's confidence in the Government.

DHS is actively working to develop a tactical plan, due in December 2004, to fulfill the responsibilities laid out in *Homeland Security Presidential Directive 7* (HSPD-7); however, DHS recognizes that it cannot wait until December to begin protecting critical infrastructure and has therefore begun implementing key programs. Mr. Liscouski noted the importance of industry working with State and local governments to ensure that critical infrastructures are secure, emphasizing that effective public and private sector coordination is a critical component of planning and preparedness. Mr. Liscouski noted that one major effort under way at DHS is to raise the Nation's current base level of security by elevating the security expectations and activities for the "yellow" security baseline. The goal is to build the capability to sustain an elevated state of alert in the absence of a specific threat without overburdening State and local governments and the private sector.

Dr. Coffman asked Mr. Liscouski where he believes the NSTAC can provide additional input. Mr. Liscouski replied that the NSTAC's current issues (trusted access, vulnerabilities, etc.) are the appropriate ones to examine. He added that the NSTAC can help DHS identify areas where immediate action can be effective and can also help distribute the appropriate homeland security message, turning awareness to action. When asked what role DHS is playing in security measures for the summer Olympics in Athens, Greece, Mr. Liscouski said the Secret Service and the Coast Guard are supporting and advising the Greek Government.

The White House and Research and Development.

Dr. Marburger summarized the key roles and responsibilities of OSTP to ensure the delivery of NS/EP telecommunications during times of national crisis. He stated that, in contrast to the six-month outlook provided by Mr. Liscouski, the OSTP has a longer term role in providing interagency coordination of research and development (R&D) programs and science and technology policy. He suggested that swift advances in information technology present both opportunities and challenges with respect to NS/EP telecommunications. Dr. Marburger recognized the increased importance of coordination and cooperation among agencies in this rapidly changing environment. He said the unique insights of the President's NSTAC are particularly valuable, noting that committee recommendations are explicitly incorporated in OSTP plans, including annual budgetary documents.

Dr. Marburger also described his participation in the NSTAC's 2003 RDX, noting the important role this event plays in helping to determine national R&D priorities. Colonel (Select) Greg Rattray, NSC, added that the draft NS/EP definition paper, developed by the RDTF, has proven extremely helpful in the development of a report being produced within the Executive Office of the President (EOP) addressing the evolving definition of the term.

DHS and Research and Development.

Dr. Coffman introduced Dr. McQueary, who thanked the NSTAC Principals for the opportunity to speak with them. He also acknowledged the work of the Commission led by Governor Gilmore, noting that the principles of the Gilmore Commission report were used to help define the role of the new Science and Technology (S&T) Directorate within DHS.

Dr. McQueary outlined the mission of the S&T Directorate: to conduct, stimulate, and enable research, development, testing, and evaluation; and to ensure the timely transition of technologies and capabilities to first responders and others at Federal, State, and local levels. While initially focused on technology, the directorate has recently become engaged in systems application, driving and determining capabilities, investments, and improvements. To that end, the organization has a $1 billion budget, with 60 percent set aside for operational needs, and the remainder dedicated to private sector, academia, and national and Federal laboratories. Dr. McQueary recognized private industry's important role in translating capabilities into products.

Dr. McQueary commented on the growth of the S&T Directorate, which began with only 6 employees and now has a staff of 250. He noted that he has been impressed with the quality of the people it attracts and with the passion the employees have for their important mission. He emphasized the progress made in the areas of standards and interoperability for first responders and discussed the work that S&T is conducting to counter biological and chemical attacks. Dr. McQueary highlighted the blue modeling capabilities being used to enhance detection and response efforts in mass transit facilities and the BioWatch program, which is designed to monitor the air for biological agents. Closing his remarks, Dr. McQueary stated that effective working partnerships among industry, academia, Federal and national laboratories, and the Government are critical in protecting the Nation from terrorist attacks.

When asked whether the BioWatch program has the capability to detect sarin gas, the gas recently found in a shell in Iraq, Dr. McQueary replied that for security considerations, he could not publicly divulge the program's capabilities because it may draw attention to what they cannot detect. In response to a question regarding how the NSTAC can support the directorate's initiatives, Dr. McQueary replied that modeling will play a very important role in future S&T activities; and he will rely heavily on the private sector, including NSTAC member companies, for simulation capabilities.

Industry and Homeland Security.

Mr. Joseph Grano, Jr., Chairman, UBS Financial Services Inc. and Chairman, Homeland Security Advisory Council (HSAC), briefed on the impact of the war on terrorism on the financial industry. Mr. Grano reviewed the chain of events on the morning of September 11, 2001, specifically, the financial market's reactions to the events. On September 11, 2001, the New York Stock Exchange (NYSE) delayed its 9:30 a.m. opening and then announced at 9:58 a.m. that it would remain closed for the day. Later that afternoon, the NYSE, the American Stock Exchange, and the National Association of Securities Dealers Automated Quotation (NASDAQ) announced they would also be closed the following day. Due to severe damage to Verizon's central switching facility located near the World Trade Center, the connectivity of firms to customers and the markets was severely disabled.

Mr. Grano noted that on September 12, 2001, members from the financial sector and utility companies met with Government leaders to discuss the reopening of the markets the next day. As a result of the meeting, the decision was made to delay the opening of the equities markets until September 17, 2001, to avoid the risk of prematurely opening the market, causing the stock market to crash, and diminishing the global population's faith in the market. The terrorist attacks caused tremendous harm to the financial industry. The industry suffered a significant loss of life, collateral damage, loss of electrical power, communications, and transportation, as well as the closure of stock and bond markets, which greatly affected industry profits.

In response to the terrorist attacks, UBS and PaineWebber implemented their communication plans and provided support for employees as well as clients and competitors in need of assistance. Operations/technical staff and senior management immediately launched to crisis management mode. Mr. Grano highlighted several lessons learned to better prepare companies for another disaster. He emphasized the need for companies to differentiate between disaster recovery and business continuity planning, and recognize the importance of both cyber and physical security, public and private partnerships, and communications and preparedness. UBS and PaineWebber realized the importance of employee emergency contact information as well as the need to understand the psychographics of their employees.

Mr. Grano then described numerous terrorist attacks from 1979 to the present as a reminder of the magnitude of terrorism the United States faces today, but emphasized that the United States is safer today than on September 10, 2001, because the country is more aware of its vulnerabilities and has taken steps to mitigate those weaknesses. He continued by stating the importance of remembering the war on terror is "not about giving up liberty but about securing liberty."

Mr. Grano discussed the critical infrastructure landscape of the northeastern United States, illustrating the vast numbers of airports, chemical facilities, power stations, pipelines, rail lines, police departments, and hospitals, and the importance of the public and private sectors to collaborate.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets has three strategic objectives: (1) prevent terror attacks within the United States; (2) reduce the Nation's vulnerability to terrorism; and (3) minimize damage and recover from an attack quickly. He noted DHS is striving to meet the challenges of these objectives by creating directorates related to the six critical mission areas and initiatives defined in *the National Strategy,* which are intelligence and warning, protecting critical infrastructure, defending against catastrophic terrorism, emergency preparedness and response, domestic counterterrorism, and border and transportation security.

Mr. Grano concluded by emphasizing the importance of protecting the Nation's critical infrastructure and the need for the private sector's involvement, as 80 percent of the critical infrastructure is privately owned.

DHS Intelligence Overview.

Dr. Coffman introduced Lieutenant General (LTG) Patrick Hughes, U.S. Army (Ret.), Assistant Secretary of Homeland Security for Information Analysis, who began his briefing by stating that DHS has quickly become a member of the overall U.S. intelligence community, working daily with the Federal Bureau of Investigation, Central Intelligence Agency, National Security Agency, and Department of Defense. LTG Hughes then discussed the current situation of terrorist activity around the world and in the United States. He noted that the United States is "currently being probed by terrorist groups attempting to enter the United States, most likely with a plan to strike us." Intelligence suggests that these terrorist groups are planning to conduct an attack greater than the September 11, 2001, attacks by possibly employing a weapon of mass effect (e.g., biological or chemical weapons), and targeting large gatherings or critical infrastructures. To prevent these attacks, DHS is focusing on upcoming events, including the dedication of the World War II Memorial, the G-8 Summit, the Democratic and Republican national conventions, and the Presidential election and inauguration. LTG Hughes summarized his briefing by saying that the terrorists are still out there, and it is the job of DHS to prevent attacks, and if not prevented, then minimize their effects and respond to the consequences.

LTG Hughes then responded to a question expressing concern about the economic impact of another terrorist attack, specifically, if a terrorist attacked a common gathering place, such as a fast food restaurant or shopping mall. He emphasized the importance of citizens reporting suspicious activities, such as surveillance on "soft targets" of this nature. A Principal asked what more the NSTAC or information sharing and analysis centers (ISAC) can do for DHS to prevent future attacks. LTG Hughes responded that DHS needs to establish secure communications links at the secret level with the ISACs and increase training and awareness with State and local governments and the private sector, making people more aware of the ways in which they can help to secure the infrastructures vital to the United States. Participants expressed the need to keep the lines of communications open on receiving intelligence.

LTG Hughes stated that when DHS verifies intelligence on specific threats, it contacts companies or ISACs to share the information. A Principal expressed concerns about cultural diversity and viewpoints at DHS. LTG Hughes responded by noting that DHS has employees representing diverse opinions and perspectives from numerous cultures. He concluded his briefing by saying that DHS needs the NSTAC for its "information, intelligence, advice, assistance, knowledge, and wisdom."

International Views.

Dr. Coffman introduced Secretary Powell, who thanked the NSTAC Principals for the opportunity to speak with them again this year. Secretary Powell described the DOS efforts in implementing secure communications and broadband for all of its employees. He commented that the Internet has changed how the Department does business. For example, consulate officers send bulletins with pictures via telegraph regularly. In addition, visa applications including pictures and application status can be accessed remotely from anywhere in the world. He added, however, that the ease in access comes at a price. Secretary Powell stressed the importance for groups, such as the NSTAC, to address the issues related to network security, privacy, and cyber crime by building in the necessary safeguards when infrastructures are developed. He said the exporting of necessary tools—technology and legislative principles—to allies is necessary, as is ensuring that intelligence officers track the activities of terrorists.

In addition, he encouraged feedback from industry on resolutions in the United Nations and other international organizations necessary to help industry do its job, especially in the area of security and international concerns. A Principal asked how national security communications relates to next generation networks (e.g., electronic messaging for emergency communications). Secretary Powell said in recent years, the Department has begun to use secure video teleconferencing; and he would like to see the installation of secure video conferencing capabilities with select foreign ministers. Concluding his remarks, Secretary Powell said that while the Internet and new technologies are changing how DOS personnel conduct business, the telephone will remain an important communications vehicle.

Adjournment.

Dr. Coffman thanked the NSTAC Principals and the senior Government officials for their participation in the Business Session. He indicated that there would be additional opportunities for further discussion during the Executive Session and Executive Luncheon. Dr. Coffman also took the opportunity to thank DHS staff, as well as IES members, for their hard work and support throughout the past year. Dr. Coffman adjourned the Business Session at 10:25 a.m.

NSTAC XXVII Executive Session

Opening Remarks.

Dr. Coffman called to order the 27th NSTAC Executive Session in the U.S. Chamber of Commerce in Washington, DC, on May 19, 2004, at 10:35 a.m. Dr. Coffman 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. Prior to the actual Executive Session discussion, Dr. Coffman invited Ms. Janet Jefferson, Industry Operations Branch Chief, Office of the Manager, National Communications System (NCS), to the dais to be recognized for her many years of service to the Government and specifically, the NSTAC. As Ms. Jefferson planned to retire from Government service shortly after the NSTAC XXVII Meeting, Dr. Coffman presented her with a plaque of appreciation.

IAIP Six-Month Outlook.

Dr. Coffman reintroduced Mr. Liscouski, who wished to expand upon his presentation on "Security Planning for Period of Increased Risk" during the Business Session. He informed the NSTAC Principals that during the upcoming six to eight months, the Nation was to enter a period of increased risk of potential terrorist activity. Specific upcoming high-profile National Special Security Events (NSSE) that concern DHS as potential terrorist targets include the national World War II Memorial Dedication, the Democratic National Convention, the Republican National Convention, and the Presidential Inauguration.

To prepare for these incidents, DHS is planning to re-baseline the yellow threat level. DHS recognizes that the efforts implemented during times of increased threat posture (orange or red level) are not sustainable and therefore are executed only during elevated threat levels. However, to ensure that the Nation is best prepared for a terrorist incident during the yellow security posture, DHS is working to raise the level of sustainable security efforts.

In response to Mr. Liscouski's warning, the NSTAC Principals asked what DHS expects from the NSTAC companies in the upcoming period of increased risk. Mr. Liscouski emphasized the threats are of national importance, and for this reason, industry must engage not only with the Federal Government but also with the appropriate State and local agencies. Furthermore, he noted that in the event of an attack, DHS would need input from industry to rebuild the infrastructures in the aftermath. A Principal informed Mr. Liscouski that industry is best able to respond when information regarding an imminent threat is provided, and it is essential that industry be kept abreast of threat information. A participant suggested that the NSTAC examine both industry preparedness for the NSSEs and industry response in the event of an attack. Mr. Liscouski endorsed this suggestion.

Congressional Views on Homeland Security.

Dr. Coffman introduced Representative (Rep.) Barton, the recently elected Chairman of the House Committee on Energy and Commerce. On behalf of the legislative branch, Rep. Barton welcomed the out-of-town NSTAC Principals to Washington, D.C.

He stated that the NSTAC serves an important function in its unique public/private partnership role. Rep. Barton discussed his role as chairman of the House Committee on Energy and Commerce. This committee has jurisdiction on telecommunications policy and also oversees Internet privacy and security issues. Rep. Barton said the committee has made progress in identifying and developing policies on pressing issues. A few weeks ago, the committee held a hearing on spyware entitled, "Spyware: What You Don't Know Can Hurt You," and discussed the necessity to increase penalties for Internet abusers. It is expected that the bill (H.R. 2929, *The Safeguard Against Privacy Invasions Act*) will be marked up shortly. Rep. Barton predicted that the U.S. Congress would likely approve the "spyware bill" later this year.

Dr. Coffman asked about the committee's work in balancing the freedoms and rights of citizens while also maintaining protection of information. Rep. Barton explained that historically, legislation having to do with the private sector is reactive, not proactive. The legislative branch is currently trying to catch up with the private sector. Rep. Barton affirmed that every citizen has a "guaranteed right to privacy," and the computer is not necessarily an open window to information; laws are still in effect. There needs to be a balance between the need for information gathering and privacy. While the legislative branch does not necessarily have the answer, it is entertaining a privacy protection bill. Rep. Barton also noted that he; Rep. Edward Markey (D-MA); Senator Richard Shelby (R-AL); and Senator Christopher Dodd (D-CT) lead a Congressional privacy caucus.

A Principal asked how the committee is looking to balance Internet privacy and terrorist actions. Rep. Barton discussed the USA PATRIOT Act and explained that it is now mandatory to secure a writ from a Federal magistrate to obtain wiretapping capabilities. There are formal processes that check the Government's powers. When asked about monitoring Internet traffic, Rep. Barton stated that his committee did not have jurisdiction specifically on that issue because it is more of an intelligence matter.

Discussion of Future NSTAC Issues.

Dr. Coffman invited Dr. Brian Dailey, Lockheed Martin and Industry Executive Subcommittee (IES) Working Session Chair, to facilitate the discussion of future NSTAC issues for consideration. Dr. Dailey in turn invited the NSTAC Principal/Champion for each issue to briefly discuss the issue and any relevant NSTAC history on the topic.

Next Generation Networks Challenges.

Mr. Craig Mundie, Microsoft, reminded the NSTAC Principals that the convergence of the public switched telephone network and Internet protocol networks into the global next generation network (NGN) is changing how the Government and critical infrastructures meet their needs for national security and emergency preparedness (NS/EP) communications. To address this issue, on the March 4, 2004, NSTAC Principals' Conference Call, the Principals established the Cyber Scoping Group to examine issues associated with NGN convergence and cyber security.

The work of the group culminated in a conference call with several NSTAC Principals held on May 14, 2004, during which a proposal was made to establish a task force to: (1) agree on a high-level description of the expected network environment or ecosystem of the NGN, and its interdependencies, on which NS/EP applications will rely; (2) identify NS/EP user requirements for the NGN, outline how these requirements will be met, 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 (3) examine relevant user scenarios and expected cyber threats, and recommend optimal strategies and actions to address cyber threats to meeting NS/EP user requirements and delivery of services. There was wide agreement that a task force should be established.

Trusted Access.

Mr. Richard Notebaert, Qwest, provided an overview of the activities of the Trusted Access Task Force (TATF) during the NSTAC XXVII cycle. He reminded the Principals that the task force was created as a result of discussions held at the NSTAC XXVI Meeting and was tasked to address several recommendations from the Vulnerabilities Task Force's (VTF) March 2003 report, entitled "Trusted Access to Telecommunications Facilities." He noted that trusted access to telecommunications facilities and NSSEs remains of the utmost importance both for prevention of an attack as well as mitigation and restoration activities should an attack occur.

Mr. Notebaert explained that during the course of the previous NSTAC cycle, task force members quickly acted 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. To gather data, the task force distributed a questionnaire to several NSTAC member companies and Government agencies requesting input on their current background check processes. The task force also interviewed representatives from the General Services Administration's Federal Identity Credentialing Committee, the Transportation Security Administration (TSA), the Nuclear Regulatory Commission, the Department of Defense, the Federal Bureau of Investigation, and DHS. Mr. Notebaert stated that the task force has the preliminary research for the tasking completed but will continue its work into the next cycle to analyze the data gathered during the aforementioned task and apply it to the concept of a national background check process.

Mr. Notebaert further stated that while the task force members have not yet completed an extensive analysis of the data, they determined that the airport environment, with its variety of people, such as passengers, pilots, maintenance workers, and food vendors with access to important facility locations, is very similar to conditions experienced at a telecommunications facility. Consequently, the task force is interested in learning more from the TSA to determine if physical security lessons learned and/or best practices from the airport community may be applied to background check processes for the telecommunications industry.

He pointed out that the task force will have to determine how regimented the background check process should be and then decide on specific criteria that should be applied to the application process. He confirmed that work had not yet begun on tasks 3 and 4 and encouraged Government counterparts to become more actively engaged in the task force activities moving forward, especially with regard to issues related to the physical security of NSSEs over the next six to eight months.

International Concerns.

Mr. Stratton Sclavos, VeriSign, briefed the NSTAC Principals on the need to examine the threats to the Nation's cyber infrastructure from abroad. Recently, attacks to the cyber network have been increasing daily; and as a result, U.S. companies have been experiencing negative economic and productivity impacts. Mr. Sclavos explained the majority of these attacks either originated or were sustained outside of the United States, and the attacks suggest that the security of our economic and cyber infrastructure could be threatened by the global nature of the Internet. Since there is currently no international Internet regulation, Mr. Sclavos recommended that the NSTAC examine the development of an international security framework for the Internet as either an extension of the NGN convergence issue or as a separate issue altogether.

Dr. Coffman commented that the issue of international threats to the Internet is worthy of examination by the NSTAC; however, he noted that the issue is complex and needs to be more clearly defined. Colonel (Select) Greg Rattray, National Security Council, further added that the State Department may need to be involved to establish international agreements on the issue. The NSTAC Principals agreed that the IES should more clearly define the parameters of the issue and determine if the issue should be included in the work of the NGN group or if a separate task force should be established to address it.

Adjournment.

Dr. Coffman expressed his appreciation to the NSTAC Principals and the senior Government officials for their active participation in both the Business and Executive Sessions. He also recognized the important work of the IES and how it provided the framework for a successful NSTAC meeting. Dr. Coffman adjourned the NSTAC XXVII Executive Session at 12:05 p.m.

NSTAC XXVII Executive Luncheon

Opening Remarks.

Dr. Coffman called the Executive Luncheon to order at 12:15 p.m. in the Herman Lay room at the U.S. Chamber of Commerce, Washington, D.C. He introduced General John Gordon, Assistant to the President for Homeland Security, and asked him to administer the oath of office to those NSTAC Principals who were recently appointed to the Committee by President George W. Bush.

NSTAC Oath of Office.

General Gordon welcomed the NSTAC Principals to the Luncheon and congratulated them on their appointments to one of the Nation's most successful public–private partnerships. He noted that the NSTAC has the honor of being the Presidential advisory committee with the most recommendations acted upon by the President. General Gordon then called the following NSTAC Principals forward for the oath of office:

- Mr. Gary Forsee, Sprint Corporation;
- Mr. Richard Notebaert, Qwest Communications;
- Ms. Patricia Russo, Lucent Technologies;
- Mr. Stratton Sclavos, VeriSign, Inc.; and
- Mr. William Swanson, Raytheon Company.

General Gordon presented each NSTAC Principal with a certificate recognizing and honoring his/her participation on the NSTAC. He then introduced FCC Chairman Michael Powell and invited him to come forward to share with the Principals his views of the telecommunications environment and the FCC's recent activities related to national and homeland security.

Remarks, FCC Chairman Michael Powell.

Chairman Powell thanked the NSTAC for inviting him to participate in its annual meeting. He noted that the FCC and the NSTAC share the same desire and commitment to provide the American public with the most secure, competitive, and technologically advanced telecommunications system possible. He commented that when the NSTAC was created over 20 years ago, the Federal Government was concerned with the divestiture of AT&T and the long-lasting effects the break-up would have on national security. Since that time, the Nation's telecommunications network has evolved into one of the most innovative and advanced networks in the world and offers unprecedented choices for consumers. However, with new services and capabilities, interdependencies within and across the telecommunications network and other critical infrastructures continue to deepen, causing increased security risks. Over the last several years, the FCC has embraced and encouraged a new economic environment, which led to increased competition; however, it must also continue to focus on enhancing security across the network.

Chairman Powell stated that two issues—the converging telecommunications network and the complexity of the threat to the Nation—make securing the network ever more challenging. While the Cold War pitted the U.S. Federal Government against a definable enemy with a specific threat, the war on terrorism is far more diffuse, fragmented, and elusive, making the constantly morphing threat much harder to neutralize. Chairman Powell noted that the FCC has taken several steps to mitigate threats to the telecommunications infrastructure by striving to deeply integrate a homeland security focus into its daily operations and actively encouraging industry to do the same. Recently, the FCC revised its Strategic Plan, making homeland security (HLS) one of the six pillars of its operations. As such, each FCC bureau/office must integrate an HLS focus into its work with the goal of evaluating and strengthening the communications infrastructure and facilitating new thinking to assist in rapid restoration following an attack. In addition, the FCC created the HLS Policy Council, composed of senior managers from each of the bureaus, to raise HLS issues the FCC must address, and the Office of Homeland Security to act as a single conduit for other Government departments and agencies in their interactions with the FCC on HLS related topics.

Chairman Powell also outlined several initiatives the FCC has undertaken to keep pace with the changing technological and market environment.

In 2002, the FCC re-chartered its Network Reliability and Interoperability Council (NRIC) to address new threats to the homeland by significantly broadening both the focus and membership of the group to gain a more holistic view of network security. Membership in the group now includes representatives from the Internet service provider, wireless, and satellite communities. In early 2004, NRIC expanded its focus from primarily wireline issues to include wireless topics and appointed Mr. Timothy Donahue, President and Chief Executive Officer (CEO), Nextel, as the Chair of NRIC VII—the first time a CEO from the wireless sector has assumed that position. The NRIC VII goal of driving rapid growth of alternative communications issues directly reflects emerging trends in the industry. In addition to re-chartering the NRIC, the FCC created the Media Security and Reliability Council (MSRC) to better utilize and secure the Nation's media assets. As a result of the terrorist attacks on September 11, 2001, 22 of New York City's broadcasters lost broadcast facilities, which severely degraded service to the largest broadcasting market in the United States. The FCC will use the MSRC to study, develop, and report on best practices to ensure the reliability and security of multi-channel video facilities such as cable television.

Chairman Powell also noted several areas in which the FCC is working with other Federal partners to enhance Government-wide communications capabilities. Specifically, the FCC works with the National Communications System to make enhancements to the Wireless Priority Access System and the Telecommunications Service Priority System.

In addition, the FCC is also interacting with State regulatory agencies to set up a forum for examining interdependencies between the water, energy, and telecommunications sectors.

Moving forward, Chairman Powell commented that the Nation is turning the corner on digital migration, and very soon, emerging technologies such as wireless fidelity, broadband over power lines, cable to the home, and new applications such as voice over Internet protocol and streaming media will be commonplace. Currently, two percent of U.S. firms use Internet protocol (IP) telephony; however, by 2007, IP telephony usage is expected to reach 19 percent. According to a Yankee Group survey, 73 percent of wireline service providers and 31 percent of wireless service providers are either implementing or testing packet telephony technology. While these innovations will continue to bring enhancements and benefits to the American consumer, they will also increase the complexity of securing the infrastructure. As the Nation's telecommunications regulatory body, the FCC is embracing the realities of IP technology and must create a regulatory environment in which companies will flourish.

In closing, Chairman Powell stated that as the telecommunications networks continue to expand, so must the Nation's focus on security measures to protect them. Unlike the situation with circuit switched technology, the telecommunications industry has the opportunity to employ security mechanisms in the emerging technologies at the front end of implementation.

He encouraged all NSTAC member companies to embrace the evolving network realities and work to secure the networks as they continue to emerge.

Adjournment.

Dr. Coffman thanked Chairman Powell and the NSTAC Principals for their participation in the Executive Luncheon and welcomed the new members to the Committee. He reminded the Principals that they would be traveling to the White House imminently to meet with the President. Dr. Coffman adjourned the Luncheon at 1:10 p.m.

Attachment 1
Report Recommendations to the President from the 27th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVII) May 19, 2004

The President's National Security Telecommunications Advisory Committee (NSTAC) Satellite Task Force (STF) examined potential national security and emergency preparedness (NS/EP) issues related to satellites. Based on STF analysis and review of related policy issues, 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 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 satellite communications (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 National Communications System (NCS) to procure and manage the non-Department of Defense satellite facilities and services necessary to increase the robustness of Government communications.
- 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.

To guide rapid implementation of these recommendations with specific steps to secure the commercial SATCOM infrastructure for NS/EP, the task force provided the framework of an action plan for Federal departments and agencies.

To improve NS/EP policy, the task force suggested the establishment of a steering committee to examine how commercial SATCOM can best be used in an operational support role to the *National Response Plan*, study satellite technology export controls and their impact on the economic stability of the domestic satellite industry, and reevaluate domestic and foreign policies on the use of commercial SATCOM in support of NS/EP missions.

To increase the robustness of Government communications through better use of commercial SATCOM, the task force suggests the following actions: (1) maintain awareness of commercial SATCOM usage within the Federal Government, enabling decision makers to rapidly prioritize commercial satellite services required to support NS/EP needs; (2) extend the purview of the Telecommunications Service Priority to all fixed satellite service operators and extend the Wireless Priority Service model to mobile satellite operators; and (3) develop, in coordination with the commercial satellite industry, a strong and proactive information assurance policy to further reduce the vulnerability of command and control links.

Furthermore, the task force suggests actions to mitigate vulnerabilities in the SATCOM infrastructure. These suggestions include conducting studies on physical vulnerabilities, identifying a system-wide hierarchy of physical and cyber vulnerabilities to terrorist attack, developing a plan and process to rapidly mitigate interference, and developing security requirements commensurate with NS/EP communications needs.

The Financial Services Task Force (FSTF) 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—

- Support the Alliance for Telecommunications Industry Solutions' 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, and
  - The benefits and complexities of aggregating sector-wide 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.
- 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.

The Legislative and Regulatory Task Force (LRTF) 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,* and other existing authority, direct the appropriate departments and agencies, in coordination with industry, to:

- Develop a process to resolve multi-jurisdictional (Federal, State, and local) conflicts within the appropriate boundaries of federalism and national, homeland, and economic security.
- Work with Congress to modify the *Critical Infrastructure Information Act of 2002* (CII Act) so that the Department of Homeland Security (DHS) is the clearinghouse and dispenser of CII information.
- Encourage Congress to extend the protections of the CII Act to cover departments and agencies other than the 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.
- Work diligently with Congress to ensure the CII Act's *Freedom of Information Act* exemption and liability provisions remain intact.

The NSTAC's Operation, Administration, Maintenance, and Provisioning (OAM&P) Standards Working Group was formed to further examine the standard and develop conclusions and recommendations for further action. The OAM&P Standards Working Group made the following recommendations to the President:

- Direct the National Institute of Standards and Technology (NIST) to review the T1.276-2003 standard. If a review finds a conflict between the T1.276-2003 standard and existing Federal Information Processing Standards (FIPS) and NIST publications, NIST should make these conflicts known to the appropriate standards bodies.

- Encourage Federal departments and agencies to use the T1.276-2003 standard in requests for proposals, as appropriate.

- Encourage other infrastructures through the Department of Homeland Security to consider the elements of the T1.276-2003 standard as a baseline for security requirements and adapt appropriate requirements for their respective infrastructure.

Attachment 2
Attendance of Members at the 27th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XXVII) May 19, 2004

Dr. Vance D. Coffman, Chair	Lockheed Martin Corporation
Mr. F. Duane Ackerman, Vice Chair	BellSouth Corporation
Dr. J. Robert Beyster	Science Applications International Corporation
Mr. Gregory Brown*	Motorola, Inc.
Mr. Gary Forsee	Sprint Corporation
Mr. Van B. Honeycutt	Computer Sciences Corporation
Mr. Clayton M. Jones	Rockwell Collins, Inc.
Mr. Craig O. McCaw	Teledesic Corporation
Mr. Craig 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
Dr. Hector de J. Ruiz	Advanced Micro Devices, Inc.
Ms. Patricia F. Russo	Lucent Technologies

* Membership pending White House approval (as of May 19, 2004).

Mr. Stratton Sclavos	VeriSign, Inc.
Mr. Stanley Sigman*	Cellular Telecommunications & Internet Association
Mr. William Swanson	Raytheon Company
Mr. Lawrence A. Weinbach	Unisys

* Membership pending White House approval (as of May 19, 2004).

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 Administration

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 for Telecommunications

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

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-..... Telecommunications

ISAC..... Information Sharing and Analysis Center

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