The President's National Security Telecommunications Advisory Committee

May 2000

ISSUE REVIEW

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

Issue Review

A review of NSTAC issues addressed through
NSTAC XXIII

May 2000

PREFACE

PREFACE

The President's National Security Telecommunications Advisory Committee

Executive Order (E.O.) 12382 mandated formation of the National Security Telecommunications Advisory Committee (NSTAC) on September 13, 1982, to provide the President with a unique source of national security and emergency preparedness (NS/EP) telecommunications policy expertise. For 18 years, the NSTAC has advised the President on issues pertaining to the reliability and security of telecommunications and the information infrastructure—issues that are critical to America's security and commercial interests. Today, the NSTAC is recognized 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 telecommunications and related information systems posture. Enhancements in the form of operational programs and policy solutions benefit both industry and Government as the security requirements for the telecommunications infrastructure evolve.

Composed of up to 30 presidentially appointed senior executives, the NSTAC has representatives from the telecommunications, information services, electronics, aerospace, and banking industries. Mr. Van B. Honeycutt, Chairman, President, and Chief Executive Officer (CEO) of Computer Sciences Corporation, is the NSTAC Chair. Chair positions rotate within the membership about every 2 years. Appendix A provides a list of current NSTAC members.

Four factors provided impetus for the establishment of the NSTAC:

1. the divestiture of AT&T and the resulting loss of a single point of contact within industry to satisfy Government NS/EP telecommunications requirements,
2. increased Government reliance on commercial communications,
3. the potential impact of new technologies on telecommunications supporting NS/EP requirements, and
4. the growing importance of command, control, and communications to military and disaster response modernization.

In addition to the NSTAC, others assisting the President on NS/EP telecommunications matters are the Vice President; the Assistant to the President for National Security Affairs; the Secretary of Defense (also designated as the Executive Agent, National Communications System [NCS]); the Assistant to the President for Science and Technology; the Director, Office of Management and Budget; and the NSTAC's Designated Federal Official, who is the Manager, NCS.

During the past 18 years, the President's NSTAC has worked cooperatively with the NCS, an interagency consortium of Federal departments and agencies that serves as the focal point for industry/Government NS/EP telecommunications planning. Originally created in 1963 as a result of inadequacies in command, control, and communications during the Cuban Missile Crisis, the NCS underwent a fundamental change in 1984 when President Ronald Reagan signed E.O. 12472. E.O. 12472 established a new and broader organizational structure for the NCS, expanding its membership to include all Government entities with significant telecommunications assets—currently 22 Government organizations.

Today, the NCS' charge is to coordinate the planning of NS/EP communications to support any crisis or disaster. The NCS Committee of Principals (COP) and its subordinate Council of Representatives (COR) represent each NCS member organization. The NCS COP and COR provide advice and recommendations on NS/EP telecommunications and participate in industry and Government planning and NSTAC-related activities through the Office of the Manager, NCS (OMNCS). The OMNCS provides technical and executive assistance to the President's NSTAC and its subordinate groups, as well as to the NCS COP and COR.

The principal 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, or recommendations for presentation to the NSTAC. When the IES identifies an issue that requires further examination, the subcommittee forms a working group or task force to address it.

The IES convened a special offsite meeting in August 1999 to identify and prioritize issues, to reorganize its subgroup structure to best address those issues, and to optimize the process by which its subgroups conduct business. Specifically, the meeting resulted in a new structure which is described below.

- The Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF) develops recommendations to facilitate further progress toward goals laid out in Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection.*

- The Globalization Task Force (GTF) addresses the NS/EP telecommunications implications of emerging globalization trends.

- The Information Technology Progress Impact Task Force (ITPITF) is analyzing the NS/EP implications of Internet Protocol–public switched network convergence.

- The Protecting Systems Task Force (PSTF) is developing recommendations to assist the Government in focusing efforts to enhance the security of the Nation's telecommunications and information technology systems that support NS/EP activities.

- The IES activates the Legislative and Regulatory Working Group (LRWG) when a task force requires further examination of legal and regulatory aspects of a current issue.

Many NSTAC recommendations result in operational activities that enhance NS/EP telecommunications and information systems. For example, the National Coordinating Center for Telecommunications, an industry and Government coordination center for day-to-day operational support to NS/EP telecommunications, began as an NSTAC recommendation. 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 telecommunications services for Federal, State, and local government users, as well as nongovernmental users. Also originating from NSTAC activities, separate NSTAC and Government Network Security Information Exchanges (NSIE) have been created and meet regularly to address the threat of electronic intrusions and software vulnerabilities, as well as mitigation strategies to protect the Nation’s critical telecommunications and information systems.

Appendix B contains the NSTAC XXII Executive Report to the President, a summary of the most recent NSTAC meeting and recommendations. Copies of NSTAC reports pertaining to the issues addressed in this document are available through the Office of the Manager, National Communications System, Customer Service Division, 701 S. Courthouse Road, Arlington, Virginia 22204-2198. The telephone number is (703) 607-6211.

TABLE OF CONTENTS

TABLE OF CONTENTS

PAGE

TABLE OF CONTENTS
(Continued)

PAGE

APPENDICES

INTRODUCTION

INTRODUCTION

PURPOSE

This edition of the *Issue Review* provides a status report of issues addressed by the President's National Security Telecommunications Advisory Committee (NSTAC) from its first meeting in December 1982 until the May 15-16, 2000, meeting of the NSTAC. The *Issue Review* documents the history of issues currently and previously addressed by the NSTAC. For each issue, 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, recent and planned activities to further address the issue, actions resulting from NSTAC recommendations, members of the current investigating groups, and reports issued. Appendix C provides related acronyms for the reader's convenience.

ACTIVE ISSUES

NSTAC Task Forces addressed issues in the following areas:

- Information Assurance/Infrastructure Protection
- Network Security
- Legislation and Regulation
- Industry/Government Information Sharing and Response
- Globalization

PREVIOUSLY ADDRESSED ISSUES

Since its first meeting on December 14, 1982, the NSTAC has addressed a wide range of national security and emergency preparedness telecommunications issues. The committee's findings have provided the Government with industry-based expertise and advice on telecommunications and information systems plans and policies. The *Issue Review* records the contributions that industry and Government representatives have made to ensure the security and the emergency response capability of the Nation's telecommunications 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

INFORMATION ASSURANCE/ INFRASTRUCTURE PROTECTION

Investigation Groups:
Information Assurance Task Force (IATF);
Information Infrastructure Group (IIG);
Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF)

Periods of Activity:
IATF: May 15, 1995–April 22, 1997
IIG: April 22, 1997–September 23, 1999
IS/CIPTF: September 23, 1999–Present

Issue Background: At NSTAC XVII, the Director of the National Security Agency (NSA) 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 Information Assurance/Critical Infrastructure Protection (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.

Following a reevaluation of NSTAC subgroups in September 1999, the IES created the IS/CIPTF to address information sharing issues associated with 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.

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 (R&D) 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 national security and emergency preparedness (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 possibilities for industry and Government participation on mutually beneficial projects were discussed. These efforts ultimately resulted in DOJ's Cyber Citizen program.

Building on past NSTAC efforts in addressing IA and infrastructure protection issues, the IIG continued to coordinate with Federal officials responsible for PDD-63 implementation during the NSTAC XXII cycle. Specifically, in accord 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 (NCC) 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.

Recent and Planned Information Assurance/Infrastructure Protection Activities: During the NSTAC XXIII cycle, the IS/CIPTF assumed responsibility for NSTAC's examination of CIP issues. The task force focused on infrastructure protection initiatives at the national and cross-sector level through outreach efforts with Government representatives responsible for PDD-63 implementation.

Building on work conducted by the IIG during the NSTAC XXII cycle, the IS/CIPTF continued to provide input to the Director, Critical Infrastructure Assurance Office (CIAO) on the *National Plan for Information Systems Protection (Version 1.0)*. The plan is the first major element of a more comprehensive effort by the Administration 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 constructively shape the plan. In its report to NSTAC XXIII, the IS/CIPTF provided NSTAC recommended input to the plan regarding the NCC ISAC. The task force anticipates that this dialogue will continue as the Government, working with industry, drafts subsequent versions of the plan.

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. Industry and Government envisioned the Partnership to provide a forum for representatives of the critical infrastructures to exchange views on interdependencies, threats, workforce developments, standards and best practices, technology and R&D, risk management, international matters, legal and regulatory matters, and other areas of mutual concern. The Partnership also serves to facilitate industry participation in the national process to address CIP. Through individual NSTAC member company participation, NSTAC expertise, successes, lessons learned, and experiences were shared to further facilitate the development of the Partnership in support of PDD-63 objectives.

The IS/CIPTF concluded that efforts by industry and Government departments and agencies to promote outreach and awareness across the critical infrastructures, with an emphasis on the information and communications sector, should be continued. Specifically, in its May 2000 report to NSTAC XXIII, the IS/CIPTF recommended that the NSTAC XXIV workplan include the following tasks:

- Continue outreach efforts to support implementation of PDD-63 related initiatives

- Continue to actively engage in a dialogue with the Federal Government to provide telecommunications industry input to subsequent versions of the *National Plan for Information Systems Protection*

Reports Issued:

- *Information Assurance Task Force Report,* March 1997.
- *Electric Power Information Assurance Risk Assessment Report,* March 1997.
- *Information Infrastructure Group Report,* December 1997.
- *Financial Services Risk Assessment Report,* December 1997.
- *Interim Transportation Information Risk Assessment Report,* December 1997.
- *Cyber Crime Point Paper,* December 1997.
- *Information Infrastructure Group Report,* September 1998.
- *Cyber Security Training and Forensics Issue Paper,* September 1998.

- *Information Infrastructure Group Report,* June 1999.
- *Transportation Information Infrastructure Risk Assessment Report,* June 1999.
- *Report on NS/EP Implications of Electronic Commerce,* June 1999.
- *Information Sharing/Critical Infrastructure Protection Task Force Report,* May 2000.

Information Sharing/Critical Infrastructure Protection Task Force Membership:

Chair:	Mr. Lowell Thomas, GTE
Vice Chair:	Mr. Hank Kluepfel, SAIC

AT&T	Mr. Gordy Bendick
Boeing	Mr. Bob Steele
Cisco Systems	Mr. Ken Watson
COMSAT	Mr. Ernie Wallace
CSC	Mr. Guy Copeland
EDS	Mr. Bob Donahue
ITT	Mr. Joe Gancie
Lockheed Martin	Mr. Mike Collins
Nortel Networks	Dr. Jack Edwards
NTA	Mr. Bob Burns
Raytheon	Mr. Bob Tolhurst
Rockwell	Mr. Ken Kato
TRW	Mr. Bill Gravell
USTA	Mr. Paul Johnson
U S WEST	Mr. Jon Lofstedt

Information Sharing/Critical Infrastructure Protection Task Force Participants:

AT&T	Mr. Harry Underhill
CSC	Ms. Sheila Andahazy
GTE	Ms. Ernie Gormsen
COMSAT	Dr. Jack Oslund
OMNCS	Mr. Bernie Farrell
Unisys	Dr. Dan Wiener

NETWORK SECURITY

Investigation Groups:
Network Security Task Force (NSTF); Network Security Information Exchange (NSIE); Network Security Standards Oversight Group (NSSOG); Network Security Steering Committee (NSSC); Network Security Group (NSG); Network Group (NG); Embedded Interoperable Security Issue Scoping Group (EISISG); Information Technology Progress Impact Task Force (ITPITF); Protecting Systems Task Force (PSTF).

Periods of Activity:
NSTF: February 21, 1990–August 26, 1992
NSIE: June 25, 1991–Present
NSSOG: August 26, 1992–January 12, 1995
NSSC: August 26, 1992–December 1994
NSG: December 1994–April 22, 1997
NG: April 22, 1997–September 23, 1999
EISISG: June 1999–November 1999
ITPITF: September 23, 1999–Present
PSTF: September 23, 1999–Present

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Also in September 1996, the NSG sponsored the Network Security Research and Development (R&D) Exchange. The event's purpose was to analyze R&D activities ongoing in both the public and private sectors and to address issues of authentication, intrusion detection, and access control from the capabilities management perspective.

In November 1996, the NSG organized the Forward-Looking Analysis Panel to consider the impact of the Telecommunications Act of 1996 on network security and NS/EP telecommunications services. The panel addressed issues such as carrier interconnection, collocation, and open network architecture. The Federal Communications Commission's (FCC) Network Reliability and Interoperability Council (NRIC) considered the panel's input and subsequently included it in the NRIC's final report.

At the March 18, 1997, NSTAC XIX meeting, the NSG reported on its work to address the impact of the changing regulatory and technological environment on NS/EP telecommunications services. The NSG also reviewed its recent activities in the areas of R&D, intrusion detection, and forward-looking network control security analysis. At the meeting, the NSG outlined the efforts of the newly established Intrusion Detection Subgroup (IDSG) and its charge to explore a more cooperative approach to developing enhanced intrusion detection tools. The NSG concluded by addressing the activities of the NSIEs and noted that the NSTAC NSIE expanded its membership from 9 to 20.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

As the IDSG focused primarily on R&D issues related to intrusion detection technology, the Government was exploring broader R&D issues. In particular, the President’s

Commission on Critical Infrastructure Protection (PCCIP) examined R&D issues affecting the security of all critical infrastructures. NSTAC's findings and recommendations are consistent with those resulting from the PCCIP's work. Further, Presidential Decision Directive (PDD) 63 assigned the Office of Science and Technology Policy (OSTP) responsibility for coordinating R&D agendas and programs for the Government through the National Science and Technology Council.

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

Following NSTAC XXI, the Government took measures to make critical Government systems Y2K compliant and to develop contingency plans to deal with any potential system failures that might occur. NSTAC's *Year 2000 Problem Status Report,* issued in September 1998, influenced the President's Council on Year 2000 Conversion on the need to develop comprehensive contingency plans to mitigate any potential harmful effects on the Nation's NS/EP posture.

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

Recent and Planned Network Security Activities: Following NSTAC XXII in June 1999, the IES identified the following network security tasks:

- Identify how the progress of information technology may affect the Government process, particularly as it relates to NS/EP issues
- Prepare for an R&D Exchange Symposium
- Develop recommendations for the President regarding how the Government can optimally focus its efforts to enhance the security of the Nation's NS/EP telecommunications and information technology systems
- Scope the issue of embedding security in depth in the infrastructure

The IES subsequently formed two task forces to address the first three tasks. The IES created the ITPITF to address the first two tasks and the PSTF to address the third task. The IES formed a scoping group to address the last task.

The ITPITF's primary objective was to examine the potential implications of IP network and PSN convergence on existing NS/EP services (e.g., GETS and TSP). The ITPITF analyzed issues related to GETS functionality in IP networks, relying in part on information from the GETS Program Management Office (PMO). 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. In relation, the ITPITF concluded that as the Next Generation Network (NGN) evolves, telecommunications carriers' SS7 networks will become less discrete and more reliant on IP technology and interfaces. Therefore, it will be necessary to consider the security, reliability, and availability of the NGN control space as it relates to the provision and maintenance of NS/EP service capabilities.

In addition, the ITPITF analyzed potential implications of convergence on TSP services, relying partly on information from the TSP Oversight Committee (OC). The ITPITF concurred with the OC 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 IES consider including an examination of the potential NS/EP implications related to possible security and reliability vulnerabilities of the control space in the NGN in the NSTAC XXIV work plan.

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

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

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

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

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

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

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

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

The NG incorporated these and other issues into the program for the fourth R&D Exchange in September 2000.

Reports Issued:

- *Network Security Scoping Task Force Report: Report of the Network Security Task Force,* October 1990.
- *Network Security Task Force Final Report,* July 1992.
- *NSTAC/NSIE Report on Deficiencies in Federal Laws on Computer Crime,* April/May 1993.
- *Network Security Standards for the Public Switched Network: Issues and Recommendations,* October 1994.
- *An Assessment of the Risk to the Security of Public Networks, Government and NSTAC NSIEs,* December 12, 1995.
- *Report of the Network Security Group Research and Development Exchange,* September 18, 1996.
- *Network Security Group Forward Looking Analysis Panel Proceedings,* November 19, 1996.
- *Local Number Portability and Its Implications for the Public Switched Network: An NSIE White Paper,* July 1997.
- *Software Integrity: An NSIE White Paper,* July 1997.
- *Report on the Likelihood of a Widespread Telecommunications Outage,* December 1997.

- *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development,* December 1997.
- *The Insider Threat: Legal and Practical Human Resources Issues: An NSIE White Paper,* April 1998.
- *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment: An NSIE White Paper,* June 1998.
- *The President's NSTAC Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration,* October 1998.
- *An Assessment of the Risk to the Security of the Public Network,* April 1999.
- *Network Group Internet Report: An Examination of the NS/EP Implications of Internet Technologies,* June 1999.
- *Protecting Systems Task Force Report on Enhancing the Nation's Network Security Efforts,* May 2000.
- *Information Technology Progress Impact Task Force Report on Convergence,* May 2000.

Information Technology Progress Impact Task Force Membership:

Chair:	Dr. Jack Edwards, Nortel Networks
Vice Chair:	Mr. Jim Massa, Cisco Systems
AT&T	Mr. Paul Waldner
Boeing	Mr. Bob Steele
COMSAT	Mr. Jack Oslund
CSC	Mr. Guy Copeland
GTE	Mr. James Bean
ITT	Mr. Joe Gancie
Lockheed Martin	Dr. Chris Feudo
MCI WorldCom	Mr. Mike McPadden
Raytheon	Mr. John Grimes
SAIC	Mr. Hank Kluepfel
USTA	Dr. Vern Junkmann

Protecting Systems Task Force Membership:

Chair:	Mr. Ken Watson, Cisco Systems
Vice Chair:	Mr. Bob Burns, NTA
AT&T	Mr. Paul Waldner
Boeing	Mr. Bob Steele
CSC	Mr. Guy Copeland
EDS	Mr. Randy Jensen
GTE	Mr. James Bean
ITT	Mr. Dave Kelly
Lockheed Martin	Dr. Chris Feudo
MCI WorldCom	Mr. Mike McPadden
Nortel Networks	Dr. Jack Edwards
Raytheon	Mr. Thomas O'Connell
SAIC	Mr. Nelson Williams, Jr.
U S WEST	Mr. Jon Lofstedt

LEGISLATION AND REGULATION

Investigation Group:
Funding and Regulatory Working Group (FRWG)
Legislative and Regulatory Group (LRG)
Legislative and Regulatory Working Group (LRWG)

Period of Activity:
FRWG: December 14, 1982–December 1994
LRG: December 1994–September 23, 1999
LRWG: September 23, 1999–Present

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 (FNI) 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 (see the Previously Addressed Issues section of this *Issue Review* for detailed information on these issues). The 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 landmark Telecommunications Act of 1996. The NSTAC's Industry Executive Subcommittee (IES) reconstituted the LRG as the LRWG following the IES reorganization in September 1999. The IES established the LRWG as a permanent working group, which receives taskings from the IES when task forces require clarification or analysis on legislative or regulatory matters affecting a specific issue.

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

In its charge to the LRG, the IES placed particular emphasis on monitoring implementation of the Telecom Act. In addressing this charge, the group established a framework for analysis, and in January 1997, began working closely with industry and Government to develop a common understanding of the NS/EP implications of the new law.

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

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

In response to this finding, the IES charged the LRG to examine options for enhancing communication on NS/EP matters among industry, the 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 (NCS), 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 outlines 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). 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.

Recent and Planned Activities:
Following the June 1999 NSTAC XXII meeting, the LRWG examined impediments to information exchange, especially critical infrastructure information sharing. The group undertook an in-depth analysis of the Freedom of Information Act (FOIA), specifically examining FOIA's potential to hinder information exchange between industry and Government. In accordance with FOIA, the public may request and gain access to records maintained by Government departments and agencies. For various reasons, such potential disclosure of data may be a deterrent to industry's sharing of information with the Government. Although there are a number of exemptions to FOIA's requirement for disclosure of information, none of the exemptions clearly cover information pertaining to critical infrastructure protection. To address this issue, 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 that is voluntarily shared with the Government. The LRWG shared its analysis with the NSTAC's Information Sharing/Critical Infrastructure Protection Task Force (IS/CIPTF), which addressed the issue in its May 2000 report to NSTAC XXIII.

In addition to FOIA, the DOJ is examining antitrust and liability issues as impediments to information sharing between industry and Government. The LRWG will continue dialogue with the DOJ to exchange ideas and findings related to antitrust and liability impediments and their impacts to critical infrastructure protection.

During the NSTAC XXIII cycle, the LRWG also examined foreign ownership regulations and their impact on NS/EP. The group 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 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.

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.

Legislative and Regulatory Working Group Membership:

Chair:	Dr. Jack Oslund, COMSAT
Vice Chair:	Mr. Joe Gancie, ITT

AT&T	Mr. Gordy Bendick
CSC	Mr. Guy Copeland
Cisco Systems	Mr. Jim Massa
GTE	Mr. Lowell Thomas
Hughes	Ms. Jennifer Smolker
Lockheed Martin	Mr. Michael Collins
MCI WorldCom	Mr. Cliff Greenblatt
NTA	Mr. Bob Burns
Rockwell	Mr. Ken Kato
SAIC	Mr. Hank Kluepfel
Unisys	Dr. Dan Wiener
USTA	Mr. Paul Johnson

Legislative and Regulatory Working Group Participants:

AT&T	Mr. Harry Underhill
COMSAT	Mr. Ernie Wallace
EDS	Mr. Randy Jensen
GTE	Ms. Ernie Gormsen
Telcordia Technologies	Ms. Louise Tucker

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)

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–Present

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 (see the Previously Addressed Issues section of this *Issue Review* for detailed information). 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 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 PN 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 roll-over period translated into functions to be performed as ISAC (in accordance with PDD-63). In addition the OSG continued to monitor enhancements to the NCC that ensured an electronic 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 10 NCC chartered functions and updated the *NCC Operating Guidelines* (both written in 1984) for the current operational environment. The subgroup also determined that an electronic intrusion incident information processing function could be integrated into the NCC's activities. In August 1997, the subgroup held an industry/Government tabletop exercise to test the draft concept of operations for NCC intrusion incident information processing. The OSG documented the subgroup's activities and accomplishments in the OSG's report to the December 11, 1997, NSTAC XX meeting.

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

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

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

In 1998, the NCC modified its standard operating procedures to accommodate an electronic intrusion incident information processing capability. With the OSG's support and assistance, the NCC began its intrusion incident information processing pilot on June 15, 1998. The NCC Vision-Operations Subgroup worked closely with the 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 (IIG) 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.

Recent and Planned Activities: The IS/CIPTF, working with the NCC, continued to examine the role the NCC plays in the PDD-63 information sharing context. In considering information sharing, the IS/CIPTF identified three areas on which to focus. The task force examined information sharing at the national level, the cross-sector level, and the telecommunications-sector level. The Information Assurance/Infrastructure Protection portion of the Active Issues section of this document discusses the IS/CIPTF examination of information sharing at the national and cross-sector levels. This section focuses on task force efforts to examine operational information sharing conducted by the telecommunications sector.

The IES tasked 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. To accomplish this, the task force examined the historical experiences of the NCC to determine how and what information is shared and the utility of information sharing for industry and Government. The task force also identified benefits that can be derived from information sharing by both industry and Government.

The IS/CIPTF recognized that the NCC ISAC is evolving. External relationships and organizational structures and processes will be addressed to ensure that participants receive benefits from information sharing. As a result, in its report to NSTAC XXIII, the task force recommended that the IES consider including in the NSTAC XXIV work plan the following task:

- Continue to observe and collaborate in the development of the NCC ISAC function and make appropriate recommendations

In addition, the IS/CIPTF 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. Finally, the IS/CIPTF examined the NCC's Y2K experiences for lessons learned that could benefit infrastructure protection efforts. 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 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

In addition, the IS/CIPTF concluded that lessons learned from Y2K do not universally apply to CIP, potentially making it more difficult to rapidly achieve CIP information sharing at the levels achieved during the Y2K effort.

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

*Consult page 6 to see the Information Sharing/Critical Infrastructure Protection Task Force membership list.

GLOBALIZATION

Investigation Groups:
National Information Infrastructure Task Force (NII), 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–Present

Issue Background: In 1993, the NSTAC established a National Information Infrastructure (NII) Task Force and charged it with examining the implications of the evolving U.S. information infrastructure for national security and emergency preparedness (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 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.

Recent and Planned Globalization Activities: 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 (QoS) 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

Globalization Task Force Membership:

Chair:	Mr. Bob Donahue, EDS
Vice Chair:	Mr. Ernie Wallace, COMSAT
AT&T	Mr. Paul Waldner
Boeing	Mr. Bob Steele
Cisco Systems	Mr. Art Mackin
CSC	Mr. Guy Copeland
EDS	Mr. Dale Fincke
GTE	Mr. Lowell Thomas
ITT	Mr. Joe Gancie
MCI WorldCom	Mr. Mike McPadden
Nortel Networks	Dr. Jack Edwards
Raytheon	Mr. John Grimes
SAIC	Mr. Bob Rankin

PREVIOUSLY ADDRESSED ISSUES

PREVIOUSLY ADDRESSED ISSUES

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 national security and emergency preparedness (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 (R&D) focus areas, pilot/demonstration projects, and civil/military telecommunications issues identified by OSTP and the National Economic Council (NEC)

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 (FCC) 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 (IITF) 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.

An *NII Task Force Status Report* was presented 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 (PDD) 63, *Critical Infrastructure Protection.* Specifically, in an approach consistent with the NSTAC's ISSB recommendation, the Administration's Critical Infrastructure Assurance Office has 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.

WIRELESS SERVICES

Investigation Groups:
Wireless/Low-Bit-Rate Digital Services Task Force (W/LBRDSTF)
Wireless Services Task Force (WSTF)

Periods of Activity:
W/LBRDSTF: March 15, 1991–October 1991
WSTF: December 11, 1991–September 22, 1995

Issue Background: At the March 15, 1991, meeting, the IES established the W/LBRDS Task Force. The IES established the task force 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 (PSN) 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 NS/EP users.

On October 3, 1991, in its final report to NSTAC XIII, the W/LBRDS Task Force 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, Government tasked the OMNCS Wireless

Services Program Office (WSPO) with the responsibility.

In December 1991, following the Government's action in establishing the WSPO, the IES approved the establishment of a follow-on 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 (FWUF), 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 the September 22, 1995, IES meeting, the WSTF was placed 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 monitors the development and modifications of standards and regulatory issues relevant to CPAS.

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 NSTAC XVII, held on January 12, 1995, the task force reported on its activities in the areas of wireless interoperability and cellular priority access.

At NSTAC XVIII, 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.

Actions Resulting from NSTAC Recommendations: A Memorandum of Understanding (MOU) established the WSPO as the Government focal point within the OMNCS, Technology and Standards Division (N6), 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.

On April 18, 1996, the FCC published a CPAS Public Notice, soliciting comments from industry on the CPAS Petition for Rulemaking. As of October 1996, the FCC had received all Comments and Reply Comments on the Public Notice.

The OMNCS worked on CPAS implementation through four parallel approaches: modified cellular standards to incorporate CPAS, encouraged the FCC to issue CPAS rules, developed CPAS administrative processes, and stimulated competitive interests of service providers to implement the CPAS capability.

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.

COMMON CHANNEL SIGNALING

Investigation Groups:
Common Channel Signaling (CCS) Task Force; National Security and Emergency Preparedness (NS/EP) Panel

Periods of Activity:
CCS Task Force: April 28, 1993–January 31, 1994
NS/EP Panel: March 1994–March 1995

Issue Background: At the April 28, 1993, IES meeting, the Operations Working Group (OWG) 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 (PSN) and NS/EP telecommunications. The IES established the CCS Task Force to:

- Determine if there were failure mechanisms that could potentially lead to widespread, long-duration CCS outages among multiple interconnected carriers

- Evaluate the risk to NS/EP user telecommunications

- If significant risk existed, examine procedural or technological alternatives for mitigating it

- 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 (NSIE) 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 that the task force be deactivated 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 (NOF) 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 need for standardized guidelines in requesting the protection of critical telecommunications facilities was identified during the April 1992 civil disturbance in Los Angeles. 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 (DOD) representatives briefed the panel on the roles of the DOJ, the National Guard, and active duty military personnel during national emergencies.

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

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

In an October 1996 conference call, participants of the industry/Government exercise discussed options for clarifying the federalization issues. The NS/EP Panel added new language to the document, indicating that both federalized and non-federalized National Guard troops, each with different chains of command, may participate in restoring and maintaining law and order. In addition, the panel added a section authorizing the Secretary of Defense to determine when Federal military forces should withdraw from the disturbance area and when National Guard units would return to State control.

Reports Issued:

- *Guidelines for Obtaining Protection of Critical Telecommunications Facilities During Civil Disturbances*, May 1994.
- *Protection of Critical Facilities Exercise, After-Action Report*, December 1995.

ENERGY

Investigation Groups:
Energy Task Force; NS/EP Panel

Periods of Activity:
Energy Task Force: August 31, 1988–March 29, 1990
Energy Task Force: October 3, 1991–May 27, 1993
NS/EP Panel: March 8, 1994–October 5, 1994

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

The 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 [CFR] Part 280)
- Ensure that NS/EP telecommunications users who need electric power to operate their customer premises equipment (CPE) have a backup power capability that can operate through at least a 7-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 first Energy Task Force was formed. 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 (TSP) 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 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 which 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 had indicated their desire to voluntarily participate in the TESP initiative; and additional States were expected to follow.

At the October 13, 1994, OWG-PWG meeting, DOE explained that its ESP program in support of telecommunications had replaced the TESP initiative. 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:
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 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 an ECC Task Force be established to determine how existing and evolving technologies could best be exploited to enhance the priority access, transport, and egress of NS/EP traffic. The FRWG's study also stated that the proposed task force should evaluate the *Intelligent Networks Task Force Final Report* and recommendations, and coordinate its efforts with those of the OMNCS to avoid duplication.

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

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

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

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

At the August 2, 1993, IES meeting, members approved the deactivation of the ECC Ad Hoc Group, which had completed its work. The group had served as a forum for issues such as cellular priority access, preferential access for North Atlantic Treaty Organization (NATO) countries, and future broadband services. It assisted the Government in its effort to obtain approval of the HPC standard, which was published as American National Standards Institute (ANSI) 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 (NLP) initiatives, the group assisted the Government in developing educational materials such as the *ECC Services Cost/Benefit Analysis Report*, and the 1993 *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 Office of the Manager, National Communications System (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 (ECSA) 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:
IES Funding and Regulatory Working Group (FRWG)

Period of Activity:
April 12, 1990–March 1, 1991

Issue Background: In 1988, the Energy Task Force was concerned 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 CFR 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 had modified or replaced several thousand underground storage tanks (UST) pursuant to these regulations and had 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 (PSN) 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 (LEC) and interexchange carriers (IC) 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 IES Plans Working Group

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 has 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, Plans Working Group (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, 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 SYSTEMSSURVIVABILITY

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 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 (EMP) Task Forces, and submitted them to the NSTAC on November 6, 1987. The task force submitted similar reports on automated information processing (AIP) and the National Coordinating Mechanism (NCM) to NSTAC IX on September 22, 1988. The NSTAC approved these reports and forwarded them to the President on the respective dates. The TSS Task Force also completed an assessment of the applicability of network management technology to NS/EP telecommunications survivability, which the NSTAC forwarded to the President on September 22, 1988. The TSS Task Force assisted the OMNCS in developing the Federal Government's policy on essential line service (ELS).

On June 8, 1989, the NSTAC approved the TSS Task Force's final report and disbanded the task force. The NSTAC also directed the IES to proceed with the study of intelligent networks and virtual networks usefulness for enhancing network survivability, which the TSS Task Force initiated, pending review of the issue by the IES 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 (LEC) 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 (DOE) 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 IES established the TSP Task Force on February 21, 1985, to advise and assist the OMNCS in developing the TSP System, specifically regarding provisioning, restoration, maintenance, legal, and regulatory issues.

History of NSTAC Actions and Recommendations: The task force worked closely with the OMNCS in the development of the TSP System and provided assistance with its implementation. Specifically, the task force had a significant advisory role in creating the *Petition for Rulemaking and Proposed FCC Rules* for the TSP System. The task force also assisted the TSP Program Office in establishing the initial TSP System Oversight Committee charter. The NCS Council of Representatives (COR) TSP Subcommittee and the TSP task force drafted and approved the charter in February 1990, and the Department of Defense (DOD) and the General Services Administration (GSA) approved the charter in November 1990. Subsequently, an amendment was adopted 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 (DOT), Federal Emergency Management Association (FEMA), DOD, GSA, Department of Energy (DOE), Department of Commerce (DOC), National Telecommunications and Information Administration (NTIA), and the Federal Communications Commission (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, which was 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 the NCS Directive 3-1, which clarified the responsibilities of and procedures for all TSP System entities. The task force also assisted in the development of the *TSP Service User Manual*, which provided a set of guidelines for all users of the TSP System.

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

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

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

Reports Issued:
- TSP Information Guide, December 1989 *(published for the TSP Task Force by USTA).*
- TSP Service Vendor Handbook (NCSH 3-1-2), July 1990.
- Final Report of the Telecommunications Service Priority (TSP) Task Force, September 1990.

TELECOMMUNICATIONS SERVICE PRIORITY CARRIER LIABILITY

Investigation Group:
IES Funding and Regulatory Working Group (FRWG)

Period of Activity:
November 16, 1990–January 31, 1991

Issue Background: The FCC *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 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

Investigation Group:
IES Plans Working Group (PWG)

Period of Activity:
December 13, 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 had resurfaced in the National Research Council (NRC) 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 OMNCS to address this issue. The IES subsequently assigned the Plans Working Group (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 NCC industry representatives on physical security policy, operational procedures, and methods. The study also documented past NSTAC task force and OMNCS efforts regarding physical security of NS/EP telecommunications facilities, sites, and assets and relevant conclusions and recommendations of those past efforts. The study concluded that current industry/Government activity and past NSTAC and OMNCS documents demonstrated industry and Government 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 no further NSTAC review was needed 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 Task Force

Period of Activity:
August 1989–October 1991

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

NSTAC XI extended the activities of the Intelligent Networks Task Force until NSTAC XII, December 13, 1990. To meet its charge, the task force worked with the OMNCS to derive a set of desired NS/EP user features and compared them with intelligent network services. The task force determined the advantages and disadvantages of identified intelligent network services for NS/EP telecommunications, including interoperability considerations. The IES extended the Intelligent Networks 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 Intelligent Networks 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 intelligent networks in response to the IES charge to evaluate and refine the conclusions and recommendations of the *Intelligent Networks Task Force Final Report*. NSTAC XIII directed the IES to disband the Intelligent Networks 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 Intelligent Networks 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 5-year AIN NS/EP contract to Bellcore to provide a mechanism for collecting Intelligent Networks (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 Intelligent Networks Task Force Final Report: The Impact of Intelligent Networks on NS/EP Telecommunications*, November 7, 1990.
- *The Industry Executive Subcommittee: Executive Report on Intelligent Networks*, 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: June 1989, the NSTAC noted that the NRC report, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness*, differed from Telecommunications Systems Survivability (TSS) Task Force findings. The NSTAC, therefore, charged the IES with examining those differences and reporting back in early 1990. In response, the IES formed the NRC Report Task Force and issued the following charges:

- If it agreed with the NRC report, address what actions should be taken by industry to assist the Government in implementing the NRC's recommendations
- If it did not agree, give the reasons why and the factors bearing on the differing perspectives of the IES and the NRC
- 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 public switched network (PSN) was growing more survivable. This survivability stems from the increased network diversity provided by the existence of three major interexchange carriers (IC), 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 to 11, 1993, in Washington, DC on industry's best practices for avoiding and minimizing the risk and impact of future telephone network outages.

Report Issued:

- *National Research Council 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 (REWG) 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 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 (VSAT) technology to restore selected trunking between IC switches and LEC end offices, and selected users in the United States to access the 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.

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 (IIS) 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 (NLP).

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 Commercial Satellite Survivability Task Force*, December 1989.
- *Final Report of the Commercial Satellite Survivability Task Force, Appendix A, Technical Subgroup Report*, December 1989.
- *Final Report of the Commercial Satellite Survivability Task Force, Appendix B, Operational Subgroup Report*, December 1989.
- *Final Report of the Commercial Satellite Survivability 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 IES established the IIS Task Force to develop industry's perspective on the issue. The original IIS Task Force defined and identified sensitive information categories, the relationship between telecommunications and automated information systems, an analysis methodology, and areas for further investigation. The IES then established a follow-on IIS Task Force to improve information security in telecommunications and automated information systems. The IIS Task Force submitted its final report to the NSTAC on September 22, 1988. It contained 10 conclusions and 8 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: 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 (INFOSEC) education program.

Reports Issued:

- *The Industry Information Security Task Force Report, Volume I*, November 1986.
- *The Industry Information Security Task Force Report, Volume II, Appendices*, November 1986.
- *Status Report of the Industry Information Security Task Force*, October 1987.
- *Final Report of the Industry Information Security Task Force—Industry Information Protection, Volume I*, June 1988.
- *Final Report of the Industry Information Security Task Force—Industry Information Protection, Volume II, Appendices*, June 1988.
- *Final Report of the Industry Information Security 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 OMNCS 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 (NTCN) 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 (COR) NTMS Subcommittee to assist in achieving NTMS initial operational capability. The NTMS program became operational with the implementation of the northeast region in October 1990. In September 1991, the activation of the southwest and northwest regions provided additional capability. The subcommittee also completed NTMS regional validations in Chicago, Illinois, during November 1992; in Atlanta, Georgia, during February 1993; and in Denver, Colorado, during April 1993.

Report Issued:

- *NTMS Implementation Concept (Final)*, November 1987.

TELECOMMUNICATIONS INDUSTRY MOBILIZATION

Investigation Group:
Telecommunications Industry Mobilization (TIM) Task Force

Period of Activity:
June 7, 1985–June 8, 1989

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

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

- Telecommunications service surge requirements
- Personnel issues
- Maintenance of stockpiles and inventories
- Dependence on foreign sources
- Dependence on other infrastructure systems
- Industry and Government mobilization management structure
- 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 (NSC) and the Executive Office of the President initiated a review of overall national security mobilization preparedness. FEMA implemented several TIM recommendations as part of the *Graduated Mobilization Response (GMR) Plan*. The OMNCS Office of the Joint Secretariat developed a plan of action, involving all NCS member organizations, designed to track implementation of the TIM recommendations. The plan included identification of task responsibilities, a time-phased work plan, and a schedule of status reports. The Baseline Mobilization program involved assigning "lead" organizations to follow up and take actions necessary to implement each TIM recommendation during a 3-year period, with 36 tasks distributed among the NCS member organizations.

In September 1993, the OMNCS Office of the Joint Secretariat issued its *Final Report on Telecommunications Industry Mobilization (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 Telecommunications Industry Mobilization (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 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 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 SATCOM Interconnectivity (CSI) and the Government Emergency Telecommunications Service (GETS). 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 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 (ECC) 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 (LRG) 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 IES 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 (HEMP)-induced transients and to develop new techniques for limiting transient effects.

Actions Resulting from NSTAC Recommendations: The TSS Task Force reviewed the Government actions taken on the NSTAC's EMP recommendations. It found that the Government had implemented nine of the EMP initiatives or was implementing them. The Telecommunications Systems Survivability (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 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 (ANSI) T1Y1 Committee as a forum for developing electromagnetic standards in support of industry and issued an unclassified EMP handbook (*EMP Mitigation Program Approach, NCS-TIB 87-17*). The OMNCS received results from a simulated EMP test on an AT&T PSN switch. The OMNCS assessed the EMP impact on the PSN based on test results of transmission, signaling, and switching facilities. EMP test analysis results showed little cause for concern regarding the physical EMP survivability of the PSN, but revealed an increasing PSN vulnerability to EMP-induced switch and signaling upset.

Reports Issued:
- *EMP Task Force Status Report*, January 12, 1984.
- *EMP Final Task Force Report*, July 1985.

INTERNATIONAL DIPLOMATIC TELECOMMUNICATIONS

Investigation Group:
International Diplomatic Telecommunications (IDT) Task Force

Period of Activity:
September 27, 1983–December 12, 1984

Issue Background: National Security Decision Directive No. 97 (NSDD-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 NCS 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 IES formed the International Diplomatic Telecommunications (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 2 years.

History of NSTAC Actions and Recommendations: In July 1983, NSTAC II recommended that the President direct the National Security Council (NSC), 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/EPAIP policy

- Initiate efforts to enhance the survivability of NS/EPAIP 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 (CNS) 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 telecommunication 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 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 IES meeting. (See Industry/Government Coordination and Response section for a fuller discussion of recent NCC actions.)

Reports Issued:
- *NCM Task Force Report*, May 16, 1983.
- *NCM Implementation Plan (Final Report)*, January 30, 1984.

THE NSTAC AND ITS MEMBERS

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

MEMBERSHIP (as of June 21, 2000)

*Mr. Herbert W. Anderson	Corporate Vice President Northrop Grumman Corporation
Mr. C. Michael Armstrong	Chairman and CEO AT&T
Dr. J. Robert Beyster	Chairman and CEO Science Applications International Corporation (SAIC)
Ms. Margo H. Briggs	President and CEO Executive Security and Engineering Technologies, Inc. (ESET)
Mr. Richard H. Brown	Chairman and CEO Electronic Data Systems, Inc. (EDS)
*Mr. Daniel P. Burnham	President and CEO Raytheon Company
*Mr. Frank Carlucci	Chairman Nortel Networks
Mr. John T. Chambers	President and CEO Cisco Systems, Inc.
Dr. Vance D. Coffman	Chairman and CEO Lockheed Martin Corporation
Mr. D. Travis Engen	Chairman and CEO ITT Industries, Inc.
Mr. William T. Esrey	Chairman and CEO Sprint Corporation
Mr. James W. Evatt	President, Information and Communications Systems The Boeing Company

THE PRESIDENT’S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

MEMBERSHIP
(Continued)

*Mr. Christopher Galvin	Chairman and CEO Motorola, Inc.
Mr. Van B. Honeycutt (NSTAC Chair)	Chairman, President and CEO Computer Sciences Corporation (CSC)
Mr. Clayton M. Jones	President Rockwell Collins, Inc.
*Mr. Milton H. Jones, Jr.	Executive Vice President, Technology Solutions Group Bank of America, Inc.
Mr. Charles R. Lee	Chairman and CEO GTE Corporation
Mr. John H. Mattingly	President, COMSAT Satellite Services COMSAT Corporation
Mr. Craig O. McCaw	Chairman Teledesic Corporation
*Mr. Richard McGinn	Chairman and CEO Lucent Technologies
*Mr. Craig Mundie	Senior Vice President Microsoft Corporation
Mr. Bert C. Roberts, Jr.	Chairman MCI WorldCom
*Mr. G.William Ruhl	CEO of D&E Telephone Company U. S. Telephone Association (USTA)
Mr. Larry J. Schumann	President and CEO National Telecommunications Alliance, Inc.
Mr. Michael T. Smith	Chairman and CEO Hughes Electronics Corporation

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

MEMBERSHIP
(Concluded)

Dr. Ronald D. Sugar	President and COO, TRW Aerospace and Information Systems TRW, Inc.
Mr. Solomon D. Trujillo	President and CEO U S WEST
Mr. Lawrence A. Weinbach	Chairman and CEO Unisys Corporation

* Approval pending at The White House

EXECUTIVE REPORT ON THE 22ND MEETING

EXECUTIVE REPORT ON THE 22ND MEETING OF THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC XXII)

JUNE 9, 1999

This executive report summarizes the presentations and deliberations of the President's National Security Telecommunications Advisory Committee's 22nd meeting (NSTAC XXII). The NSTAC received briefings from its Industry Executive Subcommittee (IES) and several guest speakers during the Business Session and engaged in discussion with a number of senior Administration officials during the Executive Session. The agenda included topics related to national security telecommunications, including critical infrastructure protection and the Year 2000 (Y2K) technology problem. Attached are the recommendations to the President from NSTAC XXII (Attachment 1) and an attendance list of NSTAC Principals (Attachment 2).

Business Session Opening Remarks.
Mr. Van Honeycutt, Chairman, President and Chief Executive Officer, Computer Sciences Corporation (CSC) and NSTAC Chair, called the NSTAC XXII Business Session to order at the Department of State (DOS), Washington, DC. He then introduced Mr. Fernando Burbano, Chief Information Officer, DOS, who presented the opening remarks. Mr. Burbano welcomed the NSTAC Principals and meeting attendees, noting NSTAC's value to the Administration in providing objective advice on telecommunications issues of critical national importance. He also commended the NSTAC for addressing the Y2K technology problem and challenges to critical infrastructure protection, two issues that require strong public/private partnership. Turning to DOS efforts to address the Y2K problem internationally, Mr. Burbano reported that DOS was continuing to assess international preparations for Y2K. He stated that U.S. embassies are working with the National Intelligence Council to analyze their host country's Y2K readiness and develop contingency plans. Mr. Burbano concluded his remarks by emphasizing that information sharing and partnerships between industry and Government, as embodied in the NSTAC, would be vital to the successful transition to the Year 2000 and for continued efforts toward infrastructure protection.

Mr. Honeycutt then welcomed two new NSTAC Principals–Mr. Milton Jones, Executive Vice President, Technology Solutions Group, Bank of America; and Mr. David House, President, Nortel Networks. He also recognized the members of the National Communications System's (NCS) Committee of Principals and Council of Representatives for their support of the NSTAC's work and their vital role in the industry/Government planning process.

Year 2000.
Mr. John Koskinen, Assistant to the President and Chair of the President's Council on Year 2000 Conversion, briefed the NSTAC Principals and meeting attendees on the progress made by the Council since he spoke at the NSTAC XXI Business Session in September 1998. He described the Council's three-tiered approach to the Y2K problem, which divides the Nation's information infrastructure into Federal systems, State and local systems, and private sector systems. Mr. Koskinen explained that the Council originally focused on domestic preparedness and now has expanded its efforts to the global Y2K readiness effort.

Mr. Koskinen informed the NSTAC that 93 percent of Federal mission-critical systems are prepared for the date rollover, with the remainder of those systems being monitored on a case-by-case basis. In light of that progress, few problems are expected due to failure of Federal systems. He then highlighted the progress of the Department of Defense (DOD), which he commended for making the issue a priority throughout the past year.

While Federal efforts to prepare for the transition to Y2K are on target, Mr. Koskinen cautioned that the readiness of State and local systems is expected to vary, with roughly 20 percent of States still in need of major assistance. He explained that because the States administer 10 major Federal programs, including Food Stamps and Medicaid, the Council is working with less-prepared States to address their needs and help prepare contingency plans.

Mr. Koskinen then reported that the Council had received tremendous support from the private sector, focusing in particular on the efforts of the telecommunications industry to prepare for Y2K. He praised the industry for working with the Council to increase information sharing and complete industry vulnerability assessments. Mr. Koskinen also applauded the efforts of telecommunications officials for their help in passing the Y2K Information and Readiness Disclosure Act, which he described as crucial to helping facilitate Y2K readiness efforts.

In light of the domestic efforts, Mr. Koskinen predicted that a nationwide infrastructure disruption as a result of the Y2K problem is unlikely. He informed the audience that the major Y2K risks are with local systems, and asked for the help of the NSTAC-member companies who are local service providers to participate in local outreach readiness efforts. Mr. Koskinen stated that all infrastructure industries must remain focused on outreach at the community level to reduce the risk of any public overreaction to the Y2K problem.

Internationally, Mr. Koskinen reported that he is participating in a series of meetings with Y2K coordinators from other countries to ensure cooperation on cross-border issues. He assured the members that all countries are aware of the Y2K problem, but some of the less-developed countries are running out of time in the areas of contingency and emergency planning. He then informed the members that the International Telecommunication Union has remained very active in the issue, and that the focus of concern is on local telecommunications in those countries. Mr. Koskinen stated that, although no significant international economic problems are likely to result from the Y2K problem, some sector-specific operational problems might arise.

Mr. Koskinen then responded to various Y2K related questions from the NSTAC Principals. In response to a question about Y2K vulnerabilities related to Internet failures, he stated that the Council had been assured by both the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST) that no problems would occur. However, the Council recently began to examine specifically the issue of degraded Internet service and its potential effects. Mr. Koskinen also discussed the area of Y2K litigation in response to questions from two NSTAC Principals. He explained that the Administration is still working on that issue but does not view its resolution as a priority because it is too soon to say how any potential damages will be addressed and what type of legislation, if any, will be required after January 1, 2000. He concluded by saying that, as with the Y2K Information and Readiness Disclosure Act, industry cooperation would be essential to any solution.

Department of Defense Perspectives on the Year 2000 Technology Problem.
Deputy Secretary of Defense John Hamre began his remarks by discussing the crisis in Kosovo, on what he hoped to be the eve of a peaceful resolution. He then discussed DOD's Y2K readiness and the progress that has been made towards remediating DOD information systems. Dr. Hamre reported that the Department is prepared for Y2K and has no doubts regarding its ability to defend the United States during the transition to the new millennium. Detailing the extent of DOD's Y2K remediation efforts, he stated that 98 percent of mission-critical systems were fixed and certified through independent testing, and that only 40 mission-critical systems (out of a total of 2,100) remained to be tested and certified. Dr. Hamre emphasized that the Department would focus its remediation efforts on fixing those systems before the end of the year. He then added that 85 percent of the Department's 4,000 non-mission-critical systems have been fixed and certified.

Dr. Hamre noted that, because Y2K remediation for DOD systems is nearly complete, emphasis has shifted to forces deployed overseas and their dependence on host country infrastructure readiness. Although the Y2K problem will not affect DOD's ability to wage war abroad, he expressed concerns about quality of life issues for the troops and their dependents. Dr. Hamre explained that DOD was working with host countries on Y2K preparedness issues, including DOD augmentation of host country resources, where needed, and the development of contingency plans.

Dr. Hamre then briefly discussed the need for open dialogue between industry and Government in the current era of dynamic technological change. He asked the NSTAC for assistance in addressing the technological challenges of designing interoperable security solutions and embedding security in the information technology infrastructure. He emphasized that a strong partnership between industry and Government was vital in finding solutions to those challenges.

In response to an NSTAC Principal's comment, Dr. Hamre agreed that the United States does not have a monopoly on the development of encryption technologies. He asserted that the key to the Nation's encryption policy is to achieve a balance so that markets are not closed to U.S. firms, but national security interests are protected. Dr. Hamre stated that he believed that a compromise could be reached between national security interests and those of multinational corporations based in the United States.

With regard to Dr. Hamre's remarks on the transition to Y2K, an NSTAC Principal asked whether there were any indications that groups might exploit potential deficiencies in the infrastructure resulting from Y2K. Dr. Hamre explained that there were no identifiable state-sponsored groups seeking to exploit the Y2K problem and damage DOD information systems, and added that detection capabilities were in place for all DOD networks. In response to a final question, Dr. Hamre agreed that the Government needs to continue to provide funding to law enforcement agencies for research and development of cyber security technologies. He emphasized that law enforcement agencies are facing technical, jurisdictional, and legal constraints in combating cyber crime. He noted that many equities are impacted in addressing the issue and cited the need for an active industry/Government partnership to devise ways to effectively combat cyber crime. Dr. Hamre concluded his remarks by thanking the NSTAC Principals for their commitment and dedication to serving the Nation and for continuing to provide advice and expertise to the Administration on issues vital to the Nation's national security policies.

Manager's Perspective on Key Issues.
Lieutenant General David Kelley, U.S. Army, Manager, NCS, and Director, Defense Information Systems Agency (DISA), discussed the importance of information assurance to the warfighter and the DOD

business enterprise in today's highly interconnected and shared risk environment. He remarked that the ability to share information within this environment depends largely on telecommunications, as shown by the military operations in Kosovo.

General Kelley briefed the NSTAC Principals and meeting attendees on the Defense Information System Network (DISN), a key resource in enabling secure DOD communications worldwide that will be fully implemented by 2010. He stated that DISN utilizes the most sophisticated telecommunications technology available, much of which is provided by NSTAC-member companies, and adapts that technology to meet the needs of the warfighter. He emphasized that while the use of terrestrial-based communications continues to grow, communications via space are becoming increasingly vital to reaching the deployed warfighter.

General Kelley then provided an overview of security risks to DOD networks and information assurance activities. He noted that the number of reported incidents on DOD unclassified networks has increased steadily during the first 5 months of 1999 and attributed the increase to a number of factors, including a heightened awareness of intrusion incidents, improved monitoring tools, and trained personnel. General Kelley cautioned that the Internet age has created an environment in which information is freely and easily disseminated, creating potential security risks within the national security and emergency preparedness (NS/EP) community.

General Kelley highlighted DOD's approach for ensuring the protection of information, which examines security at all levels—from the end user through the network. In addition, he noted that the National Coordinating Center for Telecommunications (NCC) provides the infrastructure for sharing information between Government and the telecommunications industry. In its role as an Information Sharing and Analysis Center (ISAC), the NCC will facilitate information sharing among industry, DISA, DOD's newly established Joint Task Force for Computer Network Defense (JTF-CND), and the National Infrastructure Protection Center (NIPC). In concluding his remarks, General Kelley emphasized the importance of developing an interoperable, secure solution that meets the needs of the warfighter in a joint environment and includes input from the services, coalition partners, and industry. He commented that NSTAC would serve as a vital resource to the Nation as those challenges are addressed.

General Kelley then introduced Mr. Albert Edmonds, former Manager, NCS, to discuss ways in which DOD uses electronic commerce initiatives to improve business operations and assist the warfighter. Mr. Edmonds opened his presentation by emphasizing that a strong public/private partnership is necessary to ensure the success of those electronic initiatives. He then discussed current electronic initiatives within DOD, including—

- Electronic Document Access—Electronic access to documents in support of the contracting process through a secure Web-based server;
- Central Contractor Registration—A centralized, Government trading-partner database;
- Electronic Commerce Processing Node—A single interface between the Government and private sector trading partners; and
- Wide Area Workflow—Support of electronic receipt, storage, and retrieval of documents that support electronic procurement.

Mr. Edmonds emphasized that building confidence in the process would be the key enabler of success for each of those initiatives. He stated that while DOD was confident in the security of its classified networks, steps needed to be taken to ensure that the unclassified systems on which those electronic initiatives would operate were robust and secure. Attaining that assurance would involve finding trusted commercial-off-the-shelf products, implementing trusted processes to secure the unclassified networks, and ultimately, establishing a public key infrastructure (PKI). Mr. Edmonds noted that while the technology needed to establish a PKI was in place, a strong public/private partnership was needed to ensure public confidence in the PKI.

Mr. Edmonds introduced Major General John Campbell, USAF, Vice Director, DISA, and Commander, JTF-CND. Collocated with DISA's Global Network Operations and Security Center and working in conjunction with the unified military commands, services, and agencies, the JTF-CND coordinates and directs the defense of DOD computer systems and networks. General Campbell said that to fulfill its responsibilities, the JTF-CND was engaged in a wide range of operations, including monitoring DOD computer networks; directing actions to defend the Defense Information Infrastructure (DII) from intrusions; and assessing the impact of intrusions into the DII. In addition, General Campbell detailed the JTF-CND's important role in coordinating the defense of DOD networks with other Government agencies and appropriate private organizations. In particular, he stated that the JTF-CND's cooperative information sharing agreements with the NIPC and the NCC were especially critical to the JTF-CND's ability to accomplish its operational and strategic goals. General Campbell noted that JTF-CND's formation was consistent with DOD's realization that information superiority—the capability to collect, process, exploit, and disseminate an uninterrupted flow of information, and to deny the enemy's ability to do the same—was key to the success of the United States military in the next century. He said that several recent events, including the exercise Eligible Receiver and the attack known as Solar Sunrise, had been significant in demonstrating both the DII's security vulnerabilities and the need for an organization with the authority and responsibility to direct the DII's defense. Moreover, he said that threats to the DII in the forms of state-sponsored and terrorist attacks, industrial and foreign espionage, disgruntled employees, and hackers were expected to become more serious.

General Campbell explained that by providing a computer network defense capability where none had previously existed, the JTF-CND provided an effective interim solution to DOD's computer network defense problem, pending the finalization of a Unified Command Plan to address DII defense issues. Noting that the United States Space Command would assume responsibility for DOD computer network defense in October 1999, he said that the JTF-CND would retain its present role as the DOD's single point of contact for defensive computer network operations.

Industry Executive Subcommittee Report.

Mr. Guy Copeland, CSC and IES Working Session Chair, briefed the NSTAC Principals and meeting attendees on the work of the IES during the NSTAC XXII cycle in four key issue areas:

- infrastructure protection,
- network security,
- legislation and regulation, and
- industry/Government coordination and response.

Mr. Copeland stated that the NS/EP issues related to the Y2K technology problem were addressed in each of these areas. Mr. Copeland first reviewed the subcommittee's work in the area of infrastructure protection. He stated that at the request of the Critical Infrastructure Assurance Office, the IES had been reviewing the contents of the draft National Information Systems Protection Plan ("the National Plan") and providing comments on it to them. He noted that the Transportation Information Infrastructure Workshop, held in March in cooperation with the Department of Transportation (DOT), facilitated the completion of the Transportation Information Infrastructure Risk Assessment. That assessment, Mr. Copeland explained, was the third and final one undertaken by the NSTAC as part of a Presidential request to examine the information-based risks to infrastructures identified as having strong interdependencies and a growing reliance on telecommunications and information systems. The assessment revealed that several industry-wide factors, including the globalization of transportation companies, the intermodal transport of goods and services, and increased reliance on information technology, are increasing the vulnerability of the transportation infrastructures to the large-scale effects from information system outages. The IES therefore concluded that the industry could benefit from future DOT conferences and the timely dissemination of Government information on physical and cyber threats to the transportation infrastructure.

Mr. Copeland stated that the IES also completed its investigation of the NS/EP implications of the use of Electronic Commerce (EC) in the Federal Government and how EC could affect business operations and security processes within the NS/EP community. He reported that while the IES found that the NS/EP community's use of, and dependence on, EC is still modest, it will grow steadily, therefore heightening the need for a coordinated focus to address NS/EP requirements. Toward that end, the IES recommended that the President, in accordance with Executive Order (E.O.) 12472, Assignment of National Security and Emergency Preparedness Functions, designate a focal point to examine the NS/EP issues related to the widespread adoption of EC. Mr. Copeland also explained that on the basis of previous NSTAC findings, the IES believes that the Global Information Infrastructure (GII) will present significant new opportunities, as well as vulnerabilities, for NS/EP telecommunications in the future. Therefore, the IES began a study to postulate the GII for 2010, focusing on airborne and space-based communications systems, land-based communications systems, and emerging applications and protocols. Mr. Copeland concluded the review of the current cycle's infrastructure protection activities by stating that at the request of Attorney General Janet Reno, the IES had facilitated a partnership between the Department of Justice (DOJ) and several industry associations. That partnership had been labeled the "Cyber Citizen" Program. During the next cycle, the IES plans to work with DOJ to sponsor a round table between senior industry and Government officials to discuss cyber security policy issues. He also stated that the IES plans to continue the ongoing projects that he had highlighted.

Mr. Copeland discussed the subcommittee's network security projects, focusing first on its study of the NS/EP community's use of the Internet. He explained that due to concerns about the Internet's reliability and security, the NS/EP community's direct dependence on the Internet is limited to outreach, information sharing, and e-mail, while dedicated Transmission Control Protocol/Intenet Protocol (TCP/IP) networks, or intranets, are used for mission-critical functions. However, he cautioned that the interconnected nature of TCP/IP networks could result in the disruption of service to those intranets, should the Internet infrastructure experience difficulties. Mr. Copeland also noted that the study concluded that NS/EP dependence on the Internet is expected to grow over the next several years as the Government continues to explore more efficient means of doing business. Therefore, the IES recommended that in accordance with E.O. 12472, the President establish a permanent program within the Federal Government to address NS/EP needs specific to the Internet. In addition, the NSTAC recommended that the President direct the appropriate Government departments and agencies to use existing industry/Government partnerships to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

Mr. Copeland then turned to other network security initiatives, including the Research & Development Exchange Symposium, which addressed the growing convergence within the telecommunications industry and ways to improve collaboration among Government, industry, and academia. Mr. Copeland reported that the NSTAC Network Security Information Exchange (NSIE) continued to meet with the Government NSIE. The two NSIE's had collaborated in producing two key documents?an After-Action Report on the Insider Threat Workshop and the 1999 Assessment of the Risk to the Security of the Public Network. The latter report built upon a similar risk assessment completed in 1995 and identified three factors that have increased the risk to the public network: the Telecommunications Act of 1996, the Y2K technology problem, and the changing business practices within industry. Mr. Copeland then stated that during the next cycle the IES planned to conduct another Research & Development Exchange Symposium to continue to foster information exchange among industry, Government, and academia on network security Research & Development; examine the focus of network security efforts with respect to current operations and Research & Development initiatives; and examine how the convergence of the public switched network with Internet Protocol-based networks could affect NS/EP telecommunications priority services.

The third issue area focused on legislation and regulation. Mr. Copeland stated that the primary focus of that area was information sharing between industry and Government in response to telecommunications outages and network intrusions. As a first step towards examining this problem, the IES developed a report that illustrates the current and proposed information sharing process between industry and Government. The IES also began analysis of a provision in the Fiscal Year 1999 Omnibus Appropriations Act (Public Law 105-277) that directs the Office of Management and Budget to require Federal awarding agencies to ensure all data produced under an award is available to the public through the Freedom of Information Act. Mr. Copeland explained that this provision could increase the reluctance of industry to share sensitive information with Government, or even the Information Sharing and Analysis Center (ISAC) proposed by Presidential Decision Directive 63 (PDD-63). With regard to the NSTAC's next steps in the area of legislation and regulation, Mr. Copeland said the subcommittee planned to continue to examine options for eliminating barriers to information sharing, examine the definition of foreign ownership within the telecommunications industry and how it affects NS/EP communications, and continue to monitor the regulatory environment surrounding network convergence for any impact on NS/EP communications.

Mr. Copeland then discussed the NSTAC's work examining issues related to industry/Government coordination and response. He stated that the IES had worked closely with the NCC to develop guidelines and reporting criteria for the NCC's new indications, assessment, and warning function, and had begun assessing participation in the NCC in an effort to determine if additional companies are needed to help fulfill the NCC's expanded mission. Mr. Copeland also indicated NSTAC's support of the development of a memorandum of understanding between the Manager, NCS, and the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism formally establishing the NCC as an ISAC for the telecommunications infrastructure.

Lastly, Mr. Copeland discussed NSTAC's efforts to coordinate Y2K outreach and contingency planning by sponsoring a series of meetings with industry and Government entities responsible for Y2K preparedness. He explained that those meetings facilitated discussions that ensured that NS/EP aspects of the Y2K technology problem were being addressed. Specific topics that were examined included the development of an international Y2K early warning system for telecommunications and the domestic and international roles of the NCC as a national coordinating body for response to Y2K telecommunications events. Based on the study of the Y2K problem, the IES recommended that the Federal Government take the necessary steps to ensure the timely dissemination of meaningful and accurate Y2K planning information to State and local governments, which will enhance the flow of information to the general public and community groups.

Before closing his remarks, Mr. Copeland highlighted two executive-level events planned for the next cycle—a Y2K Executive Meeting that will provide a forum for senior members of industry and Government to share contingency planning information, and the cyber security round table that NSTAC plans to co-host with DOJ.

Executive Session Opening Remarks.
Mr. Honeycutt welcomed the NSTAC Principals and Government officials to the NSTAC XXII Executive Session in the Indian Treaty Room of the Old Executive Office Building, Washington, DC. He introduced the President's advisors and key Government officials in attendance:

- The Honorable William Cohen, Secretary of Defense;
- The Honorable Neal Lane, Assistant to the President for Science and Technology;
- The Honorable Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-terrorism; and
- The Honorable Michael Powell, Defense Commissioner of the Federal Communications Commission (FCC).

Mr. Honeycutt noted that General Richard Myers, USAF, Commander in Chief of North American Aerospace Defense Command and U.S. Space Command, was also in attendance.

Executive Session Discussion.
Mr. Honeycutt initiated discussion on the agenda items for the Executive Session—domestic and international Y2K readiness and response and critical infrastructure protection. He then highlighted several connections between the two issues. First, Y2K response strategies may provide valuable lessons learned that can be applied to critical infrastructure protection. Second, information sharing and coordination of activities are issues that result from both Y2K readiness and critical infrastructure protection because they require high levels of cooperation between industry and Government. Third, many solutions to the Y2K problem may also apply to critical infrastructure protection because information technology is a commonality of all infrastructures.

Mr. Honeycutt then directed the discussion to Secretary Cohen by asking him to elaborate on: 1) how DOD is preparing to respond to potential domestic and international Y2K issues; 2) how responses will be prioritized; and 3) how industry can support the DOD in its efforts. Secretary Cohen replied that the DOD has made significant progress in preparing the Department's systems for Y2K. He reminded the NSTAC Principals that at the NSTAC XXI meeting in September 1998, the DOD's mission-critical systems were only 40 percent Y2K compliant. Currently, 95 percent have completed auditing and testing and are compliant. This dramatic improvement is due to large financial commitments made by the Department and a high level of industry involvement. Secretary Cohen also noted that the DOD is working with the Federal Emergency Management Agency on the State and local levels to develop contingency plans for any private sector infrastructure elements that may fail. He emphasized that industry must be a significant partner in addressing the issue because almost all the Department's communications capabilities are based on commercial services. Additionally, the DOD is further ensuring readiness by exercising multiple scenarios that include domestic, international, and nuclear components.

On an international level, Secretary Cohen stated that U.S. allies are working to ensure Y2K readiness, but not as intensely as the United States. The Y2K issue is forcing the United States to examine the security of other countries. He noted that Russia has not yet adequately addressed the Y2K technology problem and most likely will not be prepared when the rollover occurs. The United States is attempting to assist Russia in its efforts but is encountering numerous political barriers. Secretary Cohen also remarked that China has not expressed particular concern for the potential difficulties that may result from Y2K and views the Y2K issue as a "western" problem.

Mr. Honeycutt asked Commissioner Powell to comment on what he perceives the greatest Y2K related challenges to the telecommunications industry to be and what the NSTAC can do to address them. Commissioner Powell responded by noting several Y2K issues that have emerged from the telecommunications working group that he co-chairs under the auspices of the President's Council on Year 2000 Conversion. Commissioner Powell then stated that significant advancement has been made in two areas—awareness and assessment—since he last spoke with the NSTAC in September 1998. In addition, he reported progress with contingency planning efforts. He explained that the FCC is establishing an international real-time operations center which will be connected to the White House Y2K center and the NCC. The FCC's center is considering incorporating the necessary elements to alleviate regulatory constraints (e.g., license requirements) if the need arises during an emergency situation.

Commissioner Powell then outlined his primary concerns regarding Y2K. Domestically, small- to mid-sized telecommunications providers and public safety answering points present the most obvious challenges. Internationally, the situation is more difficult to generalize; but, like Secretary Cohen, he has not observed the same level of effort in addressing potential Y2K technical problems internationally as in the United States.

In response to an NSTAC Principal's question, Commissioner Powell and Secretary Cohen both stated that they anticipate significant leave restrictions on personnel within the Federal Government. Commissioner Powell added that he believes the year-end response requires senior leadership and participation in both industry and Government operations centers.

Mr. Honeycutt then asked Mr. Clarke to explain how the Y2K experience can be leveraged to address critical infrastructure protection and how NSTAC can assist with those efforts. Mr. Clarke responded that the transition of resources and experiences from Y2K to critical infrastructure protection is a natural progression. For example, the process of identifying mission-critical systems for Y2K also applies to critical infrastructure protection. However, because the computers of DOD and the telecommunications industry are under constant attack, the challenges do not end with software remediation for the Y2K problem. Mr. Clarke also emphasized that the effort to remediate Y2K problems in software may create its own set of information security risks because the majority of the programming occurs offshore. Therefore, the awareness of and investment in asset protection must not end with the Y2K transition.

Mr. Clarke then discussed some of the goals and accomplishments in the area of critical infrastructure protection. He began by explaining that the draft National Plan contains specific guidelines and milestones to move beyond the work of the President's Commission on Critical Infrastructure Protection and PDD-63. Mr. Clarke requested that the NSTAC review the latest draft of the National Plan and provide comments. During the discussion, he stated that the establishment of ISACs for telecommunications and banking and finance is imminent. He explained that he also sees the need for computer security alliances to be established in the private sector to address growing dependency and software issues.

Mr. Honeycutt then referred the discussion to Dr. Lane, noting Dr. Lane's predecessor's attendance at the NSTAC XX meeting in December 1997, where he discussed new Federal infrastructure protection R&D initiatives. He asked Dr. Lane to comment on the Federal Government's current R&D program, especially how it relates to the telecommunications and information infrastructure. Dr. Lane explained that the Federal Government had identified some areas in R&D that need additional attention, such as intrusion detection and network monitoring. He explained that a plan on R&D in the area of infrastructure protection had recently been drafted, and the NSTAC's assistance in identifying any gaps in the assessment is extremely valuable to the process.

Adjournment.
Before adjournment, Mr. Honeycutt expressed his appreciation to the NSTAC members and the key Government officials for their participation in the Executive Session. In the closing remarks, he noted that he would like the NSTAC members to consider meeting again in June 2000. At that point, any issues arising from the Y2K transition may be resolved and would provide input to the meeting's discussion topics.

ATTACHMENT 1

RECOMMENDATIONS TO THE PRESIDENT FROM THE 22ND MEETING OF THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC XXII)

JUNE 9, 1999

INFORMATION INFRASTRUCTURE GROUP (IIG).

Recommendations to the President

- Recommend 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 Presidential Decision Directive 63 (PDD-63). Specifically, recommend 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,

  – joint industry/Government efforts to examine emerging industry-wide vulnerabilities such as those related to the Global Positioning System, and

  – future Department of Transportation conferences to stimulate intermodal and, where appropriate, interinfrastructure information exchange on threats, vulnerabilities, and best practices.

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order (E.O.) 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* designate a focal point for examining the national security and emergency preparedness (NS/EP) issues related to widespread adoption of electronic commerce (EC) within the Government.

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

NETWORK GROUP (NG).

Recommendations to the President

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by E. 0. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:

  – work with the NS/EP community to increase understanding of evolving Internet dependencies;

  – work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements;

  – interact with the appropriate Internet organizations and initiatives to investigate, develop, and employ NS/EP-specific Internet priority services, such as priority access, end-to-end routing, and transport; and

  – examine the potential impact of Internet protocol (IP) network-public switched network (PSN) convergence on PSN-specific NS/EP priority services (e.g., Government Emergency Telecommunications Service [GETS] and Telecommunications Service Priority [TSP]).

- Recommend that the President direct the appropriate Government departments and agencies to make use of existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

OPERATIONS SUPPORT GROUP (OSG).

Recommendations to the President

- Recommend that the President direct the President's Council on Year 2000 Conversion and the Federal Government to 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.

ATTACHMENT 2

ATTENDANCE OF MEMBERS AT THE 22ND MEETING OF THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC XXII)

JUNE 9, 1999

NSTAC CHAIR
Mr. Van B. Honeycutt
Chairman, President and CEO
Computer Sciences Corporation

Dr. J. Robert Beyster
Chairman and CEO
Science Applications International Cooperation

Ms. Margo H. Briggs
President and CEO
Executive Security & Engineering
Technologies, Inc.

Mr. D. Travis Engen
Chairman and CEO
ITT Industries, Inc.

Mr. James W. Evatt
President, Information and Communications
Systems
The Boeing Company

Mr. William J. Hilsman
Chairman
Advanced Digital Technologies Company

* Mr. David L. House
President
Nortel Networks

* Mr. Milton H. Jones, Jr.
Executive Vice President, Technology Solutions
Group
Bank of America Corporation

Mr. Craig O. McCaw
Chairman
Teledesic Corporation

Mr. Dennis J. Picard
Chairman and CEO
Raytheon Company

Mr. Bert C. Roberts, Jr.
Chairman
MCI WorldCom, Inc.

Mr. Larry J. Schumann
President and CEO
National Telecommunications Alliance, Inc.

Mr. Michael T. Smith
Chairman and CEO
Hughes Electronics Corporation

Mr. Lawrence A. Weinbach
Chairman and CEO
Unisys Corporation

* Membership pending approval at the White House.

ACRONYMS

ACRONYMS

AIN	Advanced Intelligent Networks
AIP	Automated Information Processing
ANSI	American National Standards Institute
CCS	Common Channel Signaling
CFR	Code of Federal Regulations
CIAO	Critical Infrastructure Assurance Office
CIP	Critical Infrastructure Protection
CNS	Commercial Network Survivability
COAST	Computer Operations, Audit, and Security Technology
COP	Committee of Principals
COR	Council of Representatives
CPAS	Cellular Priority Access Service
CPE	Customer Premises Equipment
CSI	Commercial SATCOM Interconnectivity
CSS	Commercial Satellite Survivability
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DOS	Department of State
EC	Electronic Commerce
ECC	Enhanced Call Completion
ECSA	Exchange Carriers Standards Association
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
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FNI	Funding of NSTAC Initiatives
FOIA	Freedom of Information Act
FRP	Federal Response Plan
FRWG	Funding and Regulatory Working Group
FWUF	Federal Wireless Users Forum
GETS	Government Emergency Telecommunications Service
GII	Global Information Infrastructure
GMR	Graduated Mobilization Response
GNSS	Government Network Security Subgroup
GSA	General Services Administration
GTF	Globalization Task Force
HEMP	High-Altitude Electromagnetic Pulse
HPC	High Probability of Call Completion

ACRONYMS
(CONTINUED)

IA	Information Assurance
IATF	Information Assurance Task Force
IAW	Indicators, Assessment, and Warnings
IC	Interexchange Carrier
IDSG	Intrusion Detection Subgroup
IDT	International Diplomatic Telecommunications
IEEE	Institute of Electrical and Electronics Engineers
IES	Industry Executive Subcommittee
IIG	Information Infrastructure Group
IIS	Industry Information Security
IITF	Information Infrastructure Task Force
IN	Intelligent Networks
INFOSEC	Information Security
ISAC	Information Sharing and Analysis Center
IS/CIPTF	Information Sharing/Critical Infrastructure Protection Task Force
ISSB	Information Systems Security Board
ITPITF	Information Technology Progress Impact Task Force
JTF-CND	Joint Task Force for Computer Network Defense
LEC	Local Exchange Carriers
LRG	Legislative and Regulatory Group
LRWG	Legislative and Regulatory Working Group
MOU	Memorandum of Understanding
NATO	North American Treaty Organization
NCC	National Coordinating Center for Telecommunications
NCM	National Coordinating Mechanism
NCS	National Communications System
NEC	National Economic Council
NERC	North American Electric Reliability Council
NES	National Energy Strategy
NG	Network Group
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NLP	National Level NS/EP Telecommunications Program
NOF	Network Operations Forum
NRC	National Research Council
NRIC	National Research Interoperability Council
NSA	National Security Agency
NSDD	National Security Decision Directive
NSG	Network Security Group
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchange
NSSC	Network Security Steering Committee
NSSOG	Network Security Standards Oversight Group
NSTAC	National Security Telecommunications Advisory Committee
NSTF	Network Security Task Force
NTCN	National Telecommunications Coordinating Network
NTIA	National Telecommunications and Information Administration

ACRONYMS (CONTINUED)

NTMS	National Telecommunications Management Structure
NWC	Naval War College
OMNCS	Office of the Manager, National Communications System
OSG	Operations Support Group
OSTP	Office of Science and Technology Policy
OWG	Operations Working Group
PCCIP	President’s Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PKI	Public Key Infrastructure
PN	Public Network
PSN	Public Switched Network
PSTF	Protecting Systems Task Force
PWG	Plans Working Group
QoS	Quality of Service
R&D	Research and Development
REWG	Resource Enhancements Working Group
RP	Restoration Priority
SCOE	Security Center of Excellence
SLG	Standards Liaison Group
SS7	Signaling System 7
STU	Secure Telephone Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TESP	Telecommunications Electric Service Priority
TIM	Telecommunications Industry Mobilization
TSP	Telecommunications Service Priority
TSS	Telecommunications Systems Survivability
UST	Underground Storage Tank
USTA	United States Telephone Association
VSAT	Very Small Aperture Terminal
W/LBRDSTF	Wireless/Low-Bit-Rate Digital Services Task Force
WOS	Widespread Outage Subgroup
WSPO	Wireless Services Program Office
WSTF	Wireless Services Task Force
Y2K	Year 2000