THE PRESIDENT’S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NATIONAL SECURITY TELECOMMUNICATIONS
NSTAC
ADVISORY COMMITTEE

The NSTAC's Response to the National Plan

APRIL 2001

April 17, 2001

The President
The White House
1600 Pennsylvania Avenue, NW
Washington, DC 20500

Dear Mr. President:

At our May 16, 2000, National Security Telecommunications Advisory Committee (NSTAC) XXIII meeting,
Mr. Richard Clarke, National Coordinator for Security, Critical Infrastructure Protection, and Counter-Terrorism, National Security Council, requested industry advice and recommendations for revision of the National Plan for Information Systems Protection. Enclosed is the Committee's response.

The Committee's response is based primarily on detailed research and analysis done over recent years in reply to requests from the Executive Office of the President relating to the nation's information and communication infrastructure. Our response was shared with the industry sector coordinators and the Commerce Department's office responsible for the Information and Communications Sector. The Committee continues to address the potential for widespread outages of our nation's telecommunications and information services resulting from the convergence of the commercial telephony and Internet networks.

Our nation's critical infrastructures are highly interdependent and heavily dependent on information and communications networks and services. The next version of the National Plan should ensure that National Security and Emergency Preparedness (NS/EP) telecommunications and information systems requirements are identified and supported for the next generation of networks. Additionally, the committee recommends the inclusion of a new broad objective to the National Plan — International Considerations — based on its study of globalization.

We look forward to continuing our advice to you and your Administration on critical cyber issues facing our nation's economic security and our national security and emergency preparedness posture. Our next meeting is June 6, 2001, at the White House, and we are looking forward to meeting with you and other senior members of your Administration.

Sincerely,

Daniel P. Burnham
NSTAC Chair

Enclosure: NSTAC's Response to Version 1.0 of the National Plan

Copy to: National Security Advisor
White House Science Advisor
National Coordinator for Security, Infrastructure Protection,
and Counter-Terrorism
NSTAC Principals
Secretary of Commerce
Manager, National Communications System
Assistant Secretary of Defense for C3I

THE NSTAC'S RESPONSE TO THE NATIONAL PLAN

The National Security Telecommunications Advisory Committee (NSTAC)[1] Information Sharing for Critical Infrastructure Protection Task Force developed this document, *The NSTAC's Response to the National Plan*, to highlight the NSTAC's work in several issue areas that are important to the main objectives of Version 1.0 of the *National Plan for Information Systems Protection* (National Plan). The issue areas are discussed in the context of summaries of previous NSTAC reports presented in the Appendix: Summaries of Previous NSTAC Reports. This document is organized around the three broad objectives listed in the National Plan, which are essential for critical infrastructure protection (CIP)—Prepare and Prevent, Detect and Respond, and Build Strong Foundations. In addition, it is proposed that a new broad objective—International Considerations—be included in Version 2.0 of the National Plan.

The NSTAC's studies of Information and Communications (I&C) Sector Interdependencies and Risk Management broadly relate to the first objective of the National Plan: Prepare and Prevent. That objective addresses the National Plan goal of identifying critical infrastructure assets, shared interdependencies, vulnerabilities, and outreach programs to make Americans aware of the need for improved cyber-security. The second objective of the National Plan, Detect and Respond, connects with the NSTAC issue areas of Network Technologies and Vulnerabilities, Response and Recovery, and Information Sharing. Detect and Respond correlates to the National Plan objectives to detect attacks and unauthorized intrusions, share attack warnings and information in a timely manner, and create capabilities for responses, reconstruction, and recovery. Finally, the NSTAC has examined a variety of issues concerning Research and Development (R&D) needs, I&C Sector Interdependencies, and Information Sharing, which align with Build Strong Foundations, the third objective listed in the National Plan. Build Strong Foundations corresponds to the National Plan's intent to enhance CIP R&D efforts, train and employ adequate numbers of information security specialists, and adopt legislation in support of CIP efforts.

This response presents an overview of the NSTAC's "work in progress" and a synthesis of relevant conclusions and recommendations that have been presented to the President involving issues that could impact national security and emergency preparedness (NS/EP) in telecommunications and information services. NSTAC reports from the mid-1990s forward are presented in the Appendix. These reports relate to issues created by not only the evolving telecommunications and information infrastructure—from the public network (PN)[2] and the public switched network (PSN),[3] through the Internet to the next generation network (NGN)[4]—but also the changing nature of the threats from physical only to physical and cyber. Because these recommendations remain valid and relevant, they should be included in the National Plan. Above all, these findings have a more important, fundamental value because they have been generated by an exhaustive industry/Government information sharing process that has withstood the test of time.

The NSTAC has been involved in depth with the CIP issue since its inception and continues its work in this area, but the NSTAC is aware that the Nation is only on the threshold of the issue. The NSTAC utilizes a fairly formal process to determine work plans, which it will develop in conjunction with the upcoming NSTAC XXIV meeting; however, the NSTAC could address future issues. The NSTAC could augment prepare, prevent, and respond with an examination of consequence management policy and with this, an expansion of the roles of the National Coordinating Center for Telecommunications (NCC) and the Network Security Information Exchanges (NSIE), to include relationships with other CIP components. Although these are just examples, they emphasize the idea that *The NSTAC's Response to the National Plan* will continue to be a work in progress responsive to National needs.

This information has been shared with the I&C sector through meetings with NSTAC member companies and through joint meetings with the I&C sector coordinators' representatives from the Information Technology Association of America, the Telecommunications Industry Association, and the United States Telecom Association.

Shared Challenges

At the outset, it is recognized that the dialogue to develop a National Plan stems from the shared challenges that Government and the telecommunications and information-related industries face, albeit from different perspectives:

- National security in today's global environment is being defined and measured in terms of economic and military strength. Thus, the Nation's wellbeing is highly dependent on the protection of the interdependent critical infrastructures as emphasized in Presidential Decision Directive 63 (PDD •63).

- The Government is increasingly relying on the private sector to provide telecommunications and information services. This necessitates a continuing dialogue to promote mutual understanding of industry and Government interests and concerns as the public and private sectors strive to meet the objectives of protecting the critical infrastructures through nonregulatory solutions as anticipated by PDD•63.

- While Government is focusing on protecting national security, preventing future attacks, and identifying and punishing attackers, private owners of infrastructures are more concerned with common business imperatives. As a result of this dichotomy, any solution to, or recommendations for, the protection of critical infrastructures require the participation of private industry in concert with Government.

- The *Telecommunications Act of 1996* is opening the telecommunications industry to increased competition and interconnection, industry consolidation and integration, and foreign ownership at the same time that new service providers are gaining access to network facilities. Security measures are consequently becoming even more complicated and difficult to implement.

- The evolution to the NGN is enabling and requiring telecommunications providers to transition from proprietary protocols to open system protocols to manage their networks. Concurrently, traditional circuit switched services are migrating to the Internet's packet•switched networks. As this migration continues and new Internet services are introduced, the PN may become more susceptible to well-known Internet vulnerabilities, especially in light of the more integrated and increasing dependence on commercial-off-the-shelf technology.

- The assurance and full protection of American citizens' civil liberties, their rights to privacy, and their rights to the protection of proprietary data should be affirmatively addressed in CIP planning.

Addressing the Broad Objectives of the National Plan

In this response, which focuses on efforts that the Federal Government is undertaking to protect the Nation's critical infrastructures, it should be noted that NSTAC recommendations have already been made to the President concerning many of the programs upon which the Plan's three broad objectives are based—Prepare and Prevent, Detect and Respond, and Build Strong Foundations. This timeliness exists because many of the issues associated with the National Plan's programs have been—or are being—addressed in the NSTAC process,[5] either in response to an Administration request, as is the case with the assessment of the potential for a widespread outage due to network convergence,[6] or in anticipation by member companies of an issue or development that could impact NS/EP telecommunications services. These issues are discussed under different headings in the Appendix.

National Plan Objectives: Prepare and Prevent

A long-standing goal of the NSTAC has been to take steps to minimize the possibility of a significant and successful attack on the Nation's critical telecommunications and information infrastructure and to build an infrastructure that remains effective in the face of such an attack. Indeed, the NSTAC in 1984 recommended that the NCC be established as a national coordinating mechanism to respond to the Federal Government's NS/EP communications service. The NSTAC also initiated the development of the NSIE process in 1991 to provide a forum in which industry and Government could share information with the goal of reducing the vulnerability of the Nation's telecommunications systems to electronic intrusion.[7]

Industry in general is recommending that physical security be included in Version 2.0; it was not included in Version 1.0. However, it is interesting to note that the primary focus of the NCC in the 1980s was on physical threats—an emphasis that was consistent with the Government's overall focus, at the time, on the security of important physical structures, such as dams, bridges, tunnels, and power plants.[8]

As demonstrated in the following text, the focus consequently has broadened from assessments of physical threats leading to service outages to the inclusion of assessments of the threats or risks of unauthorized intrusions of the PN and vulnerabilities associated with network convergence. Concurrently, methodologies for conducting these assessments have been developed and refined to accommodate technological change.

PN Assessments. Assessments were conducted in 1995[9] and 1999[10] with respect to unauthorized penetration or manipulation of the evolving PN software and databases affecting NS/EP telecommunications services.

- Both assessments found that Government and corporate networks had become more interconnected as these organizations have increasingly relied on the PN to transmit critical business and operations information, thereby increasing the perceived and substantive rewards for gaining illicit access.

- The most recent assessment concluded that absent a valid baseline to establish quantitative measures of the risk to the PN from electronic intrusion, it was difficult to definitively state how risk had changed over the past few years. Indeed, little evidence suggests that the risk has diminished; and a number of factors suggest that it is growing.

Internet Assessments. In 1999 the Government's use of the Internet[11] was assessed in parallel with its increasing reliance on the Internet for conducting electronic commerce (e-commerce).[12] Many of the significant findings in those assessments were similar:

- Agencies with NS/EP responsibilities are using the public Internet mostly for outreach, information sharing, and e-mail. Direct dependence on the public Internet for mission•critical operations and e-commerce is currently modest, although the NS/EP community's dependence on the Internet is likely to grow over the next several years. Government will more likely depend on dedicated intranets for mission-critical operations.

- The informal and distributed management of Internet functions, the Domain Name System, Internet software, and procedural errors and unintentional actions invite potential vulnerabilities. Because of the interconnected nature of the public Internet, a disruption or degradation of Internet operations could also hamper the operations of dedicated intranets.

- The reliability and security of the public Internet are generally considered inadequate for NS/EP mission-critical functions and sensitive e-commerce transactions. No Internet technologies or applications yet facilitate the same type of end-to-end NS/EP-related services available in the PN. Nor are there economical incentives for Internet service providers (ISP) to develop and offer NS/EP service enhancements over their networks. A number of factors (e.g., lack of NS/EP demand and market factors) preclude the availability of NS/EP services over the Internet for the foreseeable future.

Accordingly, the following recommendations were made to the President:

- Direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should work with the NS/EP community to increase the understanding of evolving Internet dependencies and with key Internet organizations and standards bodies to increase awareness of NS/EP requirements; and

- Designate a focal point for examining the NS/EP issues related to widespread adoption of e-commerce within the Government, and direct the Federal departments and agencies, in cooperation with this Federal focal point, to assess the effect of e-commerce technologies on their NS/EP operations.

Convergence Assessments. The implications of the PSN-Internet technical convergence and of the transfer of traffic from the PSN to the NGN on the Government's voice priority NS/EP services are under continuing examination. Specific attention is being paid to potential impacts on the Government Emergency Telecommunications Service (GETS)[13] and Telecommunications Service Priority (TSP)[14] programs. A mid-2000 assessment reached a number of conclusions, including:[15]

- As the PN changes from separate switched voice and packet data networks to an interconnected network and then to a unified NGN over the next several years, the capabilities in the PN around which GETS has been designed, such as ubiquity and interoperability, access to NS/EP functional features, and high levels of network reliability and security, will no longer be available. To maintain GETS-type functions, new quality of service schemes and functional requirements will have to be developed to provide services commensurate with NS/EP needs and security safeguards.

- TSP, as originally conceived, remains relevant during convergence because restoration assignments can still be applied to identifiable segments of the PSN. But, as discussed by the program's Oversight Committee, the program is inapplicable to ISPs offering voice services; it should not have a role in the NGN; and if the NS/EP community requires similar types of priority services for packet networks, a new program will have to be established to support such services.

- Although specific NGN standards have not yet been developed to support NS/EP requirements, the NGN technology can support them. Nonetheless, these requirements are unlikely to be incorporated by industry unless the features needed to meet them are standardized by industry, perhaps with prompting from the Government.

It has been recommended that the appropriate departments and agencies, in coordination with industry, be directed by the President to promptly determine precise functional NS/EP requirements for convergence and the NGN, and to ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during standards development and implementation.

Widespread Network Outage Assessments. The Administration continues to request assessments regarding the possibility of a widespread service outage in the PN, particularly in light of increasing convergence.

In April 1997, the Assistant to the President for Science and Technology requested an assessment of the possibility of a widespread service outage in the public telephone network.[16] An initial response in December 1997[17] and a follow-up response 9 months later—[18]

- Defined widespread outage as “a sustained interruption of telecommunications service that would have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would impact the availability and integrity of telecommunications service for at least a significant portion of a business day."

- Concluded that, given the limited precedent for telecommunications outages of this magnitude and member companies' prior experiences with smaller-scale outages, there is a *low probability* of a widespread, sustained outage of public telephone service; however, the potential societal impacts of such an outage are high enough to warrant consideration.

- Offered recommendations to the President intended to decrease the overall probability of a widespread outage, including improving inter-carrier coordination for widespread outage recovery; clarifying who has the authority to resolve legal and regulatory impediments to the rapid and orderly restoration of service during such outages. These recommendations also encourage the Federal Communications Commission (FCC) to (a) ensure that local number portability (LNP) national standards and requirements, including NS/EP, are agreed upon and adhered to before implementing LNP on a widespread basis; (b) allow sufficient time to complete reliability, interoperability, and security testing of new services and products before implementing regulatory mandates; and (c) urge established entities and newer entrants to adhere to and help develop industry standards and best practices.

A "fresh look" is now being taken at the possibility of a widespread outage in the converging network environment in response to an October 2000 request by the Assistant to the President for Science and Technology.[19] Among the questions to be answered are (1) how should existing NSTAC, National Communications System (NCS)/NCC, and other private and Government organizations evolve with the networks to ensure a quick, organized, and technically competent response in the case of a widespread outage; and (2) what reasonable steps could the Government take to help the NSTAC, and industry in general, better prepare to react to a widespread outage in these networks? The preliminary analysis of NS/EP telecommunications in a converged network environment focused on its relative immaturity when compared with the legacy PSN. According to this analysis, NS/EP communications should utilize the converged network, but until complete confidence is established, the community should not rely exclusively on services based on converged networks. A formal interim report will be presented at the NSTAC XXIV meeting in June 2001.

Cross-Sectoral Assessments. An initial cross-sectoral assessment was undertaken in 1993 when an NSTAC Energy Task Force addressed the telecommunications electric service priority and national energy strategy review.[20] In January 1995, the Director of the National Security Agency briefed the NSTAC on threats to U.S. information systems and the need to improve the security of critical national infrastructures. In March, the NSTAC advised the President that "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk to intrusion and attack . . . other national infrastructures . . . [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."[21] Four months later, President Clinton "welcomed" the Advisory Committee's continuing efforts to work with the Administration in this area and asked for "input from the full range of national information infrastructure users" to assess the NS/EP requirements for the Nation's rapidly evolving information infrastructure.[22] Shortly thereafter, Presidential Decision Directive 39 was released. It directed the Attorney General to lead a governmentwide effort to reexamine the adequacy of the Nation's infrastructure protection.[23]

Building on the methodology developed by the Government and the NSTAC in the earlier risk assessments to the PN, information assurance (IA) risk assessments were conducted for the electric power infrastructure in March 1997,[24] financial services in December 1997,[25] and transportation in June 1999.[26] Extensive outreach was conducted with each of the sectors, and each infrastructure's dependency on information technology and the associated IA risks to its information systems were examined. Follow•up recommendations were sent to the President, many of which remain valid, and some of which appear applicable to other critical infrastructures. It is recommended that these assessments be referenced in the National Plan as models for developing sector-specific assessments.

National Plan Objectives: Detect and Respond

Identifying and assessing an attack in a timely way, and then containing the attack, quickly recovering from it, and affecting reconstitution requirements—the stated purpose of this objective—are functions presently being carried out by the NCC.

The NCC-Information Sharing and Analysis Center (ISAC). Established in 1984 to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications facilities and services, this coordinating mechanism's functions have since evolved in response to changes in technology and in the nature of threats to the telecommunications and information infrastructures. As previously discussed, the NCC's initial focus was on physical threats.

In response to a request from the Manager, NCS, in 1997, the NCC developed an indications, assessment, and warning response capability and began performing an electronic intrusion incident information processing function. During 1999, the NSTAC determined that the NCC was performing the primary functions of an ISAC for the telecommunications sector and recommended that industry and Government establish it as such. In January 2000, the National Security Council recognized the NCC as an ISAC;[27] and in March 2000, the NCC began initial operations as an ISAC for the telecommunications sector.[28] In this new role, the NCC-ISAC gathers information about vulnerabilities, threats, intrusions, and anomalies from the telecommunications industry, Government, and other sources, and then analyzes the data with the goal of averting or mitigating effects on the communications and information infrastructures. Results are sanitized and disseminated in accordance with information sharing agreements established by the NCC-ISAC participants. Cross-sector information sharing is also being explored.

In a “dry run” as an ISAC, the NCC served as the telecommunications sector’s focal point for the Nation’s Year 2000 (Y2K) activities. The findings and recommendations and lessons learned should prove helpful to other infrastructures as they develop their own ISACs.[29]

The NSIE Forum. The previously referenced NSIE process provides yet another capability for industry and Government sharing of sensitive information to further help reduce the vulnerability of the Nation’s telecommunications systems to electronic intrusion. However, whereas the NCC focuses on near real-time operational response to all-hazards, the NSIEs’ focus is on post-event analysis of threats to and vulnerabilities of networks.

National Plan Objective: Build Strong Foundations

This objective identifies “things we must do as a Nation to create and nourish the people, organizations, laws and traditions which will make us better able” to address the other two broad objectives—prepare and prevent, and detect and respond—to attacks on the critical information and communications sector.

Enhancement of R&D. The NSTAC has a long-standing interest in enhancing CIP-related R&D. Through its own studies and through public R&D exchanges among industry, Government, and academia, topics requiring study and funding have been affirmed and reaffirmed. The R&D Exchanges held in 1991, 1996, 1998, and 2000 are illustrative of the NSTAC’s outreach activities to improve cyber-security. More are likely to be held in the future. The NSTAC voiced a number of concerns that have yet to be resolved,[30] particularly:

- The lack of an overarching national technology policy that articulates a vision with respect to Federal intrusion detection R&D.
- The need for R&D focus on the network and infrastructure levels and on the establishment of testbeds and laboratories to develop standards, metrics, and testing procedures.
- The need to educate and train employees on recognizing intrusion and

heightening their awareness of the risks posed by electronic intrusion. This complements the National Plan's Outreach Program to Make Americans Aware of the Need for Improved Cyber-Security.

The need exists to offset the high costs and high risks associated with R&D in security technology (i.e., tax credits and other financial incentives might allow companies to minimize their risks and encourage commercial enterprises to increase the funding of security technology R&D).

During the two most recent R&D Exchanges, representatives from the academic sector played major roles; their contributions are reflected in many of the recommended areas for R&D.[31] Two of the recommendations complement the Federal National Plan's program to Train and Employ Adequate Numbers of Information Security Specialists:

- IA Centers of Excellence in academia should be supported and new ones established.
- Programs to create financial incentives for students to pursue computer security disciplines at the graduate and undergraduate levels need to be implemented, such as the Scholarship for Services Program under the Federal Cyber Service initiative. Current programs, rather than remaining concentrated on "respond and react" technologies, should consider the full range of risk management needs.

A third recommendation suggests that in seeking to build security solutions, it is vital to conduct research activities in other areas, such as operations, legal and public policy, and human factors.

Legislative Initiatives. Even though the NCC-ISAC is functioning, participants continue to express concerns with respect to the legal and regulatory barriers to voluntary information sharing, which is a linchpin of CIP.

Foremost among the legal impediments is the Freedom of Information Act

(FOIA), recognized from the outset as a barrier to voluntary information sharing. In preparation for the Y2K roll-over, the NSTAC recommended to the President that the then-pending *Y2K Information and Readiness Disclosure Act* be supported.[32] The legislation, which was enacted into law (Public Law 105-271), included a provision that information voluntarily shared with the Government is to be treated as part of a "special data gathering" and is therefore exempt from disclosure under FOIA. During the last session of Congress, the NSTAC wrote to the President and recommended support of FOIA legislation, similar to that in the Y2K legislation, relative to information voluntarily shared for CIP.[33] However, some member companies believe that a number of issues still need to be addressed and/or clarified in any new FOIA proposal.

Nevertheless, elimination of this barrier is but one of many issues that need resolution, in particular, antitrust, liability, the treatment of classified information and national security concerns, State government liability disclosure, and protection of trade secrets and proprietary information. Industry/Government dialogue in this area is needed.

Impediments to Information Sharing. Other barriers to information sharing should be addressed in the National Plan. The Government should review information sharing that is taking place in addition to that in the ISACs. Industry presently is being asked to share information, much of it the same, with Government through a number of other channels. Some companies may be reluctant to share information lest it be used to gain competitive advantage; individual participants may be reluctant as well. The voluntary information sharing processes of the NCC and the NSTAC NSIE have proven successful on a company disclosure basis. In other cases, remedies may include development of pertinent nondisclosure agreements among the participants. Anonymity based processes are starting to prove successful for larger groups. These factors should be taken into account in the development of ISACs.

Proposed New Broad Objective: International Considerations

Soon after the release of *An Agenda for Action* in the early 1990s,[34] the

Government started focusing on the development and expansion of the global information infrastructure (GII). Most recently, the NSTAC examined globalization.[35] The wide range of issues addressed included the current and future nature of the GII and the impact of the GII on NS/EP communications in 2010, the foreign ownership of NS/EP critical communications services systems, and technology export policies. Although no international issues were raised in Version 1.0, it is proposed that a new broad objective—International Considerations—be included in Version 2.0, as well as the following conclusions:

- Global Broadband Capabilities. NS/EP telecommunications capabilities in 2010 should be facilitated by a GII featuring new technologies and improved network features and by increased global availability of broadband communications, with satellite communications and wireless technologies bringing the GII and NS/EP communications to less accessible geographic regions. However, there is no guarantee that all essential communications capabilities will be ubiquitously available. It has been recommended to the President that prudent NS/EP communications contingency planning consider end-to-end systems using a broad range of wireless, satellite, and terrestrial capabilities, including operational tests. New technical and operational issues, including use of foreign Internet protocol based networks and NGN will likely need to be considered.

- Foreign Ownership. Increased foreign ownership and/or control of critical U.S. telecommunications facilities through which NS/EP services are provided is a significant. development. However, the current regulatory structure, including the regulatory review process established by the FCC, appears to be effectively accommodating the increasing levels and types of foreign ownership of U.S. facilities, while allowing the Government to retain the authority to prevent any such ownership from compromising national security interests. A Cabinet level interagency committee—the Committee on Foreign Investments in the United States—provides additional oversight in proposed mergers, acquisitions, or joint ventures involving a foreign entity. Based on the above, it has been recommended to the President that this review process remain adequate to protect NS/EP concerns.

- Export Controls. Technology export policies dealing with the transfer of strong encryption products, satellite technology, and high-performance computers are critical issues. But given that technology progresses faster than policy, industry and Government should continually evaluate the limits placed on technology exports.

Conclusions

No technology has been more responsible for the dramatic changes to the Nation's infrastructures than the technologies associated with the I&C sector. As the Nation and the Government become even more dependent on the telecommunications and information infrastructure, the role of NSTAC as an advisory body is taking on new dimensions. The cited reports, upon which this submission is based, can serve as a baseline for intensifying the dialogue as well as illustrating the type of analytic support the NSTAC's task force oriented process can provide. Specifically, we encourage the I&C sector, individual companies, and Government to continue to work together to—

- Protect the Nation's critical infrastructures, and
- Further the dialogue establishing a National Plan.

This dialogue should include discussion of one of the previously stated "Shared Challenges" that involves the different perspectives that industry and Government have regarding the threat to critical infrastructures. On the whole, industry believes it understands and is adequately mitigating the threat to its operations. At the same time, the Government has referred to an increased, hostile international threat to the critical national infrastructures; however, the nature of this threat is unclear. Without a clear and present danger, it is difficult for industry to justify spending additional dollars for augmenting protection of its systems.

Thus, beginning immediately, and at a minimum, the new Administration must continue the dialogue with industry and engage the NSTAC in order to cooperate on NS/EP issues critical to the Nation. It is key to resolution of future issues that the President and members of his new Administration attend NSTAC XXIV in June 2001. This will provide an opportunity for the President to frame and present his agenda for the ongoing issues of the NSTAC.

APPENDIX

SUMMARIES OF PREVIOUS NSTAC REPORTS

APPENDIX: SUMMARIES OF PREVIOUS NSTAC REPORTS

Introduction

Purpose of This Document

This Appendix supplies supplemental information, from previous reports of the President's National Security Telecommunications Advisory Committee (NSTAC),[36] to *The NSTAC's Response to the National Plan*. As a whole this document provides a guide to what the NSTAC believes are important points for consideration as the Nation develops a strategy for critical infrastructure protection (CIP). Because the environment has changed since many of the summarized studies were completed, the document's value should be understood in terms of the relevancy of the NSTAC's cumulative thinking and collective lessons learned to ongoing efforts; no new recommendations are offered. As an informational document, it is intended to demonstrate how the NSTAC process has worked to yield insights that can provide the basis for future actions in this arena.

Overview of the NSTAC

The President created the NSTAC by Executive Order 12382 in September 1982 to provide a unique source of national security and emergency preparedness (NS/EP) communications policy expertise. For over 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 Nation’s security requirements and information infrastructure evolve.

The principal NSTAC working body is the Industry Executive Subcommittee (IES). The IES meets regularly to identify issues, undertake analyses, and consider recommendations for presentation to the NSTAC. The IES forms ad hoc task forces to address specific policy, operational, or technical issues that require further substantive examination. This flexible working structure allows the NSTAC to proactively investigate issues as changes occur in the broader policy, technological, regulatory, business, and threat environments.

The NSTAC also collaborates with the Government through regular participation in the National Coordinating Center for Telecommunications (NCC), including its Information Sharing and Analysis Center (ISAC) component, and the Network Security Information Exchange (NSIE) process.

The NCC was established in 1984 as a result of an NSTAC recommendation to develop a joint industry/Government national coordinating mechanism to respond to the Federal Government’s NS/EP communications service requirements. The NCC’s mission is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities. Currently 15 NSTAC member companies are represented in the NCC.

The NSTAC was instrumental in formalizing the NCC's responsibilities to include functioning as an ISAC for the telecommunications infrastructure. Designated as an ISAC in January 2000, the NCC-ISAC was the second ISAC to be formed following the promulgation of Presidential Decision Directive 63 (PDD-63) and the only ISAC with both industry and Government membership. The NCC-ISAC gathers information about vulnerabilities, threats, intrusions, and anomalies from telecommunications industry, Government, and other sources, and then analyzes the data with the goal of averting or mitigating effects on the communications infrastructure. Results are sanitized and disseminated in accordance with sharing agreements established by the NCC-ISAC participants.

In 1991, the NSTAC, working with the National Communications System, recommended establishing an industry/Government partnership to reduce the vulnerability of the Nation's telecommunications systems to electronic intrusion. To that end, the NSIE process was established as a forum in which industry and Government could share information in a trusted and confidential environment. The NSIE process continues to function today, demonstrating that industry and Government will share sensitive security information if they find value in doing so. In 1998, PDD-63 called for the establishment of similar information exchange forums to reduce vulnerabilities in all critical infrastructures.

Background on NSTAC Activities As They Relate to Critical Infrastructure Protection and Information Assurance

The NSTAC has directly addressed information assurance (IA) and CIP issues since 1995. At the January 16, 1995, NSTAC XVII meeting, the Director of the National Security Agency briefed the NSTAC Principals on threats to U.S. infrastructures. In the ensuing months, the NSTAC sponsored a number of meetings with representatives from the national security community, law enforcement, and civil departments and agencies to discuss information warfare (defensive) and IA issues. At the May 15, 1995, NSTAC IES Working Session, the members established the Information Assurance Task Force (IATF) to serve as a focal point for IA issues. More specifically, the IES charged the IATF to work 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, March 18, 1997, the IES renamed the IATF the Information Infrastructure Group (IIG) and gave it the mission to continue acting as the focal point for NSTAC IA and infrastructure protection 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 to examine IA/CIP issues culminated with the release of presidential policy guidance—PDD-63. Recognizing that those infrastructures are predominantly owned and operated by the private sector, PDD-63 envisions the creation of a public-private partnership that is "genuine, mutual, and cooperative" to facilitate the elimination of vulnerabilities in the Nation's critical infrastructures. Subsequently, PDD-63 implementation became a focal point for the IIG's activities.

Applying its years of experience in joint industry/Government planning, the NSTAC initiated a dialogue with senior Administration officials on issues related to IA/CIP policy and the implementation of PDD-63. A key element was the need for public-private partnerships to address infrastructure vulnerabilities. Specifically, the NSTAC offered lessons learned in building joint mechanisms like the NCC and the Government and NSTAC NSIE. The IES, NCC, and NSIE provide the mechanisms and procedures for industry to address NS/EP telecommunications and information technology issues at the policy, operational, and technical levels respectively. The NSTAC also presented its recommendations to the President having applicability to PDD-63, including recommendations regarding an Information Systems Security Board (ISSB)[37] and the National Coordinating Mechanism (NCM)[38] concept.

NSTAC advice to the President and collaboration with the Administration have 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 (I&C) 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—the Information Technology Association of America, the Telecommunications Industry Association, and the United States Telecom Association—to serve as sector coordinators for the I&C sector.

PDD-63 also calls for the private sector to explore the feasibility of establishing one or more ISACs. On the basis of the December 1997 NSTAC XX recommendation regarding a cross•infrastructure NCM, 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 recognize the NCC as an ISAC for telecommunications. Subsequently, several sector-specific ISACs were created.

Finally, PDD-63 emphasizes the importance of relying on nonregulatory solutions to address infrastructure vulnerabilities. In satisfying this objective, the Administration has 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 an ISSB—a private sector entity intended to promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services.

At the June 9, 1999, NSTAC XXII meeting, the National Coordinator for Infrastructure Protection, Security, and Counter-terrorism asked the NSTAC to provide comments on the draft version of the *National Plan for Information Systems Protection* (National Plan). The IES reviewed the draft plan and provided general comments for the Administration's consideration. The comments were based on the NSTAC's long history of partnership with the Government and reflected input informally provided to the Director of the Critical Infrastructure Assurance Office earlier in 1999. Specifically, members recommended that a number of principles for partnership identified by the NSTAC be considered for inclusion in the National Plan. Some of these principles were incorporated into Version 1.0 of the National Plan, which the White House released on January 7, 2000. Reflecting the NSTAC's ongoing contributions to the development of CIP policy, the Department of Defense Infrastructure Assurance Plan—incorporated as part of the National Plan—specifically mentions the NSTAC as an industry/Government partnership model for exchanging information. The NSTAC is also further cited as an example of "industry commitment to . . . the public good," and of how industry can partner with Government to improve information security.

The NSTAC formed the Information Sharing for Critical Infrastructure Protection Task Force (ISCIPTF) in September 1999 to focus on information sharing issues associated with CIP. Specifically, the task force, among other things, continued interaction with Government leaders responsible for PDD-63 implementation, and examined mechanisms and processes for protected, operational information sharing that would help achieve the goals of PDD-63. Following a request by the National Coordinator for Infrastructure Protection, Security, and Counter-terrorism at the May 16, 2000, NSTAC XXIII meeting for additional NSTAC comments on Version 1.0 of the National Plan, the ISCIPTF drafted *The NSTAC's Response to Version 1.0 of the National Plan*, including this appendix.

Information and Communications (I&C) Sector Interdependencies

Profound changes in the Nation's infrastructures involving interdependency, deregulation, and reliance on technology are creating new challenges to the assurance of infrastructure services. A few particular infrastructures are so vital that their incapacity or destruction would significantly compromise the defense and economic security of the United States. No technology has been more responsible for this dramatic change and had a more profound effect on the other infrastructures than the technologies associated with the I&C infrastructure. The national critical infrastructure systems incorporate a mix of public and private ownership entities that bring to the table varying perspectives with regard to security, protection, and economic competitiveness. Private owners, faced with loss of revenue and loss of confidence by their customers, regulators, investors, and insurers, seek to restore revenue and customer confidence, satisfy regulators, document losses, and avoid liability. Governments focus on protecting national security, preventing future attacks, and identifying and punishing attackers. As a result of the dichotomy of interests, any solution to or recommendation for the protection of critical infrastructures requires the participation of private industry in concert with Government.

In January 1995, the Director of the National Security Agency briefed the National Security Telecommunications Advisory Committee (NSTAC) on threats to U.S. information systems and the need to improve the security of critical national infrastructures. Reflecting on that information, the NSTAC Principals discussed emerging threats to information systems and subsequently forwarded a correspondence on the matter to President Clinton in March 1995. It stated that "[the] integrity of the Nation's information systems, both government and public, are increasingly at risk to intrusion and attack . . . other national infrastructures . . . [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk." President Clinton replied to the NSTAC correspondence in July 1995, stating that he would “welcome NSTAC’s continuing efforts to work with the Administration to counter threats to our Nation’s information and telecommunications systems.” The President further asked the NSTAC, with “input from the full range of national information infrastructure users,” to assess the national security and emergency preparedness requirements for the Nation’s rapidly evolving information infrastructure. Through dialogue with Government, the NSTAC identified three priority critical infrastructures for assessment.

The NSTAC built on the methodology developed by the Government and the NSTAC Network Security Information Exchanges to assess the security risks to public networks. Using that methodology, the NSTAC began to study the electric power, financial services, and transportation infrastructures. Specifically, the NSTAC examined each infrastructure’s dependency on information technology and the associated information assurance risks to its information systems. The NSTAC completed the risk assessments of the electric power, financial services, and transportation infrastructures in March 1997, December 1997, and June 1999, respectively. In each assessment, follow-up recommendations were sent to the President, many of which remain valid, and some of which appear applicable to other critical infrastructures.

Information Assurance Task Force (IATF), Electric Power Information Assurance Risk Assessment, March 1997.

In March 1997, the NSTAC issued a report to the President that assessed the security of the electric power control networks and electric power grid. The NSTAC determined that the electric power industry was undergoing significant change, fueled by marketplace forces and Federal legislative and regulatory activities.

The NSTAC found that this change was stimulated by new players entering the power generation and delivery market and by existing utilities being required to offer open access to their transmission systems. The previously tightly integrated functions of power generation, transmission, and marketing were being separated within utilities; and some were even spinning off into new companies. Utilities were also rapidly expanding their use of information systems and interconnecting previously isolated networks because of competition, aging proprietary systems, and reductions in staff and operating margins.

The NSTAC recognized that, while physical destruction was still the greatest threat facing the electric power infrastructure, electronic intrusion of the utilities' information systems and networks represented an emerging threat. The NSTAC concluded that the probability of a nationwide disruption of electric power through electronic intrusion, short of a major coordinated attack, was extremely low, but the potential for short-term disruptions at the regional level was increasing. The NSTAC found that the industry considered the primary threat to information systems to be from insiders. Downsizing, increased competition, and the shift to standard protocols would add to the potential sources of attacks, whether from inside or outside a utility.

The NSTAC also examined recent legislation that had increased the jurisdiction of Federal, State, and local law enforcement authorities over attacks on electric power control systems. It found that the lack of effective reporting mechanisms, inconsistent use of logins, passwords, and warning banners, and a low probability of being detected, caught, and prosecuted hindered effective deterrence of potential attackers.

The NSTAC determined that the substations presented the most significant information security vulnerability in the power grid. The NSTAC also found that many of the automated devices used to monitor and control equipment within transmission and distribution centers and corporate data networks, widespread use of dial-up modems, and use of public networks were other sources of vulnerabilities in the electric power grid.

The NSTAC recognized that utilities used a variety of mechanisms to protect the electric power grid from disruption, including contingency analysis, redundant control centers, dial-back modems, and firewalls. However, few utilities had an information security function for their operational systems, and the lack of convincing evidence of a threat tended to lead senior managers to minimize information security investments.

Although the NSTAC's study found no evidence of a disruption of electric power caused by an electronic intrusion, it concluded that three trends would increase the exposure of the electric power control network to attack:

- The shift from proprietary mainframe control systems to open systems and standard protocols
- Increasing use of automation, outside contractors, and external connections to reduce staff and operating costs
- The requirement to provide open access to transmission system information dictated under Federal Energy Regulatory Commission orders 888 and 889.

The NSTAC included in its recommendation to the President that he consider assigning to the appropriate department or agency the mission to develop and conduct an ongoing program with the electric power industry to identify the threat and increase the awareness of vulnerabilities and available or emerging solutions.

IATF, Financial Services Risk Assessment Report, December 1997.

The NSTAC delivered a financial services Information Assurance (IA) risk assessment report to the President in December 1997. The study reflected that the financial services infrastructure was sufficiently protected and prepared, at the national level, to address a broad range of current threats, from natural disasters to electronic intrusions. However, the NSTAC found that there were security implications and potential vulnerabilities associated with the financial service sector's dependence on a 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 banking services.

The study focused on three objectives:

- Assess the security and robustness of the financial services infrastructure at the national level relative to the identified threats to its networks and information systems;
- Determine the risks to the industry that derive from its dependence on the telecommunications infrastructure; and
- Examine the implications of trends regarding the industry's use of information systems and networks.

The NSTAC found that the financial services industry approached the protection of its networks and information systems as an integral element of an overall program of risk-management accountable to the most senior levels of an institution. This approach is long established in the industry and affects every investment decision. The approach also incorporates security measures as fundamental risk controls.

The NSTAC concluded that trends in banking, securities, and new technologies indicated that information systems and networks would continue to be the primary vehicles for innovation and competition, enabling money, value, and related commerce to move with increasing velocity. It was further determined that, although the industry had suffered for its reluctance to discuss security issues in open forums through perceptions fostered by the media that the situation was far worse than it was, the financial institutions were very aware of the threats facing them. The financial institutions were also committed to any necessary investments in protection measures and had extensive experience addressing natural and man-made disasters and infrastructure outages. These measures taken by the industry put successful cyber attacks beyond the scope of all but a concerted nation-state effort. Physical attack remained the larger concern.

Information Infrastructure Group (IIG), Interim Transportation Information Risk Assessment Report, December 1997; IIG Transportation Information Assurance Risk Assessment Report, June 1999.

The NSTAC initiated its transportation IA risk assessment in December 1996.

The findings were included in an interim report to the President in December 1997. The report concluded that the transportation industry lacked a uniform understanding of information system risks and vulnerabilities, and the industry lacked consistent methods for assessing vulnerabilities or gauging information system security. The report also concluded that the transportation industry was generally skeptical that meaningful industry/Government information sharing about system threats and vulnerabilities could be achieved.

The NSTAC came to the following six conclusions about risks to the transportation infrastructure:

- The transportation industry is increasingly reliant on information technology (IT) and public networks.
- Although a nationwide disruption of the transportation infrastructure is unlikely, even a local or regional disruption could have a significant impact.
- Business pressures and widespread utilization of IT make large-scale, multimodal disruptions more likely in the future.
- There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.
- The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.
- There is a need for closer coordination between the transportation industry and other critical infrastructures.

The NSTAC recommended that the President continue support for the efforts of the Department of Transportation (DOT) to promote outreach and awareness within the transportation infrastructure as expressed in Presidential Decision Directive 63. These recommendations included the timely dissemination of Government information on physical and cyber threats, support for research and development programs to develop methods to counter emerging cyber threats, joint industry/Government efforts to examine emerging industry wide vulnerabilities, and future DOT conferences to stimulate information exchange on threats, vulnerabilities, and best practices.

Network Technology and Vulnerabilities

Since early 1990, the United States Government and the President’s National Security Telecommunications Advisory Committee (NSTAC) have been working together to address network security issues. Central to this process are separate, but closely coordinated Government and NSTAC Network Security Information Exchanges (NSIE). The activities of the NSIE focus on issues of unauthorized penetration or manipulation of the public network (PN) software and databases affecting national security and emergency preparedness (NS/EP) telecommunications services. The NSIE conducted risk assessments of the PN in 1995 and 1999.

More recently, the NSTAC undertook focused investigations of the vulnerabilities associated with the use of the Internet and electronic commerce technologies as they have become increasingly used to support NS/EP telecommunications functions. In addition, the NSTAC examined evolving network technologies and architectures, the implications for existing NS/EP priority services, and the potential for satisfying NS/EP functional requirements in the Next Generation Network (NGN) environment.

Government and NSTAC Network Security Information Exchanges (NSIE): An Assessment of the Risk to the Security of Public Networks, December 1995; Government and NSTAC NSIEs: An Assessment of the Risk to the Security of the Public Network, April 1999.

The NSIE’s most recent assessment of the risk to the PN determined that its earlier findings regarding the overall vulnerability of the PN remain valid. Old vulnerabilities are still being exploited, even though fixes are readily available for most of those discovered; vulnerabilities in many of the PN’s diverse technologies (e.g., Signaling System 7 [SS7] and Synchronous Optical Network) remain.

The following factors, summarized from the recent NSIE risk assessments, significantly heighten risk to the PN:

- **The Telecommunications Act of 1996:** The Telecommunications Act of 1996 opened the telecommunications industry to increased competition and interconnection. As more providers gain access to network facilities, security measures become more complicated and difficult to implement.

- **The Business Environment:** The telecommunications industry is a highly dynamic, fast-paced, global industry. Telecommunications organizations are increasingly adopting aggressive business practices to streamline operations and reduce costs. These business practices have increased the complexity of the PN, further increasing the difficulty of implementing network security measures. Additionally, the changing business environment and rapid integration of newer technologies have increased the vulnerabilities of the PN. The operations, administration, maintenance, and provisioning systems and network operations centers are highly integrated and are increasingly dependent on commercial-off-the-shelf technology. Potential intruders have ready access to information about these technologies and their vulnerabilities. This information is widely known and rapidly disseminated throughout the intruder community.

- **The threat to the PN continues to grow as the PN becomes a more valuable target and the intruder community develops more sophisticated capabilities to launch attacks against it:** Lately, the intelligence community has increased its efforts to focus on defining the electronic intrusion threat to the PN. Intruder tools continue to improve and have become widely available, as has information on vulnerabilities. The denial of service attacks in February 2000 provided additional evidence of malicious capabilities.

- **Technology:** Telecommunications providers are transitioning from proprietary protocols to open system protocols to manage their networks. In addition, traditional circuit switched services are migrating to packet switched networks. As this migration continues and new services, such as

Internet Protocol (IP) telephony, proliferate, the PN may become more susceptible to well-known Internet vulnerabilities.

- **Public Switched Network (PSN)/Internet Connectivity:** The Internet is rapidly converging with the PSN, increasing the opportunity for intruders to attack the PSN through the Internet.

- **Tools and Techniques:** Security tools and techniques have evolved significantly in the last few years, and the telecommunications industry is taking advantage of this evolution to improve the security of its networks. Similarly, network intrusion tools and techniques have also improved substantially; and the intruder community is using these tools and techniques to attack the PN.

The NSIE risk assessments found that as the PN has continued to expand, it has become an increasingly important part of the National Information Infrastructure. Government and corporate networks are more interconnected than ever before as these organizations increasingly rely on the PN to transmit critical business and operations information. Therefore, the perceived and substantive rewards for gaining illicit access to the PN are increasing, which makes protecting the PN more important than ever before:

- **Critical Infrastructure Protection:** Concern grows within Government and the private sector over critical infrastructure protection. As Government and the owners of critical infrastructures work to ensure the reliability and availability of their own systems, these efforts could improve the security of the PN.

- **Legislation:** Federal and State legislatures are addressing computer crime and imposing more severe penalties on electronic criminals, reflecting an increased awareness of the growing importance of the PN and the value of the information transported over its networks.

- **Government and industry organizations have worked diligently to**

improve protection measures: Technology and awareness are clearly improving, and service providers and vendors are becoming more knowledgeable and skillful in implementing protection measures. At the same time, several factors limit the effectiveness of protection measures. Service providers' knowledge of the entire network and, more important, ability to control the full extent of network connections are diminishing. Although technology protection measures, such as intrusion detection tools, have improved dramatically, their effectiveness is still inconsistent. Furthermore, the individuals with the technical skills required to effectively evaluate and implement these tools are in short supply.

- **Continuing trends in law enforcement have increased the ability of Government and corporate organizations to deter the intrusion threat:** The U.S. law enforcement community has developed a firm position on electronic intrusion. Intruders face more diligent prosecution efforts and can expect longer sentences if convicted. In addition, victims are gradually becoming more willing to report intrusions and cooperate with law enforcement.

The most recent NSIE risk assessment concluded that absent a valid baseline to establish quantitative measures of the risk to the PN from electronic intrusion, it is difficult to definitively state how risk has changed over the past few years. Rapid advances in technology and environmental factors have changed the vulnerabilities and threats facing the PN, making it difficult to protect against intrusions. At the same time, the importance of the PN and the value of information flowing over its networks are increasing, making the PN a more valuable target. Overall, according to the NSIE report, there is little evidence to suggest that the risk has diminished and a number of factors to suggest that it is growing.

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

As the Government expands its Internet use to more critical applications, such as supporting NS/EP functions, concerns arise about how a severe disruption of

Internet service might affect NS/EP operations. The NSTAC released the "Internet Report" in June 1999 to examine how a severe disruption of the Internet could affect NS/EP operations over the next 3 years, to identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, and to examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

The report concluded that agencies with NS/EP responsibilities are using the public Internet mostly for outreach, information sharing, and e-mail, while direct dependence on the public Internet for mission-critical operations is currently modest. The NS/EP community is more likely to depend on dedicated Transmission Control Protocol/ Internet Protocol (TCP/IP) networks (intranets) for mission-critical NS/EP operations at present. However, NS/EP dependence on the Internet is likely to grow over the next several years because the public Internet offers a cost-effective, efficient means of communications; the Government is rapidly adopting electronic commerce (e-commerce), and Federal policies are promoting use of the Internet. Currently, critical infrastructures, such as medical services, banking and finance, gas and electric industries, and telecommunications, are increasingly using the public Internet for various processes, including exchange of business, administrative, and research information.

The NSTAC also concluded that the informal and distributed management of Internet functions, the Domain Name System, Internet software including Berkeley Internet Name Domain, and procedural errors and unintentional actions invite potential vulnerabilities that could contribute to a disruption of Internet service. Because of the interconnected nature of the public Internet, a disruption or degradation of Internet operations could also affect the operations of dedicated TCP/IP networks/intranets. However, with the Internet's highly diverse architecture and complex interconnection arrangements, consisting of thousands of Internet service providers (ISP), it is *unlikely* that the failure of any single node or transmission facility would cause a major Internet service disruption (also see page 19 for follow-on efforts).

At present, the reliability and security of the public Internet is generally considered inadequate for NS/EP mission-critical functions. There are no Internet technologies or applications that facilitate the same type of end-to-end NS/EP-related services available in the PSN. Although certain ISPs currently offer in-network quality of service (QoS) standards, no end-to-end QoS offerings are available via the public Internet. No economical incentives exist for ISPs to develop and offer NS/EP service enhancements over their networks. A number of factors (e.g., lack of NS/EP demand and market characteristics) preclude the availability of NS/EP services over the Internet for the foreseeable future.

The NSTAC recommended that the President 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.
- Examine the potential impact of IP network-PSN Convergence on PSN-specific NS/EP priority services (e.g., Government Emergency Telecommunications Service and Telecommunications Service Priority).

The NSTAC also recommended that the President direct the appropriate Government departments and agencies to leverage of existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

Information Infrastructure Group (IIG), NS/EP Implications of Electronic Commerce Report, June 1999.

The public sector is in the midst of adopting system wide changes that will incorporate e-commerce into Government operations. In June 1999, NSTAC issued a report to discuss implications of incorporating e-commerce into business operations within the NS/EP community. To investigate this topic, the NSTAC surveyed e-commerce literature and received briefings from diverse Government, industry, and academic sources. They also interviewed public and private sector officials responsible for implementing e-commerce policies and procedures.

The NSTAC found that e-commerce use among NS/EP organizations has been limited to support of nonmission critical activities; but as these organizations increase their reliance on e-commerce operations for NS/EP functions, the security of these e-commerce transactions will become more critical. As the NS/EP community transitions, the NSTAC concluded that it should be alerted to a number of issues that could affect how e-commerce is implemented.

- NS/EP dependence on e-commerce, although modest at present, is likely to grow steadily over the next decade.
- It is important for the NS/EP community to be aware of the vulnerabilities that arise from utilizing e-commerce hardware and software and make informed decisions regarding their implementation to achieve an acceptable level of risk.
- It is important that NS/EP departments and agencies thoroughly assess current and future dependence on e-commerce application and architectures, the associated security implications, and the effect e-commerce will have on overall business operations.
- In the new electronic environment created by e-commerce, the NS/EP community will depend on commercial products and an information infrastructure that it neither owns nor operates. Therefore, the Federal Government and its partners in the private sector will share the NS/EP risks involved with e-commerce.
- There is a lack of unified and specific focus on NS/EP needs among organizations responsible for managing and administering oversight for e-commerce within the Federal Government. This lack of focus could lead to a lack of formal guidance, policy procedures, and accountability addressing

NS/EP issues related to the adoption of e-commerce.

The NSTAC concluded what is needed is a focal point within the Federal Government to work with the various public and private organizations to increase their awareness of NS/EP issues related to e-commerce. The NSTAC recommended that the President designate this focal point for examining the NS/EP issues related to widespread adoption of e-commerce within the Government. It was also recommended that the President direct the Federal departments and agencies, in cooperation with an established Federal focal point, to assess the effect of e-commerce technologies on their NS/EP operations.

The NSTAC also saw a need to increase the NS/EP community's awareness of the potential vulnerabilities related to e-commerce. Departments and agencies should work with the focal point to assess their current and future e-commerce dependence, and the vulnerabilities caused by e-commerce and its implementation.

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

The NS/EP community depends heavily on priority treatment of voice calls within the PSN to support NS/EP operations, which is provided under the Telecommunications Service Priority (TSP)[39] and the Government Emergency Telecommunications Service (GETS)[40] program. Telecommunications service providers plan to transition traffic onto the NGN. The NSTAC examined the implications of the evolving public network architecture for priority treatment of NS/EP voice and traffic data and, specifically, the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services. The NSTAC's report outlined the implications of convergence for existing NS/EP priority services and examined evolving network technologies and capabilities that could assist in satisfying existing NS/EP functional requirements in an NGN environment.

The NSTAC came to the following conclusions:

- The NS/EP community depends heavily on priority treatment of voice calls within the PSN to support NS/EP operations and will remain dependent for the immediate future.
- The public network will change from a separate switched voice and packet data networks to an interconnected network and then to a unified NGN over the next several years.
- The potential implications of Convergence and the NGN for GETS services include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and a lack of commensurate network reliability and security.
- NS/EP requirements are unlikely to be incorporated by industry unless the features needed to meet these requirements are standardized by industry, perhaps with prompting from the Government.
- NS/EP traffic requires newly designed and standardized features to overcome new problems associated with packet networks.
- To provide GETS-type services during Convergence and in the NGN, QoS schemes must be expanded to provide services commensurate with NS/EP needs.
- The current level of security safeguards incorporated into GETS is inadequate to maintain NS/EP functional requirements during Convergence and in the NGN.
- TSP, as originally conceived, remains relevant during Convergence because restoration assignments can still be applied to identifiable segments of the PSN.
- A potential implication for the TSP Program during Convergence and in the NGN as discussed by the TSP Oversight Committee (OC) is the inapplicability of the program to ISP offering voice services.
- The OC stated that TSP, as currently defined, did not and should not have a role in the NGN, and if the NS/EP community required similar types of priority services for packet networks, a new program would have to be established to support such services.
- TSP-type services in the NGN will provide for the priority provisioning and restoration of network services rather than circuit-based services.

- Although specific NGN standards have not yet been developed to support NS/EP requirements, the NGN technology is capable of supporting these requirements.
- Standards bodies are examining QoS and other new NGN capabilities that may be useful in satisfying certain NS/EP functional requirements in the NGN, and the appropriate departments and agencies should continue active participation in these groups.
- QoS and other new NGN capabilities will require some enhancement to best satisfy specific NS/EP requirements. Therefore, the NS/EP community should determine, as soon as practicable, precise functional NS/EP requirements for the NGN. The appropriate departments and agencies should continue to participate in standards bodies activities related to NGN technologies to ensure that NS/EP requirements are considered during development and implementation phases.
- As the NGN evolves, telecommunications carriers' SS7 networks will become less discrete and more reliant on IP technology and interfaces. Therefore, it is 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.

The NSTAC recommended that the President direct the appropriate departments and agencies, in coordination with industry, to promptly determine precise functional NS/EP requirements for convergence and the NGN, and ensure that relevant NS/EP functional requirements are conveyed to standards bodies and service providers during standards development and implementation.

Risk Management

Presidential Decision Directive 63 emphasizes the importance of relying on nonregulatory solutions to address infrastructure vulnerabilities. In satisfying this objective, the Critical Infrastructure Assurance Office has underscored the value of promoting industry standards and best practices to improve infrastructure assurance. That approach is entirely consistent with an NSTAC study initiated in

1995 and the resulting recommendation related to the creation of a private sector Information Systems Security Board (ISSB). The NSTAC developed the ISSB concept as a potential means for providing consistent, standardized guidelines for the protection of commercial information, systems, and networks.

National Information Infrastructure (NII) Task Force Report, February 28, 1996; National Information Infrastructure (NII) Task Force Report, March 1997.

During 1995, the NSTAC explored the concept of establishing an industry-operated security center of excellence as a potential focal point for enhancing the security component of the NII. The NSTAC identified several security functions considered important to improving NII security and appropriate for the private sector to perform. After scoping potential organizational models for an ISSB, the NSTAC concluded that a number of business issues should be considered to determine such an organization's viability.

In its in-depth follow-up study of the ISSB, which was completed in 1997, the NSTAC refined the concept and developed a model for an ISSB that could work with recognized testing laboratories and commercial security consulting services to strengthen the overall security of the information infrastructure. The NSTAC designed the model to promote information systems security principles and standards to improve the reliability and trustworthiness of commercial information products and services. To gain feedback from the broad community, an *Information Security Systems Board Concept Paper* was written to outline the functions and processes of the ISSB and serve as the centerpiece for the outreach effort. Attached to the concept paper was a questionnaire designed to stimulate discussion and elicit comments regarding the proposed ISSB concept, the need for an ISSB, an appropriate role for the Federal Government, and membership issues.

The NSTAC’s outreach effort revealed broad and general support for the ISSB concept among diverse industry groups. It also surfaced various questions and issues related to ISSB implementation, such as the appropriate role of the Federal

Government, the relationship of the ISSB to ongoing information security activities, and the international implications of the ISSB. The NSTAC concluded that the private sector was capable of establishing and operating the ISSB. Furthermore, both the private sector and Government expressed support for private sector leadership of the ISSB without Government oversight or control.

In response to additional NSTAC outreach, the private sector initiated an exploratory effort regarding the establishment of an ISSB; and the NSTAC continued to track its acceptance and progression within the community.

Response and Recovery

Based on a National Security Telecommunications Advisory Committee (NSTAC) recommendation, the National Communications System (NCS) established the National Coordinating Center for Telecommunications (NCC) in 1984 as a joint industry/Government mechanism to assist in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness (NS/EP) telecommunications services and facilities under all circumstances.

Since 1984, threats to the NS/EP telecommunications infrastructure have changed significantly. In response, the NSTAC undertook a series of studies to consider the implications of the new environment for the functions performed by the NCC. At the same time, the NSTAC revisited an earlier NSTAC concept—the National Coordinating Mechanism (NCM)—that could serve as a framework for responding to incidents across national infrastructures (e.g., electric power, financial services, and transportation). Separately, the NSTAC examined the possibility of a widespread outage in the public telecommunications network resulting from rapid changes in industry structure, regulation, and technology, as well as threat.

More recently, in October 2000, the Assistant to the President for Science and Technology requested the NSTAC to take a fresh look at the possibility of a widespread outage in the converged/Next Generation Network environment. Citing previous NSTAC work (the May 2000 NSTAC *Information Technology*

Progress Impact Task Force Report on Convergence), the request noted that convergence of voice and largely unregulated data networks will not only change the physical nature of the communications network, but may also introduce many new technical, operational, and security concerns.

Furthermore, the Assistant to the President for Science and Technology stated that these challenges may require Government to develop new policies, plans, programs, and perhaps protections under law or other mandates to help ensure the availability of NS/EP communications. Among the questions to be answered are (1) how should existing NSTAC, NCS/NCC, and other private and Government organizations evolve with the networks to ensure a quick, organized, and technically competent response in the case of a widespread outage; and (2) what reasonable steps could the Government take to help the NSTAC and the industry in general better prepare to react to a widespread outage in these networks? In November 2000, the NSTAC undertook a study to determine whether a widespread outage of the converged and next generation networks is a realistic possibility and the associated risk factors that the Government and industry need to consider. The preliminary analysis of NS/EP telecommunications in a converged network environment focused on its relative immaturity when compared with the legacy PSN. According to this analysis, NS/EP communications should utilize the converged network, but until complete confidence is established, the community should not rely exclusively on services based upon converged networks. The Convergence Task Force will explore the issue further. The NSTAC will provide an interim report to the Administration at the NSTAC XXIV meeting in June 2001.

Operations Support Group (OSG) Reports of December 1997, September 1998, and June 1999.

In 1996, the NSTAC began to examine whether the mission, organization, and capabilities of the NCC were still valid, considering the ongoing changes in technology, industry composition, threats, and requirements. Throughout 1997 the OSG worked closely with the NCS member organizations and NCC industry representatives to develop a common framework for assessing the NCC's ongoing role. The OSG validated the original 10 NCC chartered functions and updated the *NCC Operating Guide* (both written in 1984) for the current operational environment. Also—in response to a request for assistance from the Manager, NCS, to develop an indications, assessment, and warning (IAW) response capability in the NCC—the group determined that an electronic intrusion incident information processing function could be integrated into the NCC's activities. In August 1997, the group held an industry/Government tabletop exercise to test the draft concept of operations for the NCC intrusion incident information processing. In December 1997, the NSTAC approved the OSG report, which documents these activities, and endorsed the NCC's implementation of an initial intrusion incident information processing pilot program to develop the IAW function.

The OSG worked closely with the Office of the Manager, NCS, in 1998 as the NCC implemented the IAW pilot, which was completed in October 1998. In addition, the OSG developed a document, *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. On the basis of the experience of the pilot and the work of the NSTAC's OSG, the NCC decided to fully incorporate the IAW function into its operations.

In its September 1998 report, 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. Based on that finding, the NSTAC recommended that lead departments and agencies, as designated in Presidential Decision Directive 63 (PDD-63), consider adopting the NCC model, as appropriate, for the various infrastructures to provide warning and information in response to cyber incidents. Furthermore, the NSTAC recommended that such activities take place in the context of the NCM concept developed by the OSG. The OSG refashioned the original NCM concept developed by the NSTAC to coordinate planning, information sharing, and resources in response to NS/EP requirements. Unlike the original NCM plan that applied to the telecommunications infrastructure (and which led directly to the establishment of the NCC in 1984), the revised NCM concept involved linking all the Nation's critical infrastructures.

The OSG continued to assist the NCS and the NCC as the NCC implemented its pilot electronic intrusion incident processing function. The group also assessed whether the NCC required additional industry and Government participation within the NCC to widen the scope of expertise and operational personnel available to fulfill the IAW mission. Specifically, the group developed a list of companies and Government departments and agencies for the Manager, NCS, to consider as candidates for NCC participation.

After further efforts during 1999, the NSTAC agreed with the OSG determination that the NCC was performing the primary functions of an Information Sharing and Analysis Center (ISAC) for the telecommunications sector and concluded that industry and Government should establish it as such. PDD-63 proposed the concept of an ISAC as 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. In January 2000, the National Security Council agreed with the NSTAC's 1999 conclusion that the NCC was serving as an ISAC. Following this, the NCC formally announced its operation as an ISAC for the telecommunications sector.

Throughout the period from 1997 to 1999, the OSG also investigated the NCC's operational readiness and coordination capabilities for potential public network disruptions caused by the Year 2000 (Y2K) problem. Among other things, it examined 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 issues that were international in scope. The findings and recommendations related to these efforts are included in the OSG's final reports. Lessons learned from the NCC Y2K experience that could advance operational information sharing were examined by the NSTAC's Information Sharing/Critical Infrastructure Protection Task Force and are discussed in the task force's May 2000 report.

Network Group, Widespread Outage Subgroup (WOS) Report, December 1997 and
Network Group Report, September 1998.

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, requested that Mr. Charles Lee, then Chairman of the President's NSTAC, provide the NSTAC's forward-looking views on the possibility of a widespread service outage in the public telephone network.

The NSTAC defined widespread outage as a sustained interruption of telecommunications service that would have strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country, including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would impact the availability and integrity of telecommunications service for at least a significant portion of a business day.

The NSTAC found that U.S. telecommunications service providers have historically offered robustness, availability, and quality unparalleled by other public services. Although the public network (PN) track record is superlative, members determined that natural and technological threats could adversely affect telecommunications service. These threats could also disrupt other critical infrastructures, such as electric power, on which the PN is highly dependent for sustained operation. The NSTAC found that, while the PN's supporting technologies provide an expanding array of services and features and facilitate robustness, these same supporting technologies can introduce exploitable vulnerabilities with adverse effects on service availability and reliability. Considering these threats and vulnerabilities, the NSTAC agreed that the potential concern for a widespread network outage is reasonable. Given the limited precedent for telecommunications outages of this magnitude, NSTAC members' prior experiences with smaller-scale outages led them to conclude that there is a *low probability* of a widespread, sustained outage of public telephone service. However, the potential societal impacts of such an outage are high enough to warrant consideration.

The NSTAC offered recommendations for the President to decrease the overall probability of a widespread outage, including:

- improve inter-carrier coordination for widespread outage recovery.
- remove legal and regulatory obstacles to widespread outage recovery.
- foster education and awareness.

Subsequently, in a 1998 follow-up study of the issue, the NSTAC reached the following conclusions:

- The greatest opportunity for ensuring the continued reliability of the PN will ensue as both established entities and newer entrants adhere to and help develop industry standards and best practices.
- The focal point for industry/Government coordination for operational matters has been and should remain at the NCC. The NCC has initiated an effort to expand the National Telecommunications Coordinating Network to improve communications capabilities with critical entities during network outage conditions.

Information Sharing

The Information and Communications (I&C) sector has numerous forums for sharing policy, operational, and technical information. The President's National Security Telecommunications Advisory Committee (NSTAC) and associated industry/Government entities have served as models for information sharing for many years. Other new forums are being developed specifically in response to Presidential Decision Directive 63 (PDD-63), *Critical Infrastructure Protection*. By developing national security and emergency preparedness (NS/EP) telecommunications recommendations for the President, the NSTAC has provided, since 1982, a forum for developing and sharing policy information. The National Coordinating Center for Telecommunications (NCC) provides a forum for sharing operational telecommunications information among the industry and Government agencies participating in the NCC. The industry and Government Network Security Information Exchanges (NSIE) were established in 1991 for the purpose of exchanging lessons learned and technical information related to network security. Recently, the NSTAC has been investigating information sharing issues as they relate to critical infrastructure protection and network security. As one of the results of these ongoing studies, the NSTAC recommended and the NCC has been designated as an Information Sharing and Analysis Center (ISAC) within the framework of PDD-63 (see Attachment A, NCC ISAC, at the end of this section). Additionally, Congress, the Justice Department, and others are actively considering legislation designed to encourage industry NS/EP disclosures by exempting that information from release under the Freedom of Information Act (FOIA). The NSTAC has written to the President of the United States asking him to support such legislation, particularly legislation like the FOIA exemption in the *Year 2000 (Y2K) Information and Readiness Disclosure Act*. In addition, an initial outline has been developed discussing the types of provisions that FOIA legislation should include and that might best encourage industry sharing of NS/EP information.

Information Sharing/Critical Infrastructure Protection (IS/CIP) Task Force Report, May 2000.

A focal point of the NSTAC's report to the President was an examination of historical lessons learned that would advance operational information sharing in the context of critical infrastructure protection.

Benefits of Information Sharing. The NSTAC recognized that, historically, information sharing and the resulting benefits have been a function of trust. Information exchange in a trusted environment, which may be achieved only gradually, helps both industry and Government participants build on lessons learned by others. As trust builds, participants in information sharing forums may make more detailed information available. With such information, both industry and Government can strengthen security and prevent or mitigate the damage caused by future incidents or attacks. The process may also facilitate information sharing across critical infrastructures.

The NSTAC determined that specific benefits could accrue to both industry and Government. Government will be better able to determine the nature of the threat facing the Nation's critical infrastructures today and in the future through joint industry/Government information sharing initiatives. By combining private sector information about the type of incidents and attacks that are experienced with information obtained through intelligence and law enforcement sources, Government participants may develop warnings and advisories that can also assist other departments and agencies in the Federal, State, and local governments; the critical infrastructures; and security organizations in protecting their own systems and responding to incidents.

Conversely, partnering with Government may allow industry to obtain more detailed threat information. As Government provides to the private sector indications and warnings and information on specific threats facing the Nation, companies may develop a better understanding of the threats facing their particular infrastructure and may be willing and able to take further action to protect the sector. Access to Government threat-related information through information sharing initiatives may increase the opportunity for the private sector to determine where it will get the "most bang for its security buck."

Impediments to Information Sharing. The NSTAC investigated several impediments to information sharing, including legal, perceived, and operational.

Legal Impediments. Foremost among the legal impediments examined by the task force was the FOIA. In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) recognized the need for voluntary information sharing and identified the FOIA as a barrier to the information sharing process. The rationale was FOIA makes information sharing in the possession of the Federal Government available to the public upon request. As a result, and as noted by the PCCIP, potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential if shared with the Federal Government. More recently, Congress, at the urging of industry and Government, recognized that FOIA might be a barrier to voluntary information sharing in preparation for and during the Y2K roll-over.

Based upon its finding that protection of voluntarily shared information must be provided, the NSTAC recommended to the President that the then-pending *Y2K Information and Readiness Disclosure Act* be supported. The legislation, which was enacted into law (Public Law 105-271), contained a provision to protect information that is voluntarily shared with the Government. That information is to be treated as part of a “special data gathering” from disclosure under FOIA.

Both the Y2K experience and PDD-63 have raised awareness about the sensitivities of information sharing processes. However, in the context of PDD-63, critical infrastructures are being asked to share information for a longer duration and under less defined conditions than previously experienced during Y2K. Consequently, the NSTAC concluded that for PDD-63 information sharing initiatives to be fully implemented, protection of voluntarily shared information from disclosure under FOIA must be provided. As a result, the NSTAC recommended that the President support legislation similar to the *Y2K Information and Readiness Disclosure Act* for the purposes of information sharing for critical infrastructure protection.

Perceived impediments. Perceived impediments generally relate to the difference in perspectives between industry and Government regarding the threat to critical infrastructures. On the whole, industry believes it understands and is adequately mitigating the threat to its operations. At the same time, the Government has referred to an increased, hostile international threat to the critical national infrastructures; however, this threat is unclear. The NSTAC found that without a clear and present danger, it is difficult for industry to justify spending additional dollars to protect systems that may never be attacked. The NSTAC also found that an additional perceived impediment was the view that information shared between competing companies may be used to gain business advantage over the company willing to share information on operational difficulties.

Operational Impediments. Industry shares information using several channels. Providing the same information to multiple entities places demands on corporate resources. By designating one forum as a repository for information related to a particular industry sector, the demands placed on a company for information sharing should be reduced. As an ISAC for telecommunications, the NCC is positioned to serve as that forum through which industry and Government can share telecommunications indications, assessment, and warning information. The NCC, as a coordinating entity, could then forward information, in an agreed-on form, to other appropriate bodies (e.g., other ISACs, the National Infrastructure Protection Center, and the Computer Emergency Response Team Coordination Center) as permitted under information sharing agreements.

Legislative and Regulatory Group (LRG) Report, June 1999.
Following NSTAC XXI and in response to information sharing policy outlined in PDD-63, the NSTAC set out to identify and assess legal and regulatory obstacles to sharing outage and intrusion information. To that end, the NSTAC determined that identification and discussion of existing and proposed NS/EP-related outage and intrusion information sharing mechanisms could provide additional insights in assessing critical infrastructure protection issues. To better understand the information sharing environment and the entities involved in the process, the NSTAC developed a document (titled *Telecommunications Outage and Intrusion Information Sharing Report* and included in the LRG's 1999 report to the President) illustrating the entities with which telecommunications companies shared outage and intrusion information.

The LRG also reviewed potential legal barriers that could inhibit the information sharing process. The major barriers studied by the group included those associated with FOIA, liability, and antitrust. The NSTAC also examined several other potential barriers initially identified by the PCCIP, including those associated with classified information and national security, State government liability disclosure, confidential information, and trade secrets and proprietary information.

The NSTAC drew general conclusions in the following areas:

- Information sharing occurs in a number of forums.
- Legal barriers may affect information sharing.
- Information sharing is mostly voluntary.
- Voluntary information sharing is dependent on receiving a benefit.
- Information sharing is based on trusted relationships.
- Information sharing may be dependent on the company and individual participant.
- Information sharing is content-focused.

ATTACHMENT A
NCC-ISAC

(excerpted from the NSTAC's *IS/CIP Task Force Report, May 2000, Appendix D*)

NSTAC Recommended Input To The National Plan

The following text is recommended for inclusion in subsequent versions of the National Plan. The text addresses the designation and implementation of the National Coordinating Center for Telecommunications as an Information Sharing and Analysis Center for telecommunications.

National Coordinating Center for Telecommunications

In response to a National Security Telecommunications Advisory Committee (NSTAC) recommendation, the National Coordinating Center for

Telecommunications (NCC) was established and began operations on January 1, 1984, as a joint industry/Government National Coordinating Center capable of assisting in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness (NS/EP) telecommunications services and facilities under all conditions of crisis or emergency. Subsequent to beginning operations, the NCC was formalized on April 3, 1984, when President Reagan signed Executive Order 12472, *Assignment of NS/EP Telecommunications Functions.*

This joint industry/Government center facilitates information sharing between industry and Government through the following functions as identified in the industry/Government approved Charter:

- promptly provide technical analysis and damage assessment of service disruptions and identify necessary restoration actions,
- coordinate/direct prompt restoration of telecommunications services in support of NS/EP needs,
- develop and exercise comprehensive service restoration plans,
- develop watch center type functions to work through cooperating industry operation centers to effectively monitor the status of essential telecommunications facilities,
- maintain access to an accurate inventory of the minimum essential equipment, personnel, and other resources that are available for restoration operations, including the location and capabilities of all industry’s network operations centers,

- identify liaison points in each company,
- maintain ability to rapidly transfer operations from normal to emergency operations,
- coordinate/direct and expedite the initiation of NS/EP telecommunications services,
- contribute to the development of technical standards and national network planning and ensure application of those standards and dissemination of those plans to facilities serving NS/EP needs, and
- coordinate/direct network reconfiguration plans in support of NS/EP needs.

The NCC's role in fulfilling its charter functions began to evolve in the changing environment following the end of the Cold War and as the Administration determined that national security includes economic security. In 1996, the NCC began to develop an indications, assessment, and warning (IAW) capability. The NSTAC concluded that the IAW capability was within the scope of the NCC Charter, and in 1998 directed the NCC conduct an IAW pilot project. Lessons learned from the pilot project were incorporated into the NCC's ongoing operations.

Following the issuance of Presidential Decision Directive (PDD) 63, *Protecting America's Critical Infrastructures,* in May 1998, the NSTAC concluded that the NCC performs the primary functions of an Information Sharing and Analysis Center (ISAC) in the context of PDD-63. The National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism agreed in a memorandum dated January 18, 2000.

The NCC is unique as an ISAC. It is a joint industry/Government organization located in the Office of the Manager, National Communications System and staffed by both industry and Government. Information sharing between industry and Government has been taking place in a trusted environment over the past 16 years in the NCC. A phased implementation plan, developed by both industry and Government, will address expanded participation, NCC activities, and external coordination to achieve full operating capability.

Research and Development (R&D) Needs

Over the years, the President's National Security Telecommunication Advisory Committee (NSTAC) has investigated several R&D issues as they relate to the national security and emergency preparedness (NS/EP) telecommunications infrastructure. Recent issues focused on R&D for intrusion detection technologies and technologies that address telecommunications infrastructure vulnerabilities. The NSTAC has also sponsored several R&D Exchanges to surface issues and needs related to the security of the telecommunications infrastructure.

Network Group, Intrusion Detection Subgroup (IDSG) Report, December 1997. In 1997 the NSTAC conducted a study of intrusion detection technology R&D that included an examination of existing and planned intrusion detection technology R&D initiatives and provided analysis in terms of meeting NS/EP requirements. The NSTAC determined that there was no overarching national technology policy that articulated a vision with respect to Federal intrusion detection R&D. The NSTAC concluded that R&D in this area should focus on the network and infrastructure levels and establishing testbeds and laboratories to develop standards, metrics, and testing procedures. It was found that there existed a need for Federal investment in educating and training employees on recognizing intrusion and heightening their awareness of the risks electronic intrusion involves.

NSTAC R&D Exchanges.

The first R&D Exchange, sponsored in 1991, was intended to provide a forum for industry and Government officials to discuss six technology areas identified by the NSTAC and to exchange information about ongoing R&D projects. The theme for the two-part event was intrusion detection. The NSTAC held the second R&D Exchange in September 1996 to facilitate a common understanding of network security problems affecting NS/EP telecommunications, to identify R&D programs in progress to address those problems, and to identify future security technology R&D needs. Participants focused on the issue of academic excellence in information assurance (IA). Then, in October 1998, the NSTAC co-sponsored the third R&D Exchange to examine collaborative approaches to security technology R&D. The participants also discussed the need for training more information technology (IT) security professionals, creating large-scale test beds to test security products and solutions, and promoting the creation of IA Centers of Excellence in academia.

NSTAC R&D Exchange Proceedings, 2000.

In September 2000, the NSTAC sponsored its fourth R&D Exchange in conjunction with the Telecommunications and Information Security Workshop (TISW) 2000 at the University of Tulsa. The theme for the 2-day event was "Transparent Security in a Converged and Distributed Network Environment: A Dream or a Nightmare?" The purpose was to stimulate an exchange of ideas among representatives from industry, Government, and academia on the challenges posed by the convergence of the traditional public switched network and the Internet into a Next Generation Network (NGN).

The general conclusion of the R&D Exchange was that the challenges to securing networks in a converged and distributed environment grow more difficult. Further, those challenges require a greater deal of cooperation among network providers, vendors, and users. More specifically, the participants concluded that:

- The shortage of qualified IT professionals, particularly those with expertise in IA and/or computer security, remains a major impediment to strengthening the security of the NGN. The participants believed programs, such as the Scholarship for Services program under the Federal Cyber Service initiative and others designed to create financial incentives for students to pursue computer security disciplines at the graduate and undergraduate levels, need to be implemented.

- The IA Centers of Excellence program is an excellent initiative to address the growing demand for computer security professionals but needs to be expanded beyond the current 14 schools. Moreover, a need exists to make information about the IA Centers of Excellence and other IA curricula and certifications available to other schools, such as community colleges and technology trade schools. In addition, participants encouraged cyber ethics training at the K-12 level.

- The Partnership for Critical Infrastructure Security represents an important step in enhancing the relationship between the private sector and the Government, but wider participation by academia and officials in State and local governments is needed.

- Developing a business case for security poses difficult challenges in the commercial sector, and there is a need to offset the high costs and high risks associated with R&D in security technology. Tax credits and other financial incentives might allow companies to minimize their risks and encourage commercial enterprises to increase the funding of security technology R&D.

- Given the complexity introduced to networks by convergence and the proliferation of network providers and vendors, best practices, standards, and protection profiles that ensure security must be evenly applied across the NGN.

- There is a need to enhance R&D efforts to develop better testing and evaluation programs to reduce the vulnerabilities introduced by malicious software. While securing the transmission of voice and data remains an important concern, it is equally important to identify security vulnerabilities in the network control space.

- New types of threats, such as distributed denial of service attacks, challenge corporations to develop security policies to protect themselves from liability claims. For example, new legal precedents, case law, and Federal legislation, such as the Health Insurance Portability and Accountability Act of 1996, are forcing organizations to take new security measures to protect the confidentiality and integrity of information or risk civil litigation.

- Although technology remains an important component in building security solutions, it is vital to conduct research activities in other areas such as operations, legal and public policy, and human factors. The efficacy of technological solutions is often dependent on the ability of human operators to properly implement, administer, and manage the technology consistent with company policy and the legal constraints.

- There is a need to sponsor joint events like TISW 2000 and the R&D Exchange that facilitate a dialogue among representatives from industry, Government, and academia. All three communities play a crucial role in the R&D of security technologies and applications, and participants described how holding events at universities with IA programs offered unique benefits. Most notably, such events allow security practitioners from industry, Government, and academia to share views and opinions on R&D issues in an informal, research-oriented setting.

International Considerations

In the early 1990s, the Government recognized the growing importance and criticality of the information infrastructure. With the release of *An Agenda for Action*, the Administration promoted a national strategy to develop a robust, accessible, and reliable information infrastructure that would satisfy the national and economic security interests of the United States. Since that time, growing competition and technological innovation have resulted in a national and global, interconnected, open information infrastructure that offers commercial efficiencies and societal benefits.

Soon after the release of *An Agenda for Action*, the Government focused on the ongoing development and expansion of the global information infrastructure (GII). Although the expansion of the GII and the globalization of communications and information technology generate obvious economic and societal benefits, they pose new risks for critical infrastructures and services. The mitigation of these risks is necessary for the protection of our Nation's and our allies' critical infrastructures. The President's National Security Telecommunications Advisory Committee (NSTAC) has studied the current and future nature of the GII and investigated the impact of the GII on national security and emergency preparedness (NS/EP) communications. Although international considerations were not a part of Version 1 of the National Plan, NSTAC would like to include discussion of them to help further the dialogue between industry and Government concerning critical infrastructure protection issues.

Globalization Task Force (GTF) Report, May 2000.
The NSTAC studied several international issues in its May 2000 report to the President. These included NS/EP issues related to the GII in 2010, foreign ownership of NS/EP critical communications systems, and technology export policies.

The NSTAC concluded that in 2010, NS/EP communications would be facilitated by a GII featuring new technologies and improved network features. The GII in 2010 would also provide increased global availability of broadband communications, with satellite communications and wireless technologies bringing the GII and NS/EP communications to less accessible geographic regions. However, despite the plethora of technological capabilities forecasted for 2010, there is no guarantee that all essential communications capabilities will be ubiquitously available. Given the global reach and communications needs of some U.S. NS/EP missions, prudent NS/EP communications contingency planning should consider end-to-end systems using a broad range of wireless, satellite, and terrestrial capabilities.

The NSTAC also concluded that, in addition to planning for the global availability of the GII in 2010, the Government must consider the richness of service envisioned in the future network architecture and decide whether NS/EP communications will require quality of service features beyond commercially available capabilities. Any, and perhaps all, the potential protocols of 2010 could be considered candidates for hosting NS/EP requirements. Thus, the Government must continue being proactive in its attempts to cooperate in developing industry standards and technical specifications for next-generation and Internet Protocol-based networks.

The NSTAC also examined the implications of foreign ownership of critical U.S. telecommunications facilities on NS/EP services. The NSTAC developed a scoping paper on the issue and concluded that the current regulatory structure effectively accommodated increasing levels of foreign ownership of U.S. telecommunications facilities, while allowing the Federal Government to retain the authority to prevent any such foreign ownership that might compromise national security interests.

In addition, the NSTAC examined technology export policies dealing with the transfer of strong encryption products, satellite technology, and high-performance computers. The NSTAC compiled basic information about key technology export issue areas and monitored the implementation of new export policies and regulations. The NSTAC also investigated the development of guidelines to assist companies in understanding Government approval of technology sales. The NSTAC concluded that because technology progresses faster than policy, industry and Government should continue to reevaluate the limits placed on the export of technologies.

---

[1] The NSTAC, established by Executive Order 12382 in September 13, 1982, is composed of chief executive officers (CEO) who participate on a pro bono basis. The NSTAC has established the Industry Executive Subcommittee (IES) to support its activities. The IES, in turn, has established ad hoc task forces and working groups to address issues. The NSTAC also collaborates with Government through regular participation in the National Coordinating Center for Telecommunications (NCC), the NCC Information and Analysis Center (ISAC), and the Network Security Information Exchanges (NSIE). See p. 4 and Appendix, p. A-2, for a discussion of the NCC, NCC-ISAC, and NSIEs.

[2] The PN is defined as any switching system or voice, data, or video transmission system that is used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks).

[3] The PSN is defined as any common carrier network that provides circuit switching among public users.

[4] The NGN is a public, broadband, diverse, and scalable packet-based network evolving from the PSN, the advanced intelligent network (AIN), and the Internet. The NGN is characterized by a core fabric enabling network connectivity and transport with periphery-based service intelligence.

[5] The NSTAC's work is based on a process that enables the formation of interdisciplinary task forces to focus on issues that require operational, technical, policy, and regulatory analysis and recommendations in a timely manner.

[6] Convergence indicates a process over a 3- to 5-year period of NGN evolution during which traditional circuit-switched networks (including AIN) and Internet protocol (IP) based data networks will coexist and interoperate to enable end-to-end transmission of voice communications, until IP based networks subsume circuit-switched networks.

[7] See Appendix, p. A-2, for a discussion of the development of the NCC and the NSIEs.

[8] National Plan Version 1.0, Executive Summary, p. xviii.

[9] See Appendix, p. A-11, for summary of *Government and NSTAC NSIE: An Assessment of the Risk to the Security of Public Networks*.

[10] See Appendix, p. A-11, for summary of *Government and NSTAC NSIE: An Assessment of the Risk to the Security of the Public Network.*

[11] See Appendix, p. A-13, for summary of *An Examination of the NS/EP Implications of Internet Technologies*.

[12] See Appendix, p. A-15, for summary of *NS/EP Implications of Electronic Commerce Report*.

[13] GETS provides NS/EP users priority access to and specialized processing for NS/EP calls in local and long distance networks.

[14] The TSP Program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service.

[15] See Appendix, p. A-16, for summary of *Information Technology Progress Impact Task Force Report on Convergence*.

[16] April 24, 1997, letter from Dr. John Gibbons, Assistant to the President for Science and Technology, to Mr. Charles Lee, NSTAC Chair, concerning the possibility of a widespread outage affecting the public telephone network.

[17] See Appendix, p. A-23, for summary of *Widespread Outage Subgroup Report, 1997*.

[18] See Appendix, p. A-23, for summary of *Widespread Outage Subgroup Report, 1998*.

[19] October 24, 2000, letter from Dr. Neal Lane, Assistant to the President for Science and Technology, to Mr. Daniel Burnham, NSTAC Chair, concerning the possibility of a widespread outage of the converged network and NGN.

[20] *Energy Task Force Report*, NSTAC XV, May 1993. More recently, the Network Reliability and Interoperability Council has adopted the telecommunications electric service priority recommendation as part of its best practices.

[21] March 20, 1995, letter from Mr. William Esrey, NSTAC Chair, to President Clinton, regarding the security of the national information infrastructure (NII).

[22] July 7, 1995, letter from President Clinton to Mr. William Esrey, NSTAC Chair, regarding the security of the NII.

[23] *U.S. Policy on Counterterrorism*: PDD-39, July 21, 1995.

[24] See Appendix, p. A-7, for summary of *Electric Power Information Assurance Risk Assessment*.

[25] See Appendix, p. A-8, for summary of *Financial Services Risk Assessment Report*.

[26] See Appendix, p. A-9, for summaries of *Interim Transportation Information Risk Assessment Report* and *Transportation Information Assurance Risk Assessment Report*.

[27] January 18, 2000, letter from Mr. Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counter-terrorism, to Mr. Art Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence regarding the designation of the NCC as an ISAC.

[28] See Appendix, p. A-29, Attachment A, National Coordinating Center for Telecommunications.

[29] See Appendix, p. A-25, *Information Sharing/Critical Infrastructure Protection Task Force Report.*

[30] See Appendix, p. A-31, for summary of *NSTAC R&D Exchange Proceedings*.

[31] See Appendix, p. A-31, for summary of *NSTAC R&D Exchange Proceedings*.

[32] September 18, 1998, letter from Mr. Van B. Honeycutt, NSTAC Chair and CEO, Computer Sciences Corporation, to the President recommending the President support the *Y2K Information and Readiness Disclosure Act*.

[33] August 7, 2000, letter from Mr. Van B. Honeycutt, NSTAC Chair and CEO, Computer Sciences Corporation, to the President recommending the President support legislation similar to the *Y2K Information and Readiness Disclosure Act*.

[34] *An Agenda for Action*, September 15, 1993.

[35] See Appendix, p. A-34, for summary of *Globalization Task Force Report*.

[36] Copies of reports can be obtained via the World Wide Web at *www.ncs.gov* or from the Office of the Manager, National Communications System, Customer Service Division, 701 S. Courthouse Road, Arlington, VA 22204-2198.

[37] In 1997, the NSTAC finalized the concept and model for an ISSB—a private sector entity intended to improve the common understanding of the nature and purpose of information systems security. The ISSB would promote information systems security principles and standards to improve the reliability and trustworthiness of commercial information products and services.

[38] In 1997, the NSTAC revisited its earlier 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 (and which led directly to the

establishment of the NCC in 1984), the revised NCM concept involved linking all the Nation’s critical infrastructures (e.g., telecommunications, financial services, electric power, transportation).

[39] The TSP Program is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service.

[40] Developed in response to a White House tasking, GETS provides NS/EP users priority access to and specialized processing for NS/EP calls in local and long distance networks.