THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION INFRASTRUCTURE GROUP REPORT

JUNE 1999

INFORMATION INFRASTRUCTURE GROUP REPORT
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the last meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) in September 1998, the Information Infrastructure Group (IIG) has concentrated its efforts on several issues related to information assurance and infrastructure protection: global information infrastructure (GII), transportation information infrastructure risks, electronic commerce (EC), cyber crime, and Presidential Decision Directive (PDD) 63.

Global Information Infrastructure. In October 1998, the Industry Executive Subcommittee (IES) tasked the IIG to postulate the nature of the GII in 2010 and to assess the implications for national security and emergency preparedness (NS/EP) communications. To that end, the IIG began to conduct research and receive briefings from industry/Government experts on NS/EP issues related to emerging space- and land-based communications systems. The group expects to complete the GII analysis in preparation for NSTAC XXIII.

Transportation Information Infrastructure Risk Assessment. In March 1999, the IIG hosted a workshop in Tampa, Florida, to gather information on the transportation industry's reliance on telecommunications and related information systems. The workshop capped the group's efforts to gather information about that sector's dependency on the telecommunications and information infrastructures. The IIG completed its risk assessment report, which includes recommendations to the President and the transportation industry.

Electronic Commerce. Following the NSTAC XX meeting, the IES tasked the IIG to investigate the NS/EP implications associated with the adoption of EC in industry and Government. The group focused its efforts on issues associated with the changing business and security processes and policies necessary to implement EC. The IIG completed its EC report, which includes recommendations to the President.

Cyber Crime. At the NSTAC XXI Executive Session, the Attorney General requested that the NSTAC and the Department of Justice (DOJ) work together to address cyber security and crime. The IES, however, determined that the projects DOJ suggested for possible NSTAC involvement were beyond the scope of the NSTAC charter. Nevertheless, the IES agreed that the NSTAC could help facilitate a partnership between the DOJ and the private sector. This agreement resulted in a meeting on March 5, 1999, between the NSTAC chair and the Attorney General where industry/Government participation on mutually beneficial projects were discussed.

Presidential Decision Directive 63[1]. IIG members, building on the NSTAC's past efforts in addressing information assurance issues, coordinated with Federal officials responsible for PDD-63 implementation. Specifically, in accord with the PDD-63 emphasis on public-private partnerships, IIG members focused on sharing the lessons and successes of NSTAC and offering

[1] Presidential Decision Directive 63, *Critical Infrastructure Protection*, May 22, 1998.

it as a possible model for other infrastructures. The NSTAC will continue to partner with the Government and relevant private sector organizations as PDD-63 implementation proceeds.

NSTAC Recommendations to the President

- Recommend that the President continue support for the efforts of the Department of Transportation to promote outreach and awareness within the transportation infrastructure as expressed in PDD-63. Specifically, recommend that the President and the Administration ensure support for the following activities:

  - timely dissemination of Government information on physical and cyber threats to the transportation industry,

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

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

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

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

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

NSTAC Direction to the IES

- NSTAC directs the IES to support the Government's efforts in raising awareness of NS/EP issues related to EC.

- The NSTAC directs the IES to—

  - continue discussions with senior Administration officials on PDD-63 implementation, to ensure NS/EP issues are considered,

  - identify the CIP issues which affect information and communications systems,

  - conduct outreach efforts to assist Sector Coordinators in the Information and Communications sector and other critical infrastructures and to share lessons learned from the NSTAC experience,

  - work with the Office of Science and Technology Policy and the Federal departments and agencies in support of Federal infrastructure assurance research and development initiatives, and

  - participate in workshops and seminars as requested by Federal departments and agencies to increase transportation industry awareness of emerging cyber threats and infrastructure vulnerabilities.

1.0 INTRODUCTION AND BACKGROUND

In 1993, the Clinton Administration 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. The goal was a national information infrastructure (NII) that would greatly benefit Government, businesses, and the American public. Since that time, growing competition and technological innovation have resulted in an increasingly interconnected and open information infrastructure that offers commercial efficiencies and societal benefits.

While generating economic and societal benefits, the widespread use and adoption of computer and information (or "cyber") networks introduced new risks. Specifically, the Government became concerned that electronic intruders could exploit vulnerabilities in computer and information systems. The implications of cyber threats and vulnerabilities became even more pronounced with the increasing reliance of other critical national infrastructures on computer and information systems. Government concerns resulted in several studies and formation of the Presidential Commission on Critical Infrastructure Protection (PCCIP) to examine threats to and vulnerabilities of infrastructures. Ultimately, those efforts culminated in Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, which was signed by President Clinton on May 22, 1998.

In its role of providing industry-based advice to the President on national security and emergency preparedness (NS/EP) telecommunications policy, the President's National Security Telecommunications Advisory Committee (NSTAC) examined these emerging information assurance and infrastructure protection issues. Following the earlier work of the NSTAC's NII Task Force and Information Assurance Task Force, the Information Infrastructure Group serves as the focal point for the study of these issues. During the past 4 years, the NSTAC has provided advice to the President in several important areas—

- **NS/EP implications of the NII.** The NSTAC provided industry expertise and insights to the President as the Administration promoted the development of the NII. In addition, the NSTAC developed the concept for and recommended the establishment of an industry-based Information Systems Security Board (ISSB) to foster the development of industry best practices and standards for information systems security. More recently, the NSTAC launched an investigation of the NS/EP implications of the Global Information Infrastructure (GII).

- **Information assurance risks to the electric power, financial services, and transportation infrastructures.** Building on prior efforts to examine security risks to the public network (PN), the NSTAC worked closely with other industries to raise awareness of potential information assurance risks to the electric power, financial

services, and transportation infrastructures. Those risk assessments considered information dependencies and potential threats and vulnerabilities, and highlighted information-related risks relevant to each infrastructure.

- **IA and critical infrastructure protection (IA/CIP) issues.** For more than 3 years, the NSTAC has engaged senior Administration officials on issues relating to IA/CIP policy and the implementation of PDD-63. A key element of that directive was the need for a public-private partnership to address infrastructure vulnerabilities. Extracting lessons learned from its experiences to build industry/Government partnerships such as the Network Security Information Exchange (NSIE) process and the National Coordinating Center for Telecommunications (NCC), NSTAC has offered advice and guidance to the President and the Federal Government on building successful partnerships.

This report captures the efforts of the IIG through the current cycle. The NSTAC XXII IIG members are listed in Annex A. The IIG's current charge is outlined below.

2.0 CHARGE

Since NSTAC XXI in September 1998, the IIG has continued to serve as the NSTAC focal point for information assurance and infrastructure protection issues. The NSTAC's Industry Executive Subcommittee (IES) charged the IIG to—

- postulate the GII for 2010 and identify NS/EP opportunities and issues,
- complete the Transportation Information Infrastructure Risk Assessment,
- investigate NS/EP implications associated with electronic commerce (EC),
- work with the Department of Justice (DOJ) to develop a process to enhance the industry/law enforcement relationship regarding cyber crime,
- investigate the NS/EP implications associated with PDD-63, and
- partner with the Government to share NSTAC lessons learned to enhance the implementation of PDD-63.

3.0 RESULTS

3.1 Global Information Infrastructure

In 1993, the NSTAC established an NII Task Force and charged it with examining the implications of the evolving United States information infrastructure for NS/EP communications. The NII Task Force observed that the NII's connectivity to the emerging GII potentially presented both opportunities and risks for NS/EP communications. In its March 1997 report to NSTAC XIX, the NII Task Force concluded that the pervasive and rapidly evolving nature of the GII necessitated a continuing effort by NSTAC task forces and working groups to track the GII's implications for NS/EP communications. The IIG accordingly was tasked by the IES in October 1998 to conduct a forward-looking analysis of the GII and associated NS/EP opportunities and challenges.

The IIG agreed to address its charge from the IES by completing two tasks: postulate the nature of the GII in 2010 and assess the potential implications of the future GII for NS/EP communications. In selecting 2010 for the purpose of characterizing the future GII, the IIG considered the scope of similar Government projects, specifically, the Department of Defense (DOD)-sponsored "Joint Vision 2010" project involving future warfighting capabilities of the U.S. armed forces.

For the purposes of its analysis, the IIG defined the GII in the context of those physical network elements, services, and protocols that the group believed would be prominently featured in 2010. More specifically, the group agreed to gather data in three main subject areas: space- and airborne-based communications systems (e.g., satellites), land-based communications systems (e.g., terrestrial wireline and wireless), and applications/services and protocols (e.g., asynchronous transfer mode). To this end, the IIG received briefings from selected industry experts regarding the potential role of the various communications systems in the future GII.

During the current cycle, the IIG will continue to research and gather information from industry/Government experts on emerging space-, airborne- and land-based communications systems and services and their potential implications for NS/EP communications. The group expects to present its final report at NSTAC XXIII.

3.2 Transportation Information Infrastructure Risk Assessment

3.2.1 Analysis

The IIG initiated its Transportation Information Assurance Risk Assessment in December 1996. In September 1997, the IIG's Transportation Information Infrastructure Risk Assessment Subgroup hosted a workshop in Atlanta, Georgia, to gather information about the industry's dependence on telecommunications and related information systems. The findings from this workshop were included in an interim report to NSTAC XX in December 1997. The report

concluded that the transportation industry possessed an uneven knowledge 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.

Recognizing the need to gain further input from industry associations and to better understand intermodal transportation trends, the subgroup continued outreach efforts to the transportation industry throughout 1998. Specifically, the subgroup worked with the Department of Transportation to present outreach briefings to targeted transportation industry associations that represented the range of transportation modes. Based on the results of these briefings, the subgroup decided that a second workshop should be held to gather additional industry data necessary to complete the risk assessment. The second workshop took place on March 3-4, 1999, in Tampa, Florida, and included representatives from major freight and passenger carriers, transportation logistics providers, and port authorities. The workshop participants discussed emerging trends throughout the transportation industry, including increased reliance on information technology and the rapid growth of intermodal transportation. Following the workshop, the group completed its risk assessment report, which is attached as Annex B.

3.2.2 Conclusions

The IIG categorized findings from its workshops and outreach activities into four areas: 1) threats and deterrents, 2) vulnerabilities, 3) protection measures, and 4) infrastructure-wide issues. The IIG came to the following six conclusions about risks to the transportation infrastructure:

- **The transportation industry is increasingly reliant on IT and public networks.** The trend to open information systems as a result of growing customer demands will expose the industry to a greater chance of information system vulnerability.

- **Although a nationwide disruption of the transportation infrastructure is unlikely, even a local or regional disruption could have a significant impact.** Due to the diversity and redundancy of the U.S. transportation system, the infrastructure does not risk nationwide disruption resulting from information system failure. Nonetheless, a disruption of the transportation information infrastructure, on a regional or local scale, can have the potential for widespread economic or national security impacts.

- **Business pressures and widespread utilization of IT make large-scale, multimodal disruptions more likely in the future.** As the infrastructure becomes more interconnected and interdependent, the transportation industry will increasingly rely on information technology to complete its most basic business functions. As this

occurs, it becomes more likely that information system failures could result in large-scale disruptions of multiple modes of the transportation infrastructure.

- **There is a need for a broad-based infrastructure assurance awareness program to assist all modes of transportation.** The transportation industry has an uneven awareness of security risks and issues across various modes of transportation. The group concluded that a broad-based program to educate the transportation infrastructure on threat and vulnerability information would be beneficial because of the many modes that compose the infrastructure.

- **The transportation industry could leverage ongoing research and development initiatives to improve the security of the transportation information infrastructure.** The transportation industry would benefit from participation in research and development efforts to improve the security of the transportation information infrastructure and would also benefit from the development of a standard information security rating system.

- **There is a need for closer coordination between the transportation industry and other critical infrastructures.** There are strong linkages between the transportation industry and other critical infrastructures such as information and communications and electric power. Those infrastructures would mutually benefit by sharing information on emerging threats and vulnerabilities, industry trends, and information security best practices and standards.

3.2.3 NSTAC Recommendations to the President

- Recommend that the President continue support for the efforts of the Department of Transportation to promote outreach and awareness within the transportation infrastructure as expressed in PDD-63. Specifically, recommend that the President and the Administration ensure support for the following activities:

  - timely dissemination of Government information on physical and cyber threats to the transportation industry,

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

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

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

3.3 Electronic Commerce

3.3.1 Analysis

The Federal Government is incorporating EC throughout its business operations. The IIG investigated the implications of this trend for the NS/EP community. The group focused its efforts on issues associated with the changing business and security processes and policies necessary to implement EC and the potential NS/EP implications those issues raised. Toward that end, the IIG surveyed EC literature produced by industry/Government and academic sources. In addition, the IIG received briefings from those same sources related to the EC environment (e.g., how EC processes are being implemented by the private and public sectors, and EC security concerns). Finally, to gain greater insight into potential NS/EP implications of incorporating EC into business operations, the IIG interviewed public and private sector officials responsible for implementing EC policies and procedures. The group's report on the NS/EP implications of EC is attached as Annex C.

3.3.2 Conclusions

The IIG concluded that, as the NS/EP community transitions to EC for business operations, Federal departments and agencies should be alert to a number of issues:

- **Anticipated growth of NS/EP dependence on EC.** Initial analysis shows that the NS/EP community's current use of, and dependence on, EC is modest at best. However, factors such as private industry's increasing use of EC and the rising number of initiatives and pilot programs aimed at incorporating EC into the Federal Government's day-to-day operations point to increasing NS/EP dependence on EC.

- **Exposure to EC risks and vulnerabilities.** EC exposes what were once closed and paper-based business processes to the vulnerabilities of EC hardware and software and supporting information technologies. It is important for the NS/EP community to be aware of the vulnerabilities and make informed decisions on how EC technologies should be implemented at an acceptable level of risk.

- **Understanding NS/EP dependence on EC.** It is important that NS/EP departments and agencies assess current and future dependence on EC applications and architectures, the associated security implications, and the effect EC will have on overall business operations.

- **Shared risk.** It is critical to note that in the electronic environment created by EC, 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 EC, as they currently do with telecommunications.

- **Lack of unified focus on NS/EP-specific needs.** Focus on NS/EP needs is lacking among organizations responsible for managing and administrating oversight for EC within the Federal Government, such as the Federal Electronic Commerce Program Office (FECPO), the Joint Electronic Commerce Program Office (JECPO), President's Management Council (PMC), Office of Federal Procurement Policy (OFPP), and Federal Electronic Commerce Acquisition Team (ECAT). This lack of focus could cause NS/EP needs and issues to be overlooked as EC is adopted throughout the Federal Government.

3.3.3 NSTAC Recommendations to the President

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

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

3.3.4 NSTAC Direction to the IES

The NSTAC directs the IES to support the Government's efforts in raising awareness of NS/EP issues related to EC.

3.4 Cyber Crime

At the NSTAC XXI Executive Session, Attorney General Janet Reno requested that the NSTAC and the DOJ work together to address cyber security and crime. In follow-on discussions with IES representatives, the DOJ identified several projects for possible NSTAC involvement. Through subsequent deliberations, IES members determined that the projects suggested by the DOJ were beyond the scope of the NSTAC charter of providing NS/EP telecommunications advice to the President. However, the IES agreed that the NSTAC could play an important role in facilitating a partnership between the DOJ and the private sector. On March 5, 1999, the NSTAC chair met with the Attorney General and discussed potential avenues for industry—both

through industry associations and as individual companies—to participate with the DOJ on mutually beneficial projects. The NSTAC chair also reiterated the NSTAC's continued commitment to the Administration in addressing cyber security issues.

3.5 Presidential Decision Directive 63

The NSTAC has examined IA/CIP issues since 1996. During that time, NSTAC worked closely with the PCCIP and other Federal organizations to identify the threats to and vulnerabilities of critical infrastructures. Federal efforts to examine IA/CIP issues culminated in the signing of PDD-63 on May 22, 1998. That directive outlines a national policy to eliminate vulnerabilities in the Nation's critical infrastructures. 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.

Applying its nearly 16 years of experience in joint industry/Government planning, the NSTAC initiated a dialogue with senior Administration officials responsible for PDD-63 implementation. Specifically, NSTAC offered lessons learned in building joint mechanisms like the NCC and the Government and NSTAC NSIEs. The NSTAC also shared past NSTAC recommendations to the President with possible applicability to PDD-63, including the ISSB[1] and National Coordinating Mechanism (NCM)[2] concepts. The following section highlights the IIG's activities to support Federal implementation of PDD-63.

3.5.1 Analysis

With the PDD-63 emphasis on public-private partnerships, the IIG focused on sharing the lessons and successes of NSTAC and offering it as a possible model for other infrastructures. In particular, IIG members coordinated with Federal officials responsible for the following initiatives:

- **Sector Coordinators.** PDD-63 directs Federal Lead Agencies to identify a Sector Coordinator to represent the industry perspective on IA/CIP programs. At NSTAC XXI in September 1998, the NSTAC's Operations Support Group reported its conclusion that more than one entity would be required to represent the diverse Information and Communications sector. Since then, IIG members have met with officials from the Department of Commerce, the Lead Agency for the Information and Communications sector. In February 1999, the Department of Commerce acted

[1] At NSTAC XIX (March 1997), the NSTAC recommended that the President endorse the creation of an industry-based Information Systems Security Board (ISSB).

[2] At NSTAC XX (December 1997), the NSTAC recommended that the President direct the appropriate Federal agencies to work with the NSTAC to further refine the concept of a cross-infrastructure National Coordinating Mechanism (NCM).

in concert with NSTAC's advice and selected three organizations (Information Technology Association of America, Telecommunications Industry Association, and United States Telephone Association) to serve as the Sector Coordinator for the Information and Communications sector.

- **Information Sharing and Analysis Centers.** PDD-63 calls for the private sector to explore the feasibility of establishing one or multiple Information Sharing and Analysis Centers (ISAC). On the basis of the NSTAC's prior recommendation regarding a cross-infrastructure NCM concept[3], 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 selection of the NCC as an ISAC for telecommunications.

- **Standards and Best Practices.** PDD-63 emphasizes the importance of relying on nonregulatory solutions to address infrastructure vulnerabilities. In satisfying this objective, the Critical Infrastructure Assurance Office (CIAO) has underscored the value of promoting industry standards and best practices to improve infrastructure assurance. That approach is entirely consistent with the prior NSTAC recommendation related to the creation of a private sector ISSB, which would promote information systems security principles, standards, and best practices and improve the reliability and trustworthiness of commercial information products and services.

In addition, IES representatives were invited to participate in two White House meetings to discuss the roles of Sector Coordinators and ISACs in PDD-63 implementation. The IES Working Session chair also presented NSTAC lessons learned at several IA/CIP conferences sponsored by the electric power and financial services sectors. The purpose of those conferences was to identify alternative public-private partnership models.

3.5.2 Conclusions

In analyzing PDD-63 implementation issues, the IIG reached two conclusions. First, it endorses the decision of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism to select the NCC as an ISAC for telecommunications. Its selection builds on the relationships that exist at this unique center, which is jointly staffed by industry/Government representatives. Moreover, this decision is consistent with the prior NSTAC recommendation to create an NCM and to have the NCC serve as the telecommunications focal point.

[3] The concept envisioned a multiplicity of individual infrastructure sector centers modeled on the NCC. Those NCC-like centers would report to a single, national coordinating construct.

Second, the IIG concluded that PDD-63 implementation is occurring in a dynamic environment where several factors are exerting considerable pressure on the Government as it works with industry to eliminate infrastructure vulnerabilities. Those factors include the diverse and interdependent nature of infrastructures, new complexities introduced by information technology, and the changing threat environment. Consequently, it is vital for the Government to continually seek advice from the private sector as information assurance and critical infrastructure protection programs are developed, implemented, and evolve.

3.5.3 NSTAC Direction to the IES

The NSTAC directs the IES to—

- continue discussions with senior Administration officials on PDD-63 implementation, to ensure NS/EP issues are considered,

- identify the CIP issues which affect information and communications systems,

- conduct outreach efforts to assist Sector Coordinators in the Information and Communications sector and other critical infrastructures and to share lessons learned from the NSTAC experience,

- work with the Office of Science and Technology Policy and the Federal departments and agencies in support of Federal infrastructure assurance research and development initiatives, and

- participate in workshops and seminars as requested by Federal departments and agencies to increase transportation industry awareness of emerging cyber threats and infrastructure vulnerabilities.

ANNEX A

INFORMATION INFRASTRUCTURE GROUP MEMBERS

INFORMATION INFRASTRUCTURE GROUP MEMBERS

Unisys	Dr. Dan Wiener, Chair
EDS	Mr. Bob Donahue, Vice-Chair
AT&T	Dr. Larry Nelson
Boeing	Mr. Bob Steele
CSC	Mr. Guy Copeland
GTE	Mr. Lowell Thomas
ITT	Mr. Joe Gancie
Lockheed Martin	Ms. Dena Kisala
MCI WorldCom	Mr. Mike McPadden
Raytheon	Mr. John Grimes
SAIC	Mr. Bernie Ziegler
TRW	Mr. Bob Lentz
U S WEST	Mr. Jon Lofstedt

OTHER CONTRIBUTORS

AT&T	Mr. Gordy Bendick
COMSAT	Mr. Ernie Wallace
CSC	Mr. Richard Swanson
CSC	Ms. Deborah Jacobs
GTE	Ms. Ernie Gormsen
Nortel Networks	Dr. Jack Edwards
NTA	Mr. Bob Burns
Raytheon	Mr. Bob Tolhurst
Unisys	Mr. Fred Tompkins

ANNEX B

TRANSPORTATION INFORMATION INFRASTRUCTURE RISK ASSESSMENT REPORT

ANNEX C

REPORT ON NS/EP IMPLICATIONS OF ELECTRONIC COMMERCE