THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP REPORT

JUNE 1999

NETWORK GROUP REPORT
TABLE OF CONTENTS

EXECUTIVE SUMMARY ES-1

1.0 INTRODUCTION AND BACKGROUND 1

2.0 CHARGE 1

3.0 RESULTS 1

3.1 R&D Exchange 1
3.1.1 Analysis 2
3.1.2 Conclusions 2
3.1.3 Recommendations 3
3.1.4 Next Steps 4
3.2 Network Security Information Exchange (NSIE) 5
3.2.1 Insider Threat Workshop 5
3.2.2 Risk Assessment 6
3.2.3 Next Steps 6
3.3 Internet Issue 7
3.3.1 Analysis 7
3.3.2 Conclusions 8
3.3.3 NSTAC Recommendations to the President 9
3.3.4 NSTAC Direction to the IES 10
3.3.5 Next Steps 10
3.4 Gap Analysis 10
3.4.1 Status 11
3.4.2 Next Steps 11

NETWORK GROUP MEMBERS ..... ANNEX A

R&D EXCHANGE PROCEEDINGS REPORT ..... ANNEX B

NSTAC NSIE CHARTER ..... ANNEX C

INTERNET REPORT ..... ANNEX D

EXECUTIVE SUMMARY

Since the last meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) in September 1998, the Network Group (NG) has directed its efforts to four activities. Two of these activities involve the NG's ongoing responsibilities: facilitating the exchange of network security research and development (R&D) information between industry and Government and overseeing the NSTAC Network Security Information Exchange (NSIE). Discussions at NSTAC XX resulted in an additional tasking that has now been completed: examining how national security and emergency preparedness (NS/EP) operations might be affected by a severe disruption of Internet service. Lastly, in conjunction with the gap analysis effort by the Office of the Manager, National Communications System (OMNCS), NG members provided their individual perspectives on the Public Network (PN) Alternative Analysis Report developed by the OMNCS.

RESULTS

- **R&D Exchange:** The NG's network security R&D Exchange was held in collaboration with Purdue University's Computer Operations, Audit, and Security Technology Laboratory (COAST), the Institute of Electrical and Electronics Engineers (IEEE), and the Office of Science and Technology Policy (OSTP) at a workshop on security in large-scale distributed systems, held at Purdue University on October 20-21, 1998. The R&D Exchange addressed the growing convergence of telecommunications and the Internet, and methods for improving the collaboration among industry, Government, and academia on R&D efforts.
- **NSIE:** During the previous NSTAC cycle, the Government and NSTAC NSIEs sponsored a workshop on the insider threat to information systems and developed two white papers to provide background material for the workshop. The workshop offered an overview of the emerging insider threat and suggested measures organizations could take to reduce their vulnerability to it. During the current NSTAC cycle, the NSIEs developed an After-Action Report reflecting the insights that emerged from the workshop discussion so this material can be shared with a broader audience. The NSIEs also completed their *1999 Assessment of the Risk to the Security of the Public Network*. Lastly, the NSTAC NSIE charter was amended to bring it in line with the way the NSIEs function.
- **Internet Issue:** Following discussion at NSTAC XX, the Industry Executive Subcommittee (IES) tasked the NG to examine how NS/EP operations might be affected by Internet failures over the next 3 years. At NSTAC XXI, the NG presented a status update of the problem and discussed data gathering efforts. The NG completed its report and has made recommendations to both the President and the NSTAC.

- **Gap Analysis:** As part of its effort to identify alternative PN telecommunications services that are partially or totally non-dependent on the PN during various levels of service impairment, the OMNCS developed a PN Alternatives Analysis Report. NG members were asked to consider the thoroughness of selected alternatives, consistency of evaluations, accuracy of information, and ease of understanding.

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*, direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:

    a. Work with the NS/EP community to increase understanding of evolving Internet dependencies.

    b. Work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements.

    c. 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.

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

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

NSTAC Direction to the IES

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

1.0 INTRODUCTION AND BACKGROUND

The Network Group (NG) serves as the focal point for the network security activities of the President's National Security Telecommunications Advisory Committee (NSTAC). The Industry Executive Subcommittee (IES) established the NG as a permanent body to guide NSTAC's ongoing network security activities (e.g., participating in the exchange of research and development (R&D) information between industry and Government and overseeing the NSTAC Network Security Information Exchange [NSIE]). The NG also addresses new network security issues as they arise. The NSTAC XXII NG members are listed in Annex A.

2.0 CHARGE

Since NSTAC XXI in September 1998, the NG has continued its efforts to guide ongoing network security activities, concluded an ongoing task resulting from the NSTAC XX meeting, and initiated a task to review the Government's gap analysis efforts.

The two ongoing network security activities are as follows:

- **R&D Exchange.** Plan and conduct an R&D Exchange and determine the feasibility of a long-term R&D consortium.
- **Information Exchange.** Promote the exchange of information between industry, Government, and academia regarding network security vulnerabilities and threats.

The one task originating from NSTAC XX was as follows:

- **Internet Issue.** Examine how NS/EP operations might be affected by a severe disruption of Internet service caused by the failure of network routing and control mechanisms.

In addition, NG members reviewed the PN Alternatives Analysis Report, as a part of the gap analysis effort, and provided their individual comments on the thoroughness of study alternatives, consistency of evaluations, accuracy of information, and ease of understanding.

3.0 RESULTS

3.1 R&D Exchange

In late 1996, the Deputy Manager, NCS, asked the NSTAC to assist the Defense Advanced Research Project Agency (DARPA) in its work to address intrusion detection R&D. In December 1997, the NSTAC's Intrusion Detection Subgroup (IDSG) subsequently provided a report to NSTAC XX detailing its findings and recommendations for the President to promote

the R&D of intrusion detection technologies. As a follow-on to the IDSG's work, the NG decided to sponsor an R&D Exchange in the fall of 1998 to address two issues: the growing convergence of telecommunications and the Internet, and how industry, Government, and academia can better collaborate on network security R&D.

3.1.1 Analysis

The NG conducted the R&D Exchange in October 1998 in collaboration with activities sponsored by Purdue University's Computer Operations, Audit, and Security Technology (COAST) Laboratory, the Institute of Electrical and Electronics Engineers (IEEE), and the Office of Science and Technology Policy (OSTP). The findings and recommendations of the participants in the R&D Exchange are documented in *Research and Development Exchange Proceedings: Enhancing Network Security Technology R&D Collaboration*. As part of its follow-up on the R&D Exchange, the NG compared the R&D Exchange findings and recommendations with those of the NG's Intrusion Detection Subgroup (IDSG) Report issued in December 1997. Although the R&D Exchange and the IDSG had different charges and took different approaches to network security R&D, the findings and recommendations of the Exchange were consistent with and validated those of the IDSG. A copy of the 1998 R&D Exchange Proceedings is attached as Annex B.

3.1.2 Conclusions

The attendees at the Exchange arrived at the following conclusions.

- There is significant brain drain occurring in Government and academia with respect to computer and network security. Specifically, Government and academia must compete with industry to secure the services of information security professionals but are at a distinct disadvantage given their limited resources.

- A major technical impediment to improving security technologies is the lack of metrics to indicate an organization's or system's security posture. Metrics play an important role in the context of assessing risks, evaluating new security tools and products, developing professional accreditation and standards, and quantifying the value of security in organizations.

- Another technical impediment is the lack of testbeds. Participants discussed the possibility of developing joint or virtual "neutral party" testbeds that allow all organizations—industry, Government, academia, or others—to develop and test products and train students and employees in realistic environments.

- Current programs remain concentrated on respond and react technologies rather than considering the full range of risk management needs. An R&D agenda that includes technologies to prevent intrusions and reconstitute systems in the aftermath of an intrusion would provide a more balanced and comprehensive approach to addressing security needs.

- The funding models used by industry and Government are not always conducive to taking the long view of security. A short-term, deliverable-driven approach limits the ability of academia to develop long-term research programs and methodologies and to attract and retain dedicated faculty. The establishment of viable academic programs—and robust centers of excellence—requires a more stable source of funding.

- Effective industry-Government-academia collaborative models exist in disciplines other than information security. Conference participants emphasized the importance of establishing an independent clearinghouse to provide organizations interested in security R&D with access to technology, standards, industry best practices, test-case scenarios, and awareness programs. This conclusion is consistent with the findings of the NSTAC's National Information Infrastructure Task Force in examining the need for and feasibility of an Information Systems Security Board (ISSB).[1]

- Conference participants emphasized the importance of taking the "long-view" of security, projecting those computer and network security challenges likely to emerge in the next 5-10 years.

3.1.3 Recommendations

The attendees at the Exchange proposed the following recommendations for Government and NSTAC consideration.

3.1.3.1 Recommendations to the Government

- Identify potential centers of excellence in academia, industry, and Government and providing them with appropriate long-term funding to promote the development of computer and network security professionals, disciplines, and programs.

[1] "National Information Infrastructure Task Force Report," President's NSTAC, March 1997. The task force conceptualized the ISSB as a private sector entity that would promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services.

- Develop incentives (e.g., revisions of capital gains tax policy) to promote industry investment in long-term security and infrastructure assurance technologies.

- Establish Government programs that encourage undergraduate and graduate students to pursue further study in computer and information security.

- Continue to incorporate advice from leading experts from the private sector, academia, and advisory boards to assist OSTP as it develops, refines, and implements a national infrastructure assurance R&D agenda.

- Conduct a joint study with NSTAC and academia on the need for, feasibility of, and costs associated with the establishment of large-scale testbeds to: promote joint research; develop and verify metrics; test and evaluate security products; and address other technical needs in network security and information assurance.

3.1.3.2 Recommendations to the NSTAC

- Work with the Government and academia to study the need for, feasibility of, and costs associated with the establishment of large-scale testbeds to: promote joint research; develop and verify metrics; test and evaluate security products; and address other technical needs in network security and information assurance.

- Examine the business case associated with industry funding student grants, fellowships, and scholarships; sponsoring exchange programs and providing subject matter experts to assist academic programs; and funding endowed teaching positions.

- Conduct another R&D Exchange to continue the dialogue with Government and academia and to consider the long-term issues associated with infrastructure assurance and network security, including: new threats; the introduction of new technologies and vulnerabilities; and the convergence of communications and computing technologies.

3.1.4 Next Steps

During the next NSTAC cycle, the NG will continue to interact with the Government to gain an understanding of how the Government's network security R&D resources are being allocated. In addition, the NG will consider conducting another R&D Exchange after R&D network security initiatives currently in the planning stages have matured sufficiently to indicate whether they are likely to satisfy network security shortfalls. The NG will consider the R&D Exchange

conclusions and recommendations as it develops its work plan for NSTAC XXIII, in particular as it considers topics for the next R&D Exchange.

3.2 Network Security Information Exchange (NSIE)

The Government and NSTAC NSIEs have continued to exchange information and views on threats and vulnerabilities affecting information and software elements of the PN, remedies, and consequent risks. During this NSTAC cycle, the NSTAC NSIE charter was amended to bring it in line with the way the NSIEs function, i.e., primarily as information sharing bodies. For further detail about NSIE purpose and objectives, functions, membership, and operating principles, see the NSTAC NSIE Charter in Annex C.

The NSIEs have a history of sharing "lessons learned" within the information exchange process with a broader audience. During this NSTAC cycle, the NSIEs have done this by producing an After Action Report on the Insider Threat Workshop, which was held during the previous NSTAC cycle, and their risk assessment. Both efforts are described in greater detail below.

3.2.1 Insider Threat Workshop

During the last NSTAC cycle, NSIE representatives addressed the insider threat to information systems and sponsored a workshop on this topic. The workshop offered an overview of the emerging insider threat and suggested measures that organizations could take to reduce their vulnerability to it. The workshop was designed to address the needs of mid-level managers responsible for negotiating business agreements with vendors, contractors, customers, and business partners; developing and implementing computer security policies, procedures, and practices; or developing and implementing Human Resources policies, procedures, and practices.

The workshop was held in June 1998 and was attended by 101 individuals representing 52 organizations. In addition to NSTAC member companies and NCS member departments and agencies, the audience included representatives from other critical infrastructures (e.g., the financial services and electrical power industries), as well as contractors, vendors, and professional recruiters who serve the telecommunications industry. As part of this initiative, the NSIEs developed two white papers on the insider threat:

- *The Insider Threat: Legal and Practical Human Resources Issues: An NSIE White Paper,* April 1998.

- *The Insider Threat to Information Systems: A Framework for Understanding and Managing the Insider Threat in Today's Business Environment,* June 1998.

During this NSTAC cycle, the NSIEs developed and issued an After-Action Report to capture workshop-generated information and insights on the insider threat to share their findings with a broader audience.

3.2.2 Risk Assessment

The NSIEs also completed their *1999 Assessment of the Risk to the Security of the Public Network*. The NSIEs concluded that the 1995 findings regarding the overall vulnerability of the PN are still valid today—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., SS7, IN, ATM, and SONET) remain unaddressed; and technologies and networks are highly interconnected. Over the past 3 years, 3 major factors have exacerbated the overall vulnerability of the PN: the Telecommunications Act of 1996; changing business practices; and the Year 2000 (Y2K) technology problem.

With respect to protection measures, technology and awareness are clearly improving and no doubt service providers and vendors are becoming more knowledgeable and skillful in implementing protection measures. At the same time their knowledge of and, more importantly, their ability to control, the full extent of their network connections and dependencies is diminishing.

Since the last NSIE risk assessment, the intelligence community has increased its efforts to focus on defining the electronic intrusion threat to the PN. However, restrictions on gathering intelligence on U.S. citizens somewhat limit the availability of information on the domestic threat. Hacker tools continue to improve and have become widely available, as has information on vulnerabilities. This trend is expected to continue, especially as more individuals use the Internet and become more proficient in using it.

Continuing trends in law enforcement and legislation have increased the ability of Government and corporate organizations to deter the intrusion threat. In addition, victims are gradually becoming more willing to report intrusions and cooperate with law enforcement.

Absent a valid baseline to establish quantitative measures of the risk to the PN from electronic intrusions, it is difficult to definitively state how the risk has changed over the past 3 years. However, there is little evidence to suggest that the overall risk has diminished since 1995, and a number of factors to suggest that it is growing.

3.2.3 Next Steps

NSIE: The NSTAC NSIE, along with the Government NSIE, will continue to share network security information to help mitigate any potential impacts from intrusions and to explore

methods to improve information exchange between the NSIEs and the National Coordinating Center for Telecommunications (NCC).

NG: The NSIEs' 1999 risk assessment concluded that the conditions affecting risk described in the 1995 risk assessment still persist, and new factors since that time have introduced additional vulnerabilities into the PN. In spite of improvements in awareness, protection measures, and deterrents over the past 3 years, the general sense is that vulnerabilities and threats are outpacing these improvements and, consequently, the overall risk to the PN continues to grow. The NG is concerned that the increase in resources allocated to network security has not had the desired effect. Although conventional wisdom may suggest that greater progress could only be achieved with greater resources, an alternative approach may be to reconsider how those resources are allocated. Perhaps greater progress would be achieved by changing the way in which those resources are allocated among the four pillars of network security— prevention, detection, mitigation, and response. The NG plans to examine this issue during the next NSTAC cycle.

3.3 Internet Issue

Much like the private sector, the Government is using the Internet more extensively for day-to-day functions, such as electronic mail and procurement. As the Government extends its Internet use to more critical applications, such as NS/EP functions, there are concerns about how a severe disruption of Internet service might affect NS/EP operations. This issue arose during discussion at the NSTAC XX meeting in December 1997, and the IES subsequently tasked the NG to examine how NS/EP operations might be affected by Internet failures over the next 3 years.

For the purposes of the report, a severe disruption is described as a sustained interruption or severe degradation of Internet service that could have potential strategic and/or service integrity significance to industry, Government, and the general public. Such an event would likely affect Internet service in at least one region of the country including at least one major metropolitan area. It would involve multiple Internet service providers and significantly degrade the ability of at least one essential infrastructure to function and would have an impact on the availability and integrity of Internet service for at least a significant portion of a business day.

3.3.1 Analysis

The NG took the following approach to the tasking:

- examined the extent to which NS/EP operations will depend on the Internet over the next 3 years,

- identified vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the Public Switched Network (PSN), and
- examined how Internet reliability, availability, and service priority issues apply to NS/EP operations.

In compiling the information provided in the Internet report, the NG solicited information from Government NS/EP community organizations (e.g., FEMA, DOD), industry, and academia. The NG gathered information on the Internet's architecture, its vulnerabilities, and how the Internet will be used to support NS/EP operations. A copy of the Internet Report is attached as Annex D. The NG completed its study of the NS/EP community's reliance on the public Internet and dedicated TCP/IP networks (intranets) and offers the conclusions and recommendations described in sections 3.3.2 through 3.3.4.

3.3.2 Conclusions

The NG reached the following conclusions:

- Agencies with NS/EP responsibilities are using the public Internet mostly for outreach, information sharing, and electronic mail (e-mail).
- The NS/EP community's direct dependence on the public Internet for mission-critical operations is currently modest.
- NS/EP dependence on the Internet is likely to grow over the next several years because the public Internet offers cost-effective, efficient means of communications, the Government is rapidly adopting electronic commerce, and Federal policies promote use of the Internet.
- The NS/EP community is more likely to depend on dedicated Transmission Control Protocol/Internet Protocol (TCP/IP) networks (also called intranets) for mission-critical NS/EP operations at present.
- 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.
- 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 Internet is a conglomeration of inter-exchange points (IXPs) and national, regional, and local Internet Service Providers (ISPs) serving end users and organizations. With the Internet's highly diverse architecture and complex interconnection arrangements, consisting of thousands of ISPs, it is *unlikely* that the failure of any single node or transmission facility would cause a major Internet service disruption.

- The informal and distributed management of Internet functions, the Domain Name System (DNS), Internet software including Berkeley Internet Name Domain (BIND), and procedural errors and unintentional actions invite potential vulnerabilities that could contribute to a disruption of Internet service.

- At present, the reliability and security of the public Internet is generally considered inadequate for NS/EP mission-critical functions.

- Today, there are no Internet technologies or applications that facilitate the same type of end-to-end NS/EP- related services available in the PSN (i.e., priority access, routing, and transport).

- Although certain ISPs currently offer in-network quality of service (QoS) standards, there are no end-to-end QoS offerings available via the public Internet (e.g., level of availability and performance).

- There are currently no economic incentives for ISPs to develop and offer NS/EP service enhancements over their networks.

- A number of factors (e.g., lack of NS/EP demand, market factors, and lack of regulatory mandates) preclude the availability of NS/EP services over the Internet for the foreseeable future.

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*, direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:

a. Work with the NS/EP community to increase understanding of evolving Internet dependencies.

b. Work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements.

c. 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.

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

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

3.3.4 NSTAC Direction to the IES

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

3.3.5 Next Steps

The NG stands ready to investigate Internet technology developments and IP network-PSN convergence issues within the Internet community and their potential impact on NS/EP telecommunications.

3.4 Gap Analysis

The Government is currently reviewing the NS/EP telecommunications readiness of various Federal agencies to identify the Government's "minimum essential" communications requirements supporting NS/EP activities. Any potential gaps or shortfalls in the NS/EP telecommunications infrastructure between what the Government requires and what industry can provide will be identified in the analysis.

3.4.1 Status

The NG members reviewed the OMNCS's PN Alternatives Analysis Report and provided individual comments on the thoroughness of alternatives, consistency of evaluations, accuracy of information, and ease of understanding.

3.4.2 Next Steps

The NG will continue to assist the OMNCS in its gap analysis efforts.

ANNEX A

NETWORK GROUP MEMBERS

NETWORK GROUP MEMBERS

Nortel Networks	Dr. Jack Edwards, Chair
GTE	Mr. Jim Bean, Vice Chair
SAIC	Mr. Hank Kluepfel, Vice Chair
U S WEST	Mr. Jon Lofstedt, Vice Chair
AT&T	Mr. Gordy Bendick
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
ITT	Mr. Peter Steensma
MCI WorldCom	Mr. Don Frick
NTA	Mr. Bob Burns
Raytheon	Mr. John Grimes
Sprint	Dr. Sushil Munshi
Unisys	Mr. Fred Tompkins
USTA	Dr. Vern Junkmann

OTHER CONTRIBUTORS

Lockheed Martin	Dr. Chris Feudo
Raytheon	Mr. Tom Hudson
Raytheon	Mr. Robert Tolhurst

ANNEX B

R&D EXCHANGE PROCEEDINGS REPORT

ANNEX C

NSTAC NSIE CHARTER

As Amended March 1999

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC NSIE CHARTER
As Amended March 1999

NSTAC NSIE Charter
As Amended March 1999

Section I. ESTABLISHMENT

The NSTAC Network Security Information Exchange, hereinafter referred to as the NSTAC NSIE, is established under the auspices of the President's National Security Telecommunications Advisory Committee (NSTAC). The date of initial activity is June 1991.

Section II. PURPOSE AND OBJECTIVES

The purpose of the NSTAC NSIE is to provide a working forum to identify issues involving penetration or manipulation of software and databases affecting national security and emergency preparedness (NS/EP) telecommunications. In this context, the NSTAC NSIE will share information about the security of the Public Network (PN) with the objectives of:

- Learning more about intrusions into and vulnerabilities affecting the public network
- Developing recommendations for reducing network security vulnerabilities
- Assessing network risks affecting network assurance, in concert with the Government NSIE
- Acquiring threat and threat mitigation information from the Government
- Providing expertise to the NSTAC on which network security recommendations to the President can be based.

Section III. FUNCTIONS

To meet its objectives, the NSTAC NSIE shall:

- Exchange information and views on:
    - Threats and incidents affecting the software elements of the PN
    - Vulnerabilities of the PN
    - Remedies, and
    - Consequent risks to NS/EP telecommunications

- Develop or recommend measures to reduce vulnerabilities of the PN
- Develop a database of vulnerabilities affecting NS/EP telecommunications
- Assess, when alert and warning indications warrant, the potential for significant degradation of PN services and recommend approaches to reduce network impact
- Keep abreast of developments in security procedures and technologies as they affect NS/EP telecommunications
- Periodically assess NS/EP risks, including trends, international activities, and key uncertainties, and inform senior NSTAC and Government managers.

Section IV. MEMBERSHIP

Members of the NSTAC NSIE shall be NSTAC Member organizations who shall be chosen by the NSTAC's Industry Executive Subcommittee.

Each NSTAC NSIE member organization may appoint up to two individuals to participate in the NSTAC NSIE. Representatives will be subject matter experts, e.g.:

- Employees who are engaged full time in the prevention, detection, and/or investigation of network software penetration
- Employees who have security and investigative responsibilities.

When deemed appropriate by the NSTAC NSIE, an additional representative may be authorized to NSTAC NSIE member organizations to obtain specific subject matter expertise.

Voting rights are accorded to each participating Member organization.

Section V. ORGANIZATION

The Members of the NSTAC NSIE will elect a Chair and a Vice Chair. The Office of the Manager, National Communications System will serve as secretariat.

Section VI. OPERATING PRINCIPLES

The operating principles of the NSTAC NSIE are as follows:

- The NSTAC NSIE will report to the Industry Executive Subcommittee (IES) or an IES subgroup designated by the IES.

- Due to the sensitive nature of the information that may be discussed at NSTAC NSIE meetings, attendance will be limited to member representatives and guests invited with the prior approval of the Chair.

- Recording devices of any kind will not be permitted at NSTAC NSIE meetings unless specifically authorized by the group.

- All member organizations, their representatives and their guests must sign the appropriate nondisclosure arrangement before attending their first meeting.

- All representatives must have, or be capable of acquiring upon appointment, a security clearance at the SECRET level.

- Summary meeting notes will be prepared, will be marked proprietary/classified as required by the content, and will be limited in distribution.

- The NSTAC NSIE shall regularly meet jointly with the Federal Government NSIE to exchange information on threats, vulnerabilities, remedies, and risks.

- For NSTAC NSIE meetings that are joint with the Government NSIE, the attendees and agendas will be jointly agreed to by the Chairs of the two groups.

- To the maximum extent possible within the constraints of the Nondisclosure Agreement, information shared by the NSIEs will be provided to the National Coordinating Center for Telecommunications (NCC) in its role as an indications, assessment and warning center for the telecommunications industry.

- When advisable and within the constraints of the Nondisclosure Agreement, the NSIEs will share information with other organizations through workshops, symposiums and similar activities.

The NSTAC NSIE will operate within the requirements of all applicable Federal laws concerning the disclosure of information.

ANNEX D

INTERNET REPORT