THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

OPERATIONS SUPPORT GROUP REPORT

December 1997

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The President's National Security Telecommunications Advisory Committee's (NSTAC) Operations Support Group (OSG) was established in April 1997 to evaluate the overall progress and direction of NS/EP operational activities. Among its specific taskings, the OSG was instructed to assist the Government in development of a future concept of operations for the National Coordinating Center for Telecommunications (NCC), and to explore the need for and feasibility of a National Coordinating Mechanism (NCM) across infrastructures. Two OSG subgroups, the NCC Vision Subgroup and the NCM Subgroup, addressed these actions. This report presents the charge, approach, findings, conclusions, and recommendations of the OSG and its two subgroups.

The NCC is envisioned to serve as a focal point for receiving, screening, and processing electronic intrusion incident information for industry and Government telecommunications service providers and network operators. The NCC Vision Subgroup concluded that the NCC can implement an initial intrusion incident information processing capability, but more study is needed to fully integrate an electronic intrusion incident information processing function into the NCC.

An NCM and its organizational processes would provide senior Federal Government decision makers with real-time information from related components of critical national infrastructures to enhance NS/EP. The NCM Subgroup concluded that the NCM concept provides a framework for the Federal Government and the private sector to begin to discuss solutions to growing infrastructure protection concerns.

The following recommendations are based on the group's determinations:

NCC Vision Subgroup Recommendation for the President

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

NCC Vision Subgroup Recommendation for the NSTAC

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

NCC Vision Subgroup Recommendations for the Industry Executive Subcommittee (IES)

- NSTAC's IES extend the NCC Vision Subgroup tasking into the next NSTAC cycle.

- The IES approve the revised Section 2.0 and Section 3.0 of the *NCC Operational Guidelines.*

NCM/IA Policy Subgroup Recommendations for the President

The President should direct appropriate departments and agencies to identify personnel within their respective department and agency that have the requisite policy, management, and mission expertise to work with the NCS and NSTAC in carrying out the following:

- Continue to refine the NCM concept and postulate how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, research and development (R&D), standards, security investment, law enforcement capabilities, and the globalization of information systems.

- Identify details of the NCM's initial formation and operation.

- Explore the linkages within Government departments and agencies among infrastructures that will be essential to the NCM recommendation.

- Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

NCM/IA Policy Subgroup Recommendations for the NSTAC

The NSTAC should charge the IES to do the following:

- Continue to refine the NCM concept and postulate how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, R&D, standards, security investment, law enforcement capabilities, and the globalization of information systems.

- Identify details of the NCM's initial formation and operation.

- Explore the linkages with Government and between infrastructures that will be essential to the NCM recommendation.

- Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

- Based on the outreach, develop a final recommendation as soon as possible, with interim status reports at intervening NSTAC meetings.

1.0 INTRODUCTION AND BACKGROUND

In April 1997, the President's National Security Telecommunications Advisory Committee's (NSTAC) Industry Executive Subcommittee (IES) created the Operations Support Group (OSG), succeeding the former National Security and Emergency Preparedess (NS/EP) Group, to evaluate the overall progress and direction of NS/EP operational activities. OSG members represented the telecommunications, information technology, and systems integration industries, and provided unique perspectives on the challenges of NS/EP operations and planning. The following paragraphs provide the background on the five components of the OSG's charge.

In October 1996, the NSTAC's IES created the NCC Vision Task Force to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. As the task force formed, the Manager, National Communications System (NCS), requested that the NSTAC assist the NCS in developing a concept of operations and implementing an electronic intrusion indications and reporting capability in the NCC. The Manager also asked that the NCC's information assurance capabilities include the ability to evaluate intrusion incidents and to take mitigative actions against effects. The task force held its first meeting on November 15, 1996. When the IES reorganized in April 1997, the OSG was assigned oversight of the NCC Vision Task Force. The OSG renamed the task force the NCC Vision Subgroup, and the subgroup continued work on its original tasking with the same membership.

NSTAC's recognition of the increasing interdependencies of the nation's critical infrastructures (e.g., power, telecommunications, transportation, banking and finance), and the formation of the President's Commission on Critical Infrastructure Protection (PCCIP) led to a charge to the OSG to explore critical infrastructure protection. In July 1996, the President issued Executive Order 13010, creating the PCCIP to recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats to assure their continued operation. NSTAC and PCCIP outreach activities during the past year surfaced strong support for greater information sharing among and between critical infrastructures and the Federal law enforcement, intelligence, and military communities. In addition, these Government communities also recognized the need to improve information sharing. In light of these developments, the National Coordinating Mechanism (NCM) Subgroup began to examine potential organizational structures and functions of the NCM concept.

At the NSTAC XIX meeting in March 1997, Dr. John Gibbons, Office of Science and Technology Policy, requested that the NSTAC scope the threat of a widespread telecommunications service outage. The IES tasked the Network Group (NG) and the OSG to develop a response to his inquiry. The NG assumed the lead on the tasking, which included responding to three questions related to the possibility of a widespread telecommunications possibility and potential recovery procedures should such an outage occur.

Prior to its termination, NSTAC's former National Information Infrastructure Task Force concluded that the pervasive nature of the Global Information Infrastructure (GII) and its rapid

evolution required a continuing effort to track the implications to NS/EP communications.[1] The OSG became the lead working group to track GII issues following NSTAC XIX.

Finally, under Presidential Decision Directive (PDD)-39, the Federal Emergency Management Agency was tasked with analyzing the adequacy of the Federal Government to respond to the consequences of terrorist incidents involving nuclear, biological, or chemical material within the United States. The NCS, as a member of the Catastrophic Disaster Response Group, assisted in the development of that assessment. In partnership with the NCS, the NSTAC agreed to monitor PDD-39 related activities and to provide industry input as needed.

2.0 GROUP CHARGE AND APPROACH

The IES charged the OSG to evaluate the overall progress of and future challenges facing NS/EP telecommunications and information systems operations and planning. Included in the charge were the following five components:

- Assist the Government in the development of a future concept of operations for the NCC
- Explore the need for and feasibility of an NCM across infrastructures
- Provide input to the NG regarding the threat of a widespread telecommunications outage
- Assess GII developments
- Assess emergency communications capabilities in the PDD-39 context.

The following describes the OSG's approach for addressing its charge.

2.1 NCC Vision Subgroup

The NCC Vision Subgroup was charged to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. The NCC Vision Subgroup Report, including its findings, conclusions, recommendations, and appendices, is attached as Appendix B.

2.2 NCM/Information Assurance (IA) Policy Subgroup

The NCM Subgroup was tasked to explore the need for and feasibility of an NCM across infrastructures. In July 1997, the subgroup produced an issue paper describing the need, feasibility, and value of an NCM. Concurrently, the IA Policy Subgroup of the Information

[1] National Information Infrastructure (NII) Task Force Report to NSTAC, March 1997.

Infrastructure Group was developing an IA Policy Report based on the findings of NSTAC risk assessments, the lessons learned from other NSTAC outreach activities, the findings and recommendations of the PCCIP as available, and other relevant activities. The two subgroups began to meet together in September 1997 to produce a joint report, *Information Assurance: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group*. This report, which is presented as Appendix C, organizes and identifies common issues and policy solutions regarding protection of the Nation's critical infrastructures.

2.3 Widespread Telecommunications Service Outage

Members of the OSG participated in the Widespread Telecommunications Service Outage Subgroup of the NG. The group lent its expert advice to the NG as it led the widespread telecommunications outage analysis. The OSG inputs were incorporated into the NG's final report.

2.4 Global Information Infrastructure

The group received a briefing regarding the GII-related World Trade Organization (WTO) Basic Telecommunications Services Agreement. The agreement did not have any major NS/EP implications. However, the agreement is expected to facilitate telecommunications business operations in participating WTO countries, thereby facilitating international NS/EP telecommunications.

2.5 Presidential Decision Directive 39

The group received a briefing from the Director of Military Support on its mission and activities related to the Defense Against Weapons of Mass Destruction Act of 1996 (Nunn-Lugar-Domenici) and determined that no further action was needed. The group continues to monitor PDD-39 activities, and will participate as needed.

3.0 GROUP FINDINGS AND CONCLUSIONS

As a result of the findings and recommendations of the OSG subgroups and other OSG analysis, the OSG reported the following findings and recommendations.

3.1 NCC Vision Subgroup Findings and Conclusions

3.1.1 NCC Vision Subgroup Findings

The subgroup found three specific issues that remain to be resolved:

- **Reporting criteria.** Identifying and obtaining agreement on the specific intrusion incident information required to develop indications and warnings.

- **Information sharing.** Identifying and obtaining agreement on the specific information that will be shared by industry and Government telecommunications service providers and network operators, and law enforcement, intelligence, and national security entities.

- **Value.** Defining the value added for industry participants in the intrusion incident information reporting process.

Resolution of these issues is necessary before determining future NCC resource requirements, such as membership, costs, and funding.

3.1.2 NCC Vision Subgroup Conclusions

The subgroup concluded that the NCC can implement an initial intrusion incident processing capability, but more study is needed to fully integrate an electronic intrusion incident information processing function into the NCC. The NCC is envisioned to serve as a focal point for receiving, screening, and processing electronic intrusion incident information for industry and Government telecommunications service providers and network operators.

3.2 NCM/IA Policy Subgroup Findings and Conclusions

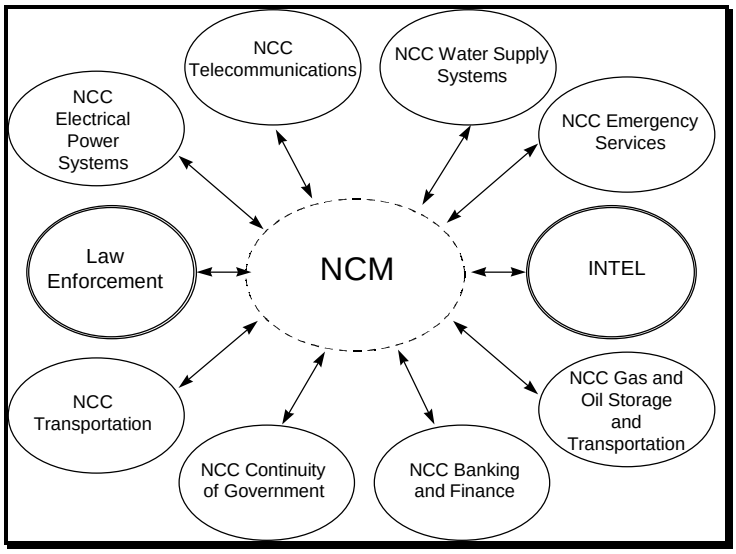
An NCM would require linking diverse sources of information within the private sector and the Government, including the intelligence and law enforcement communities. In addition, it would require developing new, trusted channels for information exchange and creating functional equivalents to the NCC within other critical infrastructures. The NCC Vision Subgroup along with the NCS NCC Vision Implementation Team has begun to address these issues in the course of assessing the future mission, organization, and capabilities of the NCC.

Operationally, the proposed NCM might best be envisioned as primarily an entity or process for sharing information among infrastructures and the Government. The success of the NCM would rest largely on the trusted relationships that would develop among all stakeholders. Information shared through the NCM would be used by the various stakeholders in accordance with their respective mission responsibilities. It is important to recognize that the feasibility of the NCM is dependent on the willingness of industry and Government to contribute meaningful information to the process. Participation in the NCM must be voluntary and industry must never perceive itself to be subordinate to the Government. The NCM would be a cooperative partnership between industry and Government based on trusted relationships and the two-way flow of information.

Information channeled to and between stakeholders would be analyzed and available to appropriate decision makers in Government and industry. As shown in the Figure, each infrastructure would have an NCC to address industry-specific issues. The NCM in turn would provide the means for coordinating infrastructure-wide consequence management to industry for infrastructure protection or restoration in the event of criminal, terrorist, or state-sponsored

actions. In addition, an NCM would provide industry with a mechanism for identifying and addressing interdependency issues across infrastructures.

Figure 1. National Coordinating Mechanism



Both conceptually and operationally, the NCM poses significant information management challenges. To effectively coordinate the flow of information, criteria for reporting information must be established and accepted by all participants. The identification of candidate participants in an NCM must be based on the ability to affect NS/EP. In addition, an ongoing analysis of the providers of new and emerging technologies and services that could affect NS/EP would need to be conducted so that the NCM process and membership could be updated to ensure effective infrastructure protection planning and response. Lastly, the reporting and sharing of information raises important proprietary, antitrust, and security issues. The answers to questions regarding the handling and security of information are key enablers for industry participation in the NCM. Although, the private sector has significant concerns about Government and other private sector entities using reported information against individual companies, the success of the NSTAC has proven that acceptable solutions can be achieved.

A major point of the NCM/IA Policy report is that an extensive amount of work on critical infrastructure protection has been done in a relatively short amount of time by groups such as the Computer System Security and Privacy Advisory Board, the National Security Telecommunications and Information Systems Security Committee, and the PCCIP. In addition, numerous other groups, including the PCCIP Transition Team, will be concerned with further investigating infrastructure protection issues. The NCS and NSTAC process provides perhaps the best means to further investigate the NCM concept and coordinate the infrastructure protection activities outlined in this report. Since 1963, the NCS's interagency forum has effectively served as a focal point for industry-Government NS/EP telecommunications planning. Within this construct, the Government and the telecommunications industry have coordinated the appropriate policy and technical expertise to address the Nation's most critical telecommunications issues. Similarly, by expanding the scope of its outreach to address the changing national security

environment, the NSTAC and NCS are best positioned to coordinate individuals within the Government and industry that have the sufficient mission, policy, and management expertise across infrastructures to adequately address the Nation's critical infrastructure protection needs.

While the NCM concept raises challenging implementation questions, it provides a framework for the Federal Government and the private sector to begin to discuss solutions to growing infrastructure protection concerns. Much work is needed to resolve the critical issues involved with the sometimes competing equities of the Government and private sector. Each community has its own interests, one driven by national security concerns and the other driven by business issues. However, the end goal¢ effective, secure, interoperable, and reliable operations¢ is mutual. This common interest in having and planning for functional networks in times of crisis is the foundation from which the NSTAC and other stakeholders can further investigate the issue of an NCM for critical infrastructure protection.

4.0 RECOMMENDATIONS

4.1 NCC Vision Subgroup Recommendations

4.1.1 Recommendation for the President

The CONOPS requires that organizations report to the NCC intrusion incident information that meets jointly developed industry and Government standardized reporting criteria.

- **Recommendation**. The President establish a mechanism within the Federal Government with which the NCC can coordinate intrusion incident information issues and with which NSTAC groups can coordinate the development of standardized reporting criteria.

4.1.2 Recommendation for the NSTAC

The NCC should initiate an intrusion incident information processing pilot that builds on the NCC's existing rudimentary capabilities and on the ideas explored in the NCC CONOPS.

- **Recommendation.** The NSTAC endorse NCC implementation of an initial intrusion incident information processing pilot based on voluntary reporting by Government and industry.

4.1.3 Recommendations for the IES

The NCC Vision Subgroup has identified several issues that require significantly more study before the original charge can be completed. Subgroup membership may require change to draw in specific technical expertise. The subgroup plans to continue working with the Government to develop specific and standardized reporting criteria.

- **Recommendation.** The IES extend the NCC Vision Subgroup tasking into the next NSTAC cycle.

The subgroup revised Section 2.0, Mission and Purpose, and Section 3.0, Intent, of the *NCC Operational Guidelines* to reflect 13 years of operational experience.

- **Recommendation.** The IES approve the revised Section 2.0 and Section 3.0 of the *NCC Operational Guidelines.*

4.2 NCM/IA Policy Subgroup Recommendations

4.2.1 Recommendations for the President

- **Recommendations.** The President should direct appropriate departments and agencies to identify personnel within their respective department and agency that have the requisite policy, management, and mission expertise to work with the NCS and NSTAC in carrying out the following:

  - Continue to refine the NCM concept and postulate how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, R&D, standards, security investment, law enforcement capabilities, and the globalization of information systems.
  - Identify initial details of the NCM's formation and operation.
  - Explore the linkages within Government departments and agencies among infrastructures that will be essential to the NCM recommendation.
  - Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

4.2.2 Recommendations for the NSTAC

- **Recommendations.** The NSTAC should charge the IES to do the following:

  - Continue to refine the NCM concept and how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, R&D, standards, security investment, law enforcement capabilities, and the globalization of information systems.
  - Identify initial details of the NCM's formation and operation.
  - Explore the linkages with Government and between infrastructures that will be essential to the NCM recommendation.
  - Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

- Based on the outreach, develop a final recommendation as soon as possible, with interim status reports at intervening NSTAC meetings.

ANNEX A

Operations Support Group Members

Operations Support Group Members

COMSAT	Mr. Ernie Wallace, Vice-chair
EDS	Mr. Bob Donahue, Vice-chair
U S WEST	Mr. Jon Lofstedt, Vice-chair
AT&T	Mr. Dave Bush
CSC	Mr. Guy Copeland
GTE	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
MCI	Mr. Mike McPadden
NTA	Mr. Bob Burns
NORTEL	Dr. Jack Edwards
SAIC	Mr. Bill Deaver
TELEDISIC	Mr. Gordon Booker
UNISYS	Dr. Dan Wiener
USTA	Dr. Vern Junkmann

ANNEX B

The NCC Vision Subgroup Report

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NATIONAL COORDINATING CENTER FOR TELECOMMUNICATIONS VISION SUBGROUP REPORT

December 1997

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The President's National Security Telecommunications Advisory Committee's (NSTAC) National Coordinating Center for Telecommunications (NCC) Vision Subgroup was established in October 1996 as the NCC Vision Task Force to examine the NCC's future mission. This NCC Vision Subgroup Report presents the results of the subgroup's deliberations and assessments.

As a result of extensive analysis, interviews, and discussions over the last year, the NCC Vision Subgroup accomplished the following: (1) determined that an electronic intrusion incident information processing function is within the chartered responsibilities of the NCC; (2) revised Section 2.0, Mission and Purpose, and Section 3.0, Intent, of the *NCC Operational Guidelines* to reflect 13 years of operational experience; (3) determined the NCC's potential relationship with a national coordinating mechanism entity or process; (4) developed and approved the Draft Concept of Operations for an NCC Intrusion Incident Information Processing Function; and (5) developed Draft NCC Intrusion Incident Reporting Criteria and Format Guidelines as a basis for future work.

The subgroup found three specific issues that remain to be resolved:

- **Reporting criteria.** Identifying and obtaining agreement on the specific intrusion incident information required to develop indications and warnings.

- **Information sharing.** Identifying and obtaining agreement on the specific information that will be shared by industry and Government telecommunications service providers and network operators, and law enforcement, intelligence, and national security entities.

- **Value.** Defining the value added for industry participants in the intrusion incident information reporting process.

Resolution of these issues is necessary before determining future NCC resource requirements, such as membership, costs, and funding.

The subgroup concluded that the NCC can implement an initial intrusion incident information processing capability, but more study is needed to fully integrate an electronic intrusion incident information processing function into the NCC. The NCC is envisioned to serve as a focal point for receiving, screening, and processing electronic intrusion incident information for industry and Government telecommunications service providers and network operators. The subgroup recommends the following:

- NSTAC's Industry Executive Subcommittee (IES) extend the NCC Vision Subgroup tasking into the next NSTAC cycle.

- The IES approve the revised Section 2.0 and Section 3.0 of the *NCC Operational Guidelines.*

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

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

1.0 INTRODUCTION AND BACKGROUND

In January 1984, the National Coordinating Center for Telecommunications (NCC) began operations with a mission to assist in the initiation, coordination, restoration, and reconstitution of national security and emergency preparedness (NS/EP) telecommunications services or facilities under all conditions of crisis or emergency. Although the mission remains unaltered, the nature of NS/EP requirements and threats, as well as telecommunications technology and industry structure, has dramatically changed. In the spectrum of threats against the NS/EP telecommunications infrastructure, electronic intrusion and information attacks are of increasing concern.

In August 1996, the President's National Security Telecommunications Advisory Committee's (NSTAC) Issues Group reviewed the NCC's charter and mission. The group made an initial assessment that the NCC's mission and charter did not restrict the NCC from responding to electronic intrusion information and physical threats to networks. Because of the importance and operational nature of the NCC, the group recommended that a task force be formed to address its future capabilities.

In October 1996, the Industry Executive Subcommittee (IES) created the NCC Vision Task Force to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. As the task force formed, the Manager, National Communications System (NCS), requested that the NSTAC assist the NCS in developing a concept of operations (CONOPS) and implementing an electronic intrusion indications and reporting capability in the NCC. The Manager, NCS, also asked that the NCC's information assurance capabilities include the ability to evaluate intrusion incidents and to take mitigative actions against effects. The task force held its first meeting on November 15, 1996.

Concurrently, the Government formed an NCS NCC Vision Implementation Team to study the NCC's future mission. The team consisted of representatives from several Government departments and agencies, and provided valuable input and advice to the task force in joint industry and Government meetings. Additionally, the Manager, NCC, actively participated in discussions and analysis.

In April 1997, the IES was reorganized, and the Operations Support Group (OSG) was created. The OSG was assigned oversight of the NCC Vision Task Force and renamed the task force the NCC Vision Subgroup. The subgroup continued work on its original tasking with the same membership. The members and participants in the NCC Vision Subgroup and NCS NCC Vision Implementation Team are presented in Appendix A.

2.0 SUBGROUP CHARGE AND APPROACH

2.1 Charge

The IES formally charged the NCC Vision Subgroup to determine whether the mission, organization, and capabilities of the NCC should be changed, considering the ongoing changes in technology, industry composition, threats, and requirements. The subgroup was instructed to focus on three considerations and to develop recommendations for submission to NSTAC XX:

- NCC industry membership, given the impacts of the Telecommunications Act of 1996 on the composition of the providers of NS/EP telecommunications services to Federal, State, and local governments and the emergence of the national information infrastructure

- The NCC's role in relation to critical control networks of other infrastructures, such as electric power, oil and gas pipelines, financial services, and transportation

- NCC indications, detection, and warning functions and relationship to national information assurance activities, such as the President's Commission on Critical Infrastructure Protection (PCCIP).

The subgroup confirmed that the NCC Charter did not require revision and an electronic intrusion incident processing capability could be integrated into the NCC's functions. However, the subgroup found that the intrusion incident information reporting processes of the future NCC must be more clearly defined before the specific IES instructions could be fully addressed. The subgroup also monitored the efforts of the PCCIP, which was established to recommend national-level actions for protecting critical infrastructures and ensuring their continued operation. The PCCIP was scheduled to complete its mission in October 1997.

2.2 Approach

In November 1996, the subgroup began work with Government and industry NCC participants to establish a common level of understanding of the NCC's history and current operational environment. The subgroup examined the NCC's charter, the changing telecommunications environment, the threat to the NS/EP community, and interactions with other Federal organizations to determine what, if any, changes needed to be made to the NCC's membership, mission, and functions. The subgroup also reviewed the missions, functions, and capabilities of intrusion detection centers of the Federal Bureau of Investigation, National Security Agency, and Defense Information Systems Agency to determine the NCC's future role in relation to them. Following a briefing from the NSTAC's Intrusion Detection Subgroup, the subgroup agreed on the following definitions:

- **Intrusion.** Unauthorized access to or activity in an information system.

- **Intrusion Detection.** The process identifying that an intrusion has been attempted, is occurring, or has occurred.

- **Indication.** Information that suggests a threat.

- **Assessment.** Analysis of indications to determine the likelihood, nature, and potential of a threat.

- **Warning.** An advisory of the results of the assessment, likely target(s), and/or recommended actions.

The subgroup then formed a working group to analyze the 1984 NCC Charter and *NCC Operational Guidelines.* The working group determined that the NCC's mission and charter did not require change. Instead, based on 13 years of operational experience, the working group revised Section 2.0, Mission and Purpose, and Section 3.0, Intent, of the Operational Guidelines to include current terminology and to reference NCS programs initiated since 1984, such as the Telecommunications Service Priority System. The revised sections of the Operational Guidelines are presented as Appendix B. The working group also determined that charter functions were sufficiently broad for electronic intrusion indication, assessment, and warning to be integrated into the future NCC.

The working group also postulated the future NCC's external environment based on two premises: (1) the future NCC would continue its current functions and add an intrusion detection reporting capability, and (2) the future NCC could be an entity in a system of several NCC-like centers for other critical infrastructures. A national-level entity could oversee the critical infrastructure reporting centers and ensure coordination among them. The working group developed a model for a national coordinating mechanism (NCM) entity or process and provided the model to the OSG for consideration. This model is presented as Appendix C.[1]

Following the charter analysis, a second working group was formed to develop a detailed CONOPS for an NCC intrusion incident information processing function. The working group developed question sets regarding the future NCC to be answered by NCC industry and Government members. Responses were collected and incorporated into a CONOPS paper entitled *Draft Concept of Operations for a National Coordinating Center for Telecommunications Intrusion Incident Information Processing Function.* The CONOPS is presented as Appendix D.

In August 1997, the CONOPS was evaluated in an NCC Vision Tabletop Exercise. Participants represented industry, military, intelligence, and law enforcement. The purpose of the exercise was to assess the CONOPS in a simulated operational environment and to identify how

[1] The OSG created the NCM Subgroup in July 1997 to determine the need for and feasibility of a cross-infrastructure national coordinating mechanism. The joint NCM/Information Assurance Policy Subgroup report is presented as Appendix C of the OSG report.

the organizations defined in the plan could work together to respond to electronic intrusions. The exercise was conducted as a facilitated panel discussion.

Following the tabletop exercise, the NCC Vision Subgroup approved the *Draft NCC Intrusion Incident Information Reporting Criteria and Format Guidelines* to provide a framework for future development of specific reporting criteria and formats. The paper is presented as Appendix E.

3.0 SUBGROUP FINDINGS

Through analysis, interviews, and the tabletop exercise, the subgroup identified a general consensus among industry and Government that the CONOPS covered the basic elements for collecting, processing, and disseminating electronic intrusion information. The subgroup also found significant issues that must be resolved before industry, Government, and law enforcement, intelligence, and national security community entities could fully participate in the future NCC intrusion incident information process. As a result of its assessments of the NCC Charter, development and exercise of the CONOPS, and progress on the original tasking, the subgroup produced the following findings.

3.1 NCC Charter

The NCC's mission and charter do not require change. The charter functions are sufficiently broad for electronic intrusion indications, assessment, and warning to be integrated into the future NCC.

3.2 Reporting Criteria

The potential participants have not clearly defined the specific parameters and criteria required to report electronic intrusion information. They have not agreed on the specific outputs of the reporting process; therefore, it is not yet determined what to include in intrusion incident reports.

3.3 Information Sharing

The potential participants believe that the intrusion data available exceeds the technical capability to process it. They desire different types of intrusion information in various levels of detail. The subgroup noted that industry and Government detection capabilities vary because of different motivations and requirements. Concerns of industry include optimizing cost-effective business operations, protecting proprietary information, and ensuring network reliability and integrity. Industry participants would be interested in learning from the intelligence community about threats to corporate systems, and from the Government or other companies about any actions they could implement to avoid financial loss. Each community of interest considers certain information to be sensitive and proprietary to its organization or community. These reporting barriers include legal restrictions, security classification, and corporate policy.

3.4 Value

The potential participants found that the benefits of collecting and sharing electronic intrusion information must outweigh the costs of implementing such a system. Industry must be able to identify the value added before investing in an electronic intrusion information processing function. The efforts of various Government departments and agencies need to be coordinated to develop an indications, assessment, and warning information processing capability. Establishing such a capability would allow the Government to accrue a body of information useful to industry and Government.

3.5 Additional Issues

Other issues, such as future NCC membership, costs, and funding, can be addressed when the foregoing major issues are resolved. When the level of intrusion incident information to be reported in the future NCC is determined, the human, physical, and financial resources required to provide and process that information will be assessed. An implementation schedule can then be developed and operations begun.

4.0 SUBGROUP CONCLUSIONS AND RECOMMENDATIONS

4.1 Conclusions

The NCC is envisioned to serve as a focal point for receiving, screening, and processing electronic intrusion incident information for industry and Government telecommunications service providers and network operators. Although the subgroup concluded that the NCC can implement an initial intrusion incident information capability, more study is needed to fully integrate an electronic intrusion incident information processing function into the NCC. Implementing a pilot will provide the initial operational experience necessary to substantiate or refute the subgroup's findings.

4.2 Recommendations

4.2.1 The NCC Vision Subgroup

The NCC Vision Subgroup has identified several issues that require significantly more study before the original charge can be completed. Subgroup membership may require change to draw in specific technical expertise. The subgroup plans to continue working with the Government to develop specific and standardized reporting criteria.

- **Recommendation to the IES.** The IES extend the NCC Vision Subgroup tasking into the next NSTAC cycle.

4.2.2 Operational Guidelines

The subgroup revised Section 2.0, Mission and Purpose, and Section 3.0, Intent, of the *NCC Operational Guidelines* to reflect 13 years of operational experience.

- **Recommendation to the IES.** The IES approve the revised Section 2.0 and Section 3.0 of the 1984 *NCC Operational Guidelines.*

4.2.3 Intrusion Incident Information Processing Pilot

The NCC should initiate an intrusion incident information processing pilot that builds on the NCC's existing rudimentary capabilities and on the ideas explored in the NCC CONOPS.

- **Recommendation to the NSTAC.** The NSTAC endorse NCC implementation of an initial incident intrusion processing pilot based on voluntary reporting by Government and industry.

4.2.4 Reporting Criteria

The CONOPS requires that organizations report to the NCC intrusion incident information that meets jointly developed industry and Government standardized reporting criteria.

- **Recommendation to the President.** The President establish a mechanism within the Federal Government with which the NCC can coordinate intrusion incident information issues and with which NSTAC groups can coordinate the development of standardized reporting criteria.

APPENDIX A

NCC Vision Subgroup Members and NCS NCC Vision Implementation Team Members

NCC Vision Subgroup Members

COMSAT	Mr. Ernie Wallace, Co-chair
EDS	Mr. Bob Donahue, Co-chair
AT&T	Mr. Dave Bush
Boeing	Mr. Bob Steele
CTC	Mr. John Grimes
ESET	Mr. James Klugh
GTE	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
MCI	Mr. Mike McPadden
NORTEL	Dr. Jack Edwards
NTA	Mr. Bob Burns
SAIC	Mr. Bernie Ziegler
U S West	Mr. Jon Lofstedt
USTA	Dr. Vern Junkmann

NCS NCC Vision Implementation Team Members

DOC	Mr. Jorome Gibbon
DOD	Mr. Joe Frizzell
DOE	Mr. John Przysucha
DOJ	Mr. Wayne Williams
DOT	LCDR Rich Weigand
GSA	Mr. Tom Sellers
NCS	Mr. Bob DeVenny
NCS	Mr. Bernie Farrell
NRC	Mr. Peter Gness
NSA	Mr. R. Michael Green
NTIA	Mr. Bill Belote

Other contributors

AT&T Wireless	Mr. Myron Proefrock
NTA	Mr. Harry Underhill

Observers

DOS	Mr. Stephen Springer
USDA	Ms. Brenda Boger

APPENDIX B

Revised Sections 2.0 and 3.0 of the NCC Operational Guidelines

2.0 MISSION AND PURPOSE

The mission of the National Coordinating Center (NCC) is to ensure that the critical national security and emergency preparedness (NS/EP) telecommunications needs of the Nation can be and are met in any emergency or crisis situation, including natural disaster, technological disaster, terrorism, military action, and the disruption or degradation of the flow of critical information. The NCC will accomplish this mission through the coordination, fusion, and reporting of information associated with such emergency or crisis situations.

The purpose of this concept of operations is to further describe the functions identified in the NCC charter to be performed by the NCC. These functions were jointly developed by Government and industry as the set of activities which must be addressed at the national level to ensure the effective coordination of telecommunications support for NS/EP. The functions have been approved by the Executive Office of the President and the National Security Telecommunications Advisory Committee. This concept of operations outlines the methods by which they will be performed.

3.0 INTENT

The NCC must perform certain specified functions in fulfilling its NS/EP mission. Some of these functions will be addressed by the government personnel in the NCC while others are accomplished by the industry representatives. The methods used in performing the specified functions are relatively constant across the range of operational situations. In general, there are three levels of NCC activity. These are:

- Normal day-to-day operations which includes support for any NS/EP type emergency (as described in DCA circular 310-130-1 Chapter II, paragraph 2) or crisis short of a Presidential declaration of an emergency or disaster.

- Emergency and major disaster situations when a Presidential declaration has been issued (but short of a National Emergency).

- Wartime situations which follow the invocation of Section 706 of the Communications Act of 1934, as amended.

The NCC functions are presented below, along with a discussion of how each will be addressed by the personnel within the NCC. Performance of these functions will be consistent in all operational situations except as noted.

1) *Promptly provide technical analysis/damage assessment of service disruptions and identify necessary restoration actions.*

Each telecommunications carrier independently reports significant outages or disruptions which may affect National Security/Emergency Preparedness (NS/EP) Government telecommunications services to the industry representatives or NCC via any appropriate method (i.e., data links, private line facilities, facsimile or dial message communication facilities).

As required, the industry telecommunications carriers will conduct further investigations of service disruptions in conjunction with the Government personnel, and provide technical analysis/damage assessment of NS/EP service disruptions affecting multiple telecommunications carriers. Industry representatives will jointly identify restoration alternatives where disruptions affect multiple telecommunications carriers or where the affected telecommunications carrier's ability to restore itself is exhausted.

2) *Coordinate/direct prompt restoration of telecommunications services in support of NS/EP needs.*

The NCC becomes involved in restoration only when carriers cannot independently recover. Such involvement is triggered when one of the following operational situations occurs:

- Telecommunications industry entities request assistance or coordination.

- The affected Federal Government agency declares that existing procedures will not sufficiently restore NS/EP service.

- The scope of the NS/EP service or support requirements involves coordination among several areas, regions, industries or organizations.

The Manager, NCC prioritizes Federal Government NS/EP telecommunications service requirements (using the assigned restoration priorities as a guide), confers with appropriate industry representatives on proposed courses of action and obtains suggested alternatives for restoration of services. Industry representatives determine available resources (e.g., facilities, equipment and personnel) and estimated response times. The Manager, NCC forwards alternatives to the affected Government entity for decision. Affected Government entity then issues orders via the normal contracting official.

The Manager, NCC coordinates multicarrier and inter-LATA restoration through interaction with company representatives or the industry entity holding the communications service authorization for the specific service. The representatives interface with their respective company(s) to expedite and provide status on restoration actions.

After Section 706 is invoked, the Manager, NCC provides direction, consistent with Government authority, and with advice and assistance from the industry representatives, for the restoration of NS/EP service via the most expeditious means in accordance with the established Telecommunications Service Priority (TSP) regulations. The Manager, NCC also allocates resources, as appropriate, under the same provisions. Each carrier performs its own restoration activities consistent with instructions issued by the Manager, NCC and within the limitations of unassigned resources remaining, as a result of direction from the Manager, NCC and reports progress to the NCC.

Under other than wartime conditions, the NCC may, with advice and assistance from industry representatives, coordinate rather than direct NS/EP service restoration via the most expeditious means in accordance with the established TSP regulations.

3) *Develop and exercise comprehensive service restoration plans.*

It is the responsibility of each industry entity to have plans in place for its own restorations. With advice and assistance from Industry representatives, the Manager, NCC develops plans for the restoration of NS/EP services and expeditiously disseminates them via appropriate communications methods. Such plans will be developed in accordance with applicable service restoration regulations (e.g., TSP) and will be based on the comprehensive service restoration plans of the industry entities, drawing on their expertise and internal assistance as appropriate.

After consultation with industry representatives, the Manager, NCC can dynamically reassign priorities consistent with Government authority and in accordance with established service restoration regulations as situations dictate. These assignments are made through interaction with appropriate industry representatives.

The Manager, NCC, with advice and assistance from industry, plans, conducts, evaluates and disseminates (with due consideration for the protection of proprietary information) results from exercises designed to test restoration plans. Industry participates in such exercises to the extent reasonably necessary, employing company restoration plans as guidelines to respond to exercise scenarios and attempting to ensure no interruption of service. Results of these exercises will be analyzed and used by Government and industry to evaluate and improve restoration plans.

4) *Develop "watch center" type function to work through cooperating industry operations centers to effectively monitor the status of essential telecommunications facilities.*

Via appropriate communications means from individual Government and industry telecommunications organizations, the NCC watch center expeditiously receives status and situation reports on disruptions which may affect NS/EP service and jointly assesses them. Industry representatives will interact with their respective operation centers/organizations to provide information about their respective facilities.

Planning to support NCC operational missions and requirements is accomplished by the joint Government/industry NCC staff. Industry representatives will assist in the formulation and enhancement of plans and procedures for the center and will maintain contact with their appropriate planning staff.

5) *Maintain access to an accurate inventory of the minimum essential equipment, personnel, and other resources which are available for restoration operations to include the location and capabilities of all industry's network operations centers (NOCs).*

The NCC watch center receives appropriate traffic and facility data directly from individual carriers' databases through the representatives. Industry will develop and maintain, in a mutually acceptable form, information reflecting:

- A list of current contacts and their locations, which include appropriate liaison points in each company
- Inventories of restoration resources and equipment, including their location and status, to support their allocation during an emergency/disaster situation
- Restoration plans for facilities with significant numbers of TSP services.

Representatives will have access to sufficient databases and monitoring capabilities — either onsite or accessible by appropriate electronic means — to allow them to participate in joint

situational analysis and alternative identifying sessions. Industry responds to requests for information from the Manager, NCC under appropriate NS/EP situations.

6) *Identify liaison points in each company.*

The industry representatives are the primary industry points-of-contact under all operational situations. These representatives will provide the Manager, NCC a detailed listing of corporate locations and appropriate contact names and numbers within their companies, and the organizations they represent, for use during periods when the primary point-of-contact is not available.

The Manager, NCC will maintain contact lists of suppliers of services and equipment for those entities not represented in the NCC. Points-of-contact within appropriate Government organizations will also be maintained.

7) *Maintain ability to rapidly transfer operations from normal to emergency operations.*

Industry representatives are available 24-hours-a-day, 7-days-a-week. Under situations other than invocation of Section 706, the implementation of emergency operating procedures is accomplished in accordance with the National Plan for Communications Support in Emergencies and Major Disasters. Industry representatives will be cognizant of individual company emergency operating procedures and will ensure continuity of NCC support and responses to emergency requests. After Section 706 is invoked, the implementation of emergency operation procedures is accomplished in accordance with applicable Federal emergency plans. Industry entities will staff alternate NCC locations when operational situations warrant. The relocation of industry NOCs and other key facilities will be exercised independently in response to NCC notification.

8) *Coordinate/direct and expedite the installation of new orders for service when the services required are critical to NS/EP needs.*

Individual Federal agencies determine their requirements for new service and place orders in accordance with the normal acquisition process. All necessary orders, contracts and other documentation will flow through the normal procurement process to the maximum extent possible.

Copies of requirements for critical new NS/EP service may be forwarded to the Manager, NCC for referral to appropriate industry representatives when normal processes are insufficient. The representative will act as liaison and expediter, following established internal company procedures, and will track the installation of critical facilities, providing appropriate status information to the Manager, NCC.

After Section 706 is invoked, the Manager, NCC with advice and assistance from the industry entities, ascertains the most expeditious alternatives available for providing the required critical services. The Manager, NCC selects from the alternatives and issues appropriate directions, consistent with Federal Government authority, to the involved industry entities. These

entities, with NCC assistance as required, coordinate activities among themselves, effect the required installation, and provide status reports to the NCC as needed. A coordinating industry entity may be designated by the Manager, NCC, if appropriate.

Under situations other than the invocation of Section 706, the Manager, NCC uses the above procedure, or, as appropriate, bypasses the collection of alternatives since the choices are more diverse than in a Section 706 situation where damage is more likely to be widespread and severe. The Manager, NCC forwards alternatives to affected Government entities for decision. The affected Government entity then issues orders via normal contract officials.

9) *Contribute to 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.*

The operational planning function for the NCC is done jointly by industry and Government under the leadership of the Manager, NCC. Industry representatives will have ready access to the technical resources of their companies and will provide appropriate liaison for planning activities undertaken by the NCC.

Other planning for the National Coordinating Mechanism (e.g., development of technical standards) comprises a separate function independent of NCC operational requirements and is accomplished outside the NCC. Such planning will be done jointly by industry and Government under the leadership of the Government. Strong liaison with existing or new industry standards organizations must be maintained.

The application of technical standards and other national network planning guidelines will be independently undertaken by industry on a voluntary or contractual basis, or under regulatory oversight. Industry representatives will provide status information on implementation in support of NS/EP requirements as appropriate.

10) *Coordinate/direct network reconfiguration plans in support of NS/EP needs.*

It is the responsibility of each industry entity to have plans in place for its own restorations. The Manager, NCC reviews restoration plans which impact NS/EP, protecting all proprietary information as specified in Section 6.0 of the *1984 National Coordinating Center Operational Guidelines* and any implementing procedures.

The Manager, NCC will develop and maintain a computerized database on all of the nation's telecommunications resources to assist in performing survivability and reconstitution planning.

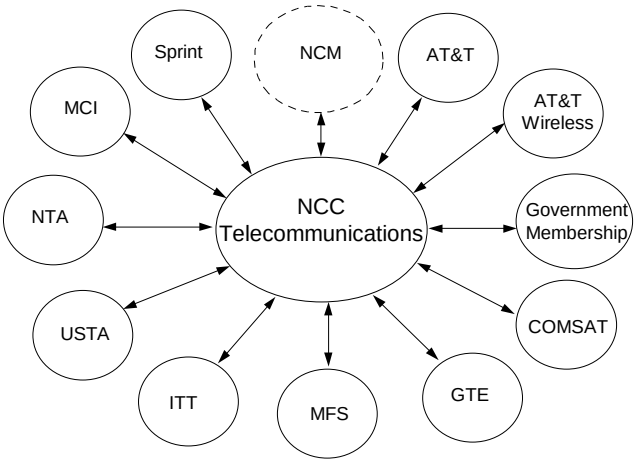
The NCC will coordinate the development of joint restoration plans to be enacted after Section 706 is invoked. This will be accomplished under the leadership of the Manager, NCC with advice and assistance from industry representatives. The representatives will consider

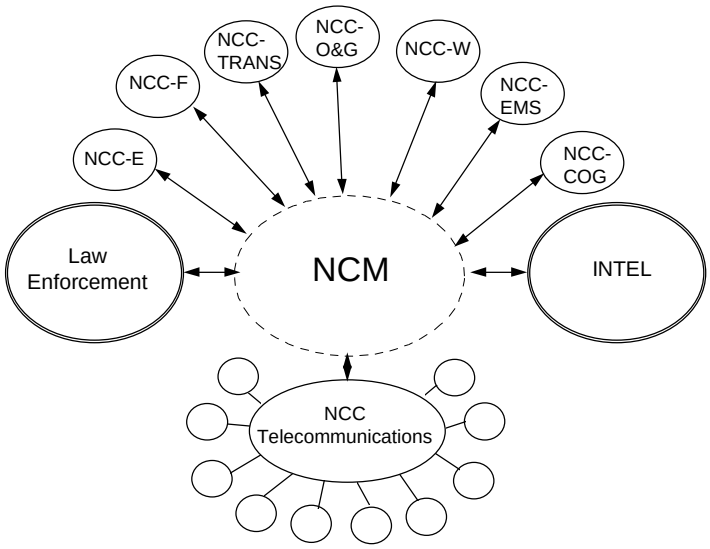
internal company restoration policies, plans and procedures and will expand on plans to encompass intercarrier restoration alternatives as well as restoration using other facilities.

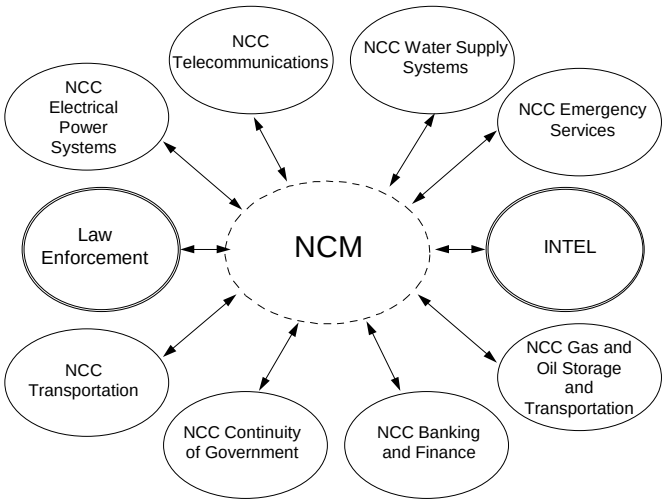
The NCC network reconfiguration planning function may encompass Government and industry networks and/or systems and, in all cases, is accomplished under the direction of the Manager, NCC with input from industry.

APPENDIX C

The NCC/NCM Organizational Relationship


Sprint
NCM
AT&T
MCI
AT&T Wireless
NTA
NCC Telecommunications
Government Membership
USTA
COMSAT
ITT
MFS
GTE


NCC-TRANS
NCC-O&G
NCC-W
NCC-F
NCC-EMS
NCC-E
NCC-COG
Law Enforcement
NCM
INTEL
NCC Telecommunications


NCC Telecommunications
NCC Water Supply Systems
NCC Electrical Power Systems
NCC Emergency Services
Law Enforcement
NCM
INTEL
NCC Transportation
NCC Gas and Oil Storage and Transportation
NCC Continuity of Government
NCC Banking and Finance

APPENDIX D

Draft Concept of Operations for an NCC Intrusion Incident Information Processing Function

TABLE OF CONTENTS

1.0 PURPOSE

This document proposes a Concept of Operations (CONOPS) for the National Coordinating Center for Telecommunications (NCC) to incorporate an intrusion incident information processing function into the existing NCC mission. For the purposes of this document an incident also includes (a) denial/disruption of service and (b) breaches in communications and data security. The CONOPS supports the goals of the overall intrusion incident information process reflected below.

- Identify new or resurrected intrusions into telecommunications infrastructures and inform the telecommunications industry
- Identify a concerted attack on the telecommunications infrastructure to facilitate implementation of mitigation strategies
- Alert law enforcement of intrusions involving illegal or terrorist activities
- Identify the precursor to a full-fledged information warfare incident and alert the appropriate Government and industry infrastructures.

2.0 SCOPE

This CONOPS will apply to all resident and nonresident Government and industry members of the NCC. Other Government and industry organizations operating networks, contracting for the operation of networks, and/or reviewing and analyzing intrusion activity will be encouraged to support the NCC intrusion incident information processing function described in this CONOPS.

3.0 INTRODUCTION

"If there is a doorway into a system, you can be assured that someone is knocking on the door." This quotation from a telecommunications network security expert summarizes the state of affairs between computer systems and those who attempt to gain unauthorized access into those systems.

The development of an intrusion incident information process in the NCC could provide a number of benefits to both Government and industry. A number of these are listed below.

- Provide ready access to near real-time intrusion information
- Provide a process to detect intrusion patterns against networks
- Provide a joint center to coordinate response to a coordinated intrusion attack against networks
- Facilitate coordination with appropriate intelligence and law enforcement agencies

- Address the national emphasis and growing concern over critical infrastructure protection.

In order for the process described in this CONOPS to be effective, both Government and industry must freely share threat, vulnerability, and intrusion information. A hesitancy on either side to do so will cause the process to falter. Neither side will receive the value added from the process needed to make it a success.

4.0 DEFINITIONS

The following definitions apply in this CONOPS.

- **Intrusion**[1]**.** Unauthorized electronic access to or activity in an information system.
- **Intrusion Detection.** The process of identifying that an intrusion has been attempted, is occurring, or has occurred.
- **Indication.** Information that suggests a threat.
- **Assessment.** Analysis of indications to determine the likelihood, nature, and potential of a threat.
- **Warning.** An advisory of the results of the assessment, likely target(s), and/or recommended actions.

5.0 NCC INFORMATION REQUIREMENTS

NCC information collection will focus on the receipt of near real-time reports and assessments by Government and industry of intrusions that may affect network integrity and performance. Under this CONOPS, the NCC serves as a focal point for telecommunications infrastructure information flowing among the Federal Government departments and agencies, telecommunications service providers, telecommunications-related user groups, and other organizations reviewing and analyzing intrusion activity. The NCC must also have the information available to allow it to detect patterns of intrusion attacks against telecommunications networks and issue appropriate warnings.

Organizations will report to the NCC intrusion incident information using established reporting criteria (to be jointly developed by a Government/telecommunications industry task force.) Information from any Government, industry, or private organization on system vulnerabilities, or on indications, assessments, and warnings as defined above will be integrated

[1] For the purposes of this document intrusion also includes (a) denial/disruption of service and (b) breaches in communications and data security.

into the NCC information and report process. General types of information that the NCC will seek to collect include the following:

- Information on an intrusion affecting, or potentially affecting, the telecommunications infrastructure
- Type and characteristics of the attacked network
- Method of intrusion to include a description of the vulnerability exploited
- Determination on objectives of the intrusion
- Impact on networks and NS/EP telecommunications
- Information on recommended defenses and/or corrective actions
- Recommendations to preclude a similar intrusion in the future
- Other types of information deemed appropriate.

6.0 INTRUSION INCIDENT REPORTING

To perform its intrusion incident information processing function, the NCC will collect information from all appropriate sources. The report processing system must be capable of appropriately handling classified and proprietary information and operate in near real-time. The value of intrusion information decreases rapidly as the time required to process it increases. Reports from industry will normally be unclassified. Many companies will not be capable of classified reporting.

Though not all inclusive, Figure 1 provides a representative list of organizations that will be encouraged to submit reports. Organizations include Government telecommunications users, telecommunications service providers and vendors, intelligence and law enforcement organizations, and user groups. Other sources may be used as well. As part of its day-to-day activities, the NCC will review any available Federal intelligence reports for indicators and information on possible network attacks that might amplify, clarify or support individual incident reports.

After a rapid organizational assessment of a network intrusion and a determination that it meets jointly developed reporting criteria, individual Government departments and agencies and telecommunications service providers will report an intrusion in near real-time using appropriate means. This CONOPS assumes the availability of a mutually agreeable intrusion reporting methodology and criteria (to be developed by a joint Government/telecommunications industry task force) supported by appropriate communications means. Reports might address incidents of

denial/disruption of service which include the physical disabling of equipment or the flooding of communications networks by waves of message traffic. Also, incidents might be reported involving breaches in communications and data security that affect the confidentiality, integrity, or availability of information, data, or a program or system. In this case, attacks on the end-user's data and control systems managing the data would be of particular interest. Data attacks lead to the unauthorized monitoring/copying/disclosure of end-user data, whereas attacks on control systems managing the data could exploit the so-called trap door to hijack a session in progress or insert Trojan horses.

Organizations with resident representatives at the NCC will submit reports through those representatives. All other organizations will submit reports directly to the Manager, NCC. It will be desirable for the reporting entity to electronically transmit the initial report to the NCC representative or Manager, NCC, as soon as possible. Movement of the report within the NCC, between infrastructures, and from infrastructures to a National Coordinating Mechanism (NCM) (if established) will use appropriate electronic media. Reports of intrusions should use the following format and include the minimum essential information elements shown to facilitate the collation, assessment, and distribution of the information.

- Type of System Attacked
- Analysis of Intrusion Incident
- Implications of Intrusion Incident
- Assessment of Damage
- Response Actions Taken.

This information will support a near real-time NCC assessment of the impact of the incident or a series of incidents on the integrity of the telecommunications infrastructure.

Examples of Organizations That May Report Information to the NCC

- Government
  - Users
  - FBI Computer Investigations and Critical Infrastructure Threat Assessment Center (CITAC)
  - Infrastructure Protection Task Force (IPTF)
  - NSA National Security Operations Center (NSOC)
  - DISA Global Operations and Security Center (GOSC)
  - DISA Defense Intrusion, Analysis and Monitoring Desk (DIAMOND)
  - GSA Center for NSEP
  - FEMA National Network Operations Center (NNOC)

- Telecommunications Service Providers
  - AT&T
  - COMSAT
  - CSC
  - EDS
  - GTE
  - ITT
  - MCI
  - NTA
  - Sprint
  - USTA Member Companies
  - WorldCom

- Telecommunications Equipment Vendors
  - Lucent
  - Nortel
  - Siemens
  - Ericsson

- User Groups
  - Network Security Information Exchange (NSIE)
  - Computer Emergency Response Team (CERT)
  - Forum of Incident Response and Security Teams (FIRST)

- Others
  - NSTAC Member Companies

7.0 INTRUSION INCIDENT INFORMATION ASSESSMENT METHODOLOGY

To maximize the overall value of intrusion information, an incident must be evaluated to determine what was done, how it was done, how it might be prevented, and, if possible why it was done. Any intrusion incident could potentially go through three separate assessments - originating organization, NCC, and national level.

The initial assessment to determine if the intrusion incident meets the reporting criteria and should be forwarded to the NCC will be made within the telecommunications or Government entity experiencing the incident. If an incident is reported, the NCC will process it to accomplish two things: (1) detect intrusion patterns against networks; and (2) organize and format the data for ease of access and use by authorized organizations. Whenever appropriate, the NCC will sanitize information it receives to ensure the anonymity of the organization attacked. The NCC also will categorize incident reports according to the type of network against which the intrusion attack was directed.

NCC staff will compare new reports with information contained in existing NCC report files, with reports from other sources including intelligence organizations, and with information contained in the NSIE vulnerability and incident databases. The information will then be assessed to determine potential intrusion trends within network types. If the NCC requires additional expertise for its trend analysis, the staff will consult Government/industry NSIEs.

The NCC representative for the reporting entity or, in the event the reporting entity is not represented in the NCC, the NCC staff will perform a secondary assessment to determine if any or all of the following actions are appropriate:

- Report the incident as appropriate to some or all other entities participating in the NCC
- Report the incident as appropriate to other Government and industry infrastructure organizations
- Report the incident as appropriate to an NCM (if established).

The final assessment will be done by an NCM (if established) to determine its impact on national security.

8.0 NCC DISTRIBUTION OF PROCESSED INFORMATION

The NCC will make incident reports available through appropriate means. The NCC will organize intrusion information to ensure easy access by authorized users and will store it in a data file to allow remote access. This will allow authorized Government and industry users to find intrusion information concerning their particular network configuration. Users will forward general or incident-specific questions to the NCC.

Alerts from within the infrastructure or originating from an NCM (if established) should be transmitted to the entities within the infrastructure by appropriate means with a "read receipt" capability if possible. As a minimum, the NCC will provide details of the attacks and an assessment of the impact of the attacks on NS/EP telecommunications capabilities. If the receipt is not returned within a specified period, a follow-up call should be placed from the NCC to the appropriate point of contact within the entity.

A secure bulletin board for incident summary information might be desirable but such a data source would certainly present a prime target for hackers. A secure means for handling access to the data must be identified or developed. If such a capability is deemed necessary, it should be established and maintained by the NCC for retrieval of information on demand by specified personnel through secure means. Such information would not be of immediate urgency but rather in the category of an after action summary report, sorted and indexed for ease of use.

APPENDIX E

Draft NCC Intrusion Incident Reporting Criteria and Format Guidelines

As of October 3, 1997

DRAFT

NCC INTRUSION INCIDENT REPORTING CRITERIA AND FORMAT GUIDELINES

1.0 GENERAL

Keep in mind that NCC intrusion information collection focuses on the receipt of near real-time reports and assessments by Government and Industry of intrusions that may directly or indirectly affect network integrity and performance involving the telecommunications sector of the critical national infrastructures

Report the incident as soon as possible even though the available information is incomplete

Report to the NCC (If your organization is one with a resident representative at the NCC, report through the resident representative; otherwise, report directly to the NCC)

Report using appropriate means

2.0 REPORTING CRITERIA

Report an intrusion incident concerning an intrusion (unauthorized electronic access to or activity in an information system to include denial/disruption of service as well as breaches in communications or data security) whenever you:

- Detect an intrusion occurred of a nature that you did not previously report, e.g.:
  - Report denial/disruption of service incidents such as the physical disabling of equipment, the flooding of a communications network by waves of message traffic, etc.
  - Report breaches in communications or data security that affect the confidentiality, integrity, or availability to an authorized user of information, data, or a program or system.
- Receive any indication (information that suggests a threat) of a planned intrusion on a Federal government or public information system or network supporting the telecommunications sector of the critical national infrastructure

3.0 REPORTING STAGES

Provide an initial intrusion incident report upon determining that an intrusion occurred

Provide subsequent interim report(s) as appropriate upon determining more relevant facts concerning the intrusion

Provide a final report upon incident closure

4.0 REPORTING FORMAT

An initial report should include the first category of information, i.e., Type of System Attacked or Intruded, and any other categories for which information is known. Any interim report(s) should include additional information placed in the appropriate categories as it is determined . The final report should include all five categories of information as follows:

- **Type of System Attacked or Intruded.** Describe the specific type of network/system, etc. involved in the intrusion in general (e.g., Netware NT network) and more specifically (e.g., security classification of the network or system such as Secret, the function/mission system running on the attacked network/system, the IP address as applicable, etc.)

- **Analysis of Intrusion Incident.** Describe as well as possible the nature of the intrusion (i.e., what happened and how it happened {e.g., specify how the intruder gained access to the network or system, the particular vulnerability exploited, how it was exploited}); specify when the intrusion occurred; specify any known source of the intrusion; specify any known intent, purpose, or motivation for the intrusion such as to corrupt or destroy data, manipulate data, achieve unauthorized access to data, block authorized access to data, etc.; and provide any other pertinent information

  Note: Report the incident as soon as possible even though the available analysis information is incomplete; provide interim reports as well as the final report later.

- **Implications of Intrusion Incident.** Describe any known potential implications of the intrusion for other network/system providers and users

- **Assessment of Damage.** Provide a succinct assessment of the actual damage/impact that resulted from the intrusion (e.g., corrupted or compromised data, etc.)

- **Response Actions.** Describe relevant actions taken or planned to correct the exposed vulnerabilities, repair any damage, etc. emphasizing any recommendations to preclude a similar intrusion in the future

5.0 INCIDENT REPORT PROCESSING AND DISTRIBUTION

When an initial report is received by the NCC, the Manager, NCC, and the NCC Representative receiving the report will determine its sensitivity. The NCC Representative will sanitize the report as necessary to protect the reporting company or its customers. NCC personnel will then enter the report contents into the NCC Intrusion Incident Database. NCC personnel will process all reports to:

- Correlate information with any other similar incidents to see if a pattern can be determined
- Determine to whom the report should be distributed
- Organize and format releasable information for ease of access and use.

As soon as meaningful information on an incident is available (this may be only after interim reports are received), NCC personnel will distribute it to NCC Government and Industry Representatives, and other authorized users based on established user profiles. This approach will allow users to receive only incident information that they find useful. NCC personnel will give special attention to providing appropriately formatted reports to the National Coordinating Mechanism (if activated), the FBI CITAC, and the NSA NSOC.

As the NCC receives interim reports and a final report on the incident, NCC personnel will update the incident database file and process the information again. NCC personnel will acknowledge, in writing (e.g., fax, e-mail, etc.), receipt of all reports received.

NCC personnel will forward appropriate reports to the NSIE. As a general rule, the NSIE will receive reports requiring special technical expertise or lengthy analysis, a consolidated incident initial/interim/final report, and any other previously agreed upon report.

ANNEX C

Information Assurance: A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION ASSURANCE:
A Joint Report of the IA Policy Subgroup of the Information Infrastructure Group and the NCM Subgroup of the Operations Support Group

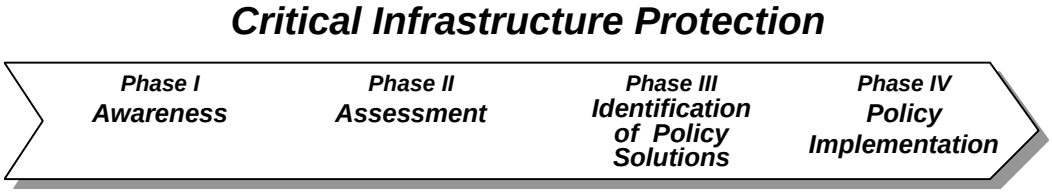
December 1997

TABLE OF CONTENTS

1.0 INTRODUCTION

In the spring of 1997, the President's National Security Telecommunications Advisory Committee's (NSTAC) Information Infrastructure Group (IIG) established the Information Assurance Policy Subgroup to develop an Information Assurance Policy Report based on the findings of NSTAC risk assessments, the lessons learned from other NSTAC outreach activities, the findings and recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) as available, and other relevant activities. In the development of its report, the subgroup was also to consider the implications of critical infrastructure interdependencies. In addition, the NSTAC's Operations Support Group (OSG) created the National Coordinating Mechanism subgroup to investigate issues regarding a mechanism or process to coordinate information sharing between critical infrastructures and the Federal Government.

As a realization of those efforts, this report organizes and identifies common issues and policy solutions regarding the protection of the Nation's critical infrastructures. An extensive amount of work on critical infrastructure protection has been done in a relatively short amount of time by government policy-makers, law enforcement officials, the defense and intelligence communities, academia, and the private sector. This level of effort undoubtedly reflects the increasingly important role the Nation's infrastructures are playing in national security. Numerous reports, briefings, meeting minutes, and other documentation have been developed in the investigation of the infrastructure assurance issue. Although stakeholders may have particular sensitivities or perspectives driven by mission or business pressures, there are common and crosscutting observations and conclusions within these reports. It is the purpose of this report to highlight those commonalities.



A brief history of the information assurance (IA) and infrastructure protection issue will provide the context for discussion of policy solutions to the problem. For illustrative purposes, noteworthy critical infrastructure protection activities and events are categorized into four general phases. Phase I is Awareness, which encompasses the period or series of events leading to a heightened awareness and identification of the critical infrastructure protection issue. The second phase is Assessment, in which various organizations and entities, in response to Phase I, have attempted to quantify and qualify the risks and vulnerabilities associated with the Nation's most critical infrastructures. Phase III, the Identification of Policy Solutions, is this paper's primary focus. Finally, Phase IV is Policy Implementation, which has yet to occur.

2.0 CRITICAL INFRASTRUCTURE PROTECTION EVOLUTION

2.1 Awareness

In 1991, the National Research Council (NRC) published the report, "Computers at Risk: Safe Computing in the Information Age." The NRC report served notice that the nation was becoming more dependent upon computers often without adequate security measures. The report claimed, "As computer systems become more prevalent, sophisticated, embedded in physical processes and interconnected, society becomes more and more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems."[1] The report advocated the creation of generally accepted system security principles, the establishment of a system-incident data repository, appropriate education and training to promote awareness and an Information Security Foundation (ISF) which would promote computer security design, selection and use of computer systems in the nonmilitary and commercial sectors.[2] The NRC report generated a great deal of interest in both the Government and private sectors, alerting everyone to potential dangers.

The unfortunate events surrounding the bombing of the World Trade Center on September 26, 1993, The Aum Supreme Truth cult nerve gas attack upon the Tokyo subway system on March 20, 1995, and the bombing of Alfred Murrah Federal Building in Oklahoma City on April 19, 1995, brought about action by the Federal Government to incorporate the findings of the NRC report with the possibility of terrorist actions against the Nation's critical infrastructures. These events created an environment of heightened awareness in regard to the vulnerability of the critical infrastructures. In this environment, the President signed Presidential Decision Directive (PDD) 39, a classified directive describing the Administration's counterterrorism policy. In an unclassified portion of PDD-39, the President directed the Attorney General to "chair a Cabinet Committee to review the vulnerability to terrorism of…critical national infrastructures and make recommendations to the President and the appropriate Cabinet member or Agency head" on how to protect those infrastructures. Accordingly, in 1995, the Attorney General established a small interagency task force led by the Department of Justice, called the Critical Infrastructure Working Group (CIWG). The CIWG's mission was as follows:

- Identify critical infrastructures and assess in broad terms the scope and nature of threats to those infrastructures
- Survey the existing mechanisms in the government for addressing those threats
- Propose options for a full-time group that will consider how the Government should address threats to critical infrastructures over the long term

---

1 *The National Research Council*, Computers at Risk: Safe Computing in the Information Age, *Washington DC; National Academy Press, 1991. p. 1.*

2 *Ibid. p. 179.*

- Propose solutions for how the Government should address the threat in the interim.[3]

The CIWG concluded that although there were actually many pockets of expertise on critical infrastructure protection within the existing intelligence, law enforcement, and defense communities, there was no central coordinating mechanism among these communities. In addition, the CIWG concluded that an unprecedented amount of private sector participation would be required to adequately address the evolving problem. During the Cold War, the intelligence community, with the help of the Department of Defense, had indications, warning, and attack assessment responsibilities. These responsibilities primarily focused on what would likely be physical attacks by foreign aircraft or missiles. As this threat environment has slowly changed including, in particular, the growing development and deployment of sophisticated information warfare techniques, infrastructure protection has begun to move out of the traditional, classified intelligence environment and into a more open forum. This is largely a reflection of the belief that interference with U.S. infrastructures will likely involve an attack on privately owned commercial networks, systems, and facilities.

In January 1995, during the 17th meeting of the NSTAC, the Director of the National Security Agency briefed the NSTAC principals on threats to U.S. information systems and the need to improve security of the Nation's critical infrastructures. The NSTAC principals discussed those issues and subsequently sent a letter in March of that year to the President, stating that "the integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack…[and that] other national infrastructures … [such as finance, air traffic, power, etc.] also depend on reliable and secure information systems, and could be at risk."[4] The President replied that he would "welcome the NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications systems.[5] The President further asked "the NSTAC principals—with input from the full range of users of the national information infrastructure (NII)—to provide me with your assessment of the national security and emergency preparedness requirements for our rapidly evolving information environment."[6] In May 1995, the NSTAC established the Information Assurance Task Force (IATF) which later became the Information Infrastructure Group, to work with the Government to identify critical national infrastructures and to act as the focal point for NSTAC's information assurance activities. The task force recommended that electric power, financial services, and transportation infrastructures be studied to assess and raise awareness of their dependence on telecommunications and information systems. NSTAC was already engaged in an assessment of the risk to the telecommunications infrastructure, which was subsequently published in December

---

3 *Jamie Gorelick, U.S. Deputy Attorney General;* Statement Before the Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations, *July 16, 1996.*

4 Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States, *March 20, 1995.*

5 Letter from the President of the United States to the NSTAC, *July 7, 1995.*

6 *Ibid.*

1995: *An Assessment of the Risk to the Security of the Public Networks*, prepared by the U.S. Government and NSTAC Network Security Information Exchanges.

In addition, the U.S. Congress was becoming aware of and concerned with the potential risks facing the Nation's vital infrastructures. In August 1995, an amendment, sponsored by U.S. Senator Jon Kyl (R-AZ), was added to the National Defense Authorization Act for fiscal year 1996; it called for a report from the White House setting forth the following information:

- The national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attacks by foreign nations, groups, or individuals, or any other entity against the national information infrastructure.

- The future of the National Communications System (NCS), which has performed the central role in ensuring national security and emergency preparedness communications for essential United States Government and private sector users, including, specifically, a discussion of —

  - whether there is a federal interest in expanding or modernizing the NCS in light of the strategic national security environment and the revolution in information technologies; and

  - best use of the NCS and the assets and experience it represents as an integral part of the larger national strategy to protect the United States from strategic attacks on the national information infrastructure.[7]

The bill was signed into law on February 10, 1996. Additional legislative language clarifying the original Kyl Amendment was added to the following year's National Defense Authorization bill. The provision specifically called for—

- A description of the national policy and plans to meet essential Government and civilian needs during a national security emergency associated with a strategic attack on elements of the national infrastructure the functioning of which depends on networked computer systems.

- The identification of information infrastructure functions that must be performed during such an emergency.

- The assignment of responsibilities to Federal departments and agencies, and a description of the roles of Government and industry, relating to

[7] Section 1053, National Defense Authorization Act of FY 1996, *Public Law 104-106.*

> indications and warning of; assessment of ; response to, and reconstitution after, potential strategic attacks on the critical national infrastructures described under paragraph 1.[8]

In the summer of 1996, the Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations heard from representatives of the executive and legislative branches, private industry, and academia during a series of hearings on "Security in Cyberspace." Facts pointed out in testimony during the hearings made national news, but last minute cancellations by some private sector witnesses also demonstrated the concerns that private industry has with sharing sensitive information with the Government. An article submitted for the official committee record and published in the *IEEE Technology and Society Magazine*, summarizes the complexity of the issues raised in the hearings.

> By their nature, developments in cyberspace blur the distinction between crime and warfare, thereby also blurring the distinction between police responsibilities to protect U.S. interests from criminal acts in cyberspace, and military responsibilities to protect U.S. interests from acts of war in cyberspace. In addition, providing protection against transnational threats in cyberspace, and apprehending their perpetrators, frequently goes well beyond the reach and resources of local and regional authorities.
>
> These two characteristics of security in cyberspace—the blurring of the distinction between crime and warfare, and the transnational nature of many security incidents—raise new questions regarding the proper roles and missions in cyberspace security and safety. Some of the agencies, organizations, and institutions that have essential roles to play include: the U.S. Federal Government, U.S. state and local governments, nongovernmental/private organizations, Governments of other nations, and International organizations. Today, this is "everybody's" problem, and therefore, "nobody's" problem. It falls into all of the cracks.[9]

The subcommittee's hearings were a milestone in the Awareness phase of the infrastructure protection policy issue. Many of the same actors began longer term assessment activities which have led to the development of policy solutions. The next section highlights some of these activities.

2.2 Assessment

On July 15, 1996, the day before the final Senate hearing on "Security in Cyberspace," the Clinton administration issued Executive Order 13010, *Critical Infrastructure Protection*. The executive order immediately established PCCIP to do the following:

---

8 Section 1022, National Defense Authorization Act of FY 1997, *Public Law 104-201.*

9 *Richard Hundley and Robert Anderson, "Emerging Challenge: Security and Safety in Cyberspace,"* IEEE Technology and Society Magazine, *Vol. 14, No. 4 (Winter 1995-1996) pp. 19-28.*

- Assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures

- Determine what legal and policy issues are raised by efforts to protect critical infrastructures

- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation

- Propose any statutory or regulatory changes necessary to effect its recommendations.

The PCCIP was designed to be a joint Government/industry commission, chaired full-time by a private sector representative and composed of representatives nominated by the heads of 10 different Federal departments and agencies. The executive order identified eight infrastructures that were considered "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[10] These infrastructures are telecommunications, electric power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. To achieve their goal for an integrated national plan for strategic defense of the Nation's critical infrastructures, the commission has undertaken considerable study, consultation, training, gaming, Government/industry discussion, outreach, technology design, testing and implementation, and dissemination of threat data. Since its establishment, the PCCIP has regularly briefed NSTAC working levels and coordinated with the NSTAC on risk assessment projects. The PCCIP final report was submitted October 22, 1997.

While the PCCIP was developing its report, the executive order provided for a temporary Infrastructure Protection Task Force (IPTF) to perform a variety of functions. The IPTF was to increase coordination of existing infrastructure protection efforts and expertise within and outside the Federal Government to—

- Provide and coordinate the provision of expert guidance on critical infrastructures to detect, prevent, halt, or confine an attack and to recover and restore service

- Provide training and education on methods of reducing vulnerabilities and responding to attacks on critical infrastructures

- Conduct after-action analysis to determine possible future threats, targets, or methods of attack

- Coordinate with the pertinent law enforcement authorities during or after an attack to facilitate any resulting criminal investigation.

10 *Executive Order 13010,* Critical Infrastructure Protection, *July 15, 1996.*

In recent years, NSTAC task forces have been engaged in a variety of projects focused on information systems security and critical infrastructure risk protection. First, the National Information Infrastructure Task Force (NIITF) investigated the advisability of establishing an Information Systems Security Board (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 information products and services.[11] The Federal Advisory Committee Act (FACA) prohibits NSTAC from implementing an ISSB. The NIITF worked closely with non-NSTAC organizations during its investigation of the ISSB issue.

From this effort, the Information Security Exploratory Committee (ISEC)—a private sector consortium of hardware and software vendors, major users of information technology, and other interested stakeholders—was formed to further investigate the ISSB concept, functionality, and implementation issues. The ISEC will be issuing a final report in the fall of 1997.

At NSTAC XIX in March 1997, the Honorable Janet Reno, U.S. Attorney General, highlighted the need to explore a more effective approach to the issues of cyber security and crime. The Department of Justice, concerned with developing an appropriate state-of-the-art capacity to deal with those issues, believed that building trust and developing a partnership with industry was essential. The NSTAC members agreed and welcomed the opportunity to cooperate with law enforcement on developing a better means for deterring and prosecuting cyber crimes. Ms. Reno also stated that she had encouraged the Federal Bureau of Investigation to share more information with industry. NSTAC members agreed to forward their suggestions to Ms. Reno on how law enforcement and industry could work together to deter cyber attacks and protect the Nation's information infrastructure. The NSTAC's IIG created the Cyber Crime Subgroup to address these issues.

In addition, the NSTAC's IATF and IIG, have been conducting risk assessments of the electric power, financial services, and transportation infrastructures to—

- Assess the security and robustness of the particular infrastructures at the national level relative to the identified threats to their networks and information systems
- Determine the risks to the industries that derive from their dependence on the telecommunications infrastructure
- Examine the implications of trends regarding the industries' use of information systems and networks.

[11] *For a more detailed discussion of the ISSB, see the* NIITF Report to NSTAC XIX, *March 1997.*

As a result of these projects, the NSTAC has forwarded several reports and recommendations to the President on enhancing information security and infrastructure protection.[12]

In previous years, the NSTAC has also worked on a bilateral basis with the electric power industry to investigate electric power and telecommunications restoration procedures. In 1990, the NSTAC recommended that the Government establish a program to provide priority electric power restoration and fuel distribution to critical telecommunications users and providers. In 1991, a second NSTAC Energy Task Force was formed to advise the Government on the implementation of energy priority initiatives for national security and emergency preparedness telecommunications facilities. The reactivated task force assisted in developing the Department of Energy's Telecommunications Electric Service Priority (TESP) initiative in response to the recommendation of the original task force.

In addition to the PCCIP and NSTAC activities, a host of other organizations and individuals have contributed to the Assessment phase of the critical infrastructure protection issue. Some of these efforts date back to the late 1980s with the evolving realization of the possible threats to the information infrastructure—

- Congress established the Computer System Security and Privacy Advisory Board (CSSPAB) as a public advisory board in the Computer Security Act of 1987. The Board is composed of 12 members who are recognized experts in the fields of computer and telecommunications systems security and technology. CSSPAB advises the National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), the National Security Agency (NSA), and the Secretary of Commerce on emerging security issues pertaining to federal computer systems.

- The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established by a classified Presidential directive entitled *National Policy for the Security of National Security Telecommunications and Information Systems.* That directive clarified the division of responsibilities between the NIST and the NSA with respect to promulgating telecommunications and information systems security policy for the U.S. Government. The NSTISSC is currently examining a number of issues, including information assurance; education, training, and awareness; and improving information security products and services.

- The Defense Science Board issued a report in November 1996 on defensive information warfare. The report asserted that, "the national security posture of the United States is becoming increasingly dependent on U.S. and international infrastructure. These infrastructures are highly interdependent, particularly because of the inter-netted nature of the information components and because of their reliance on

[12] *See NIITF Final Report, March 1997; IATF* Electric Power Risk Assessment, *March 1997; IIG* Financial Services Risk Assessment, *October 1997; RVWG* A Nation's Information at Risk: National Information Infrastructure Risk Assessment, *February 1996.*

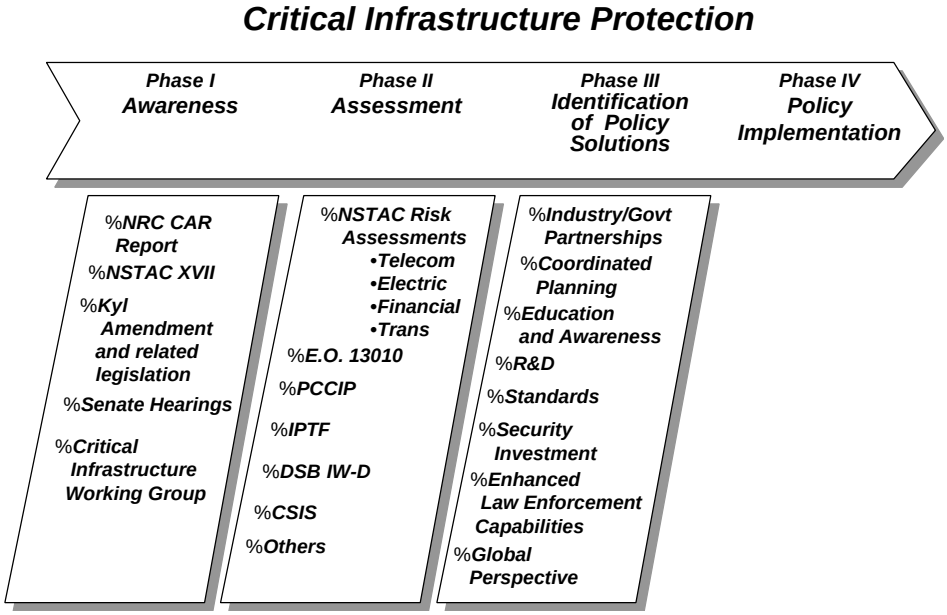
the national information infrastructure."[13] The report concluded that the information infrastructures are vulnerable and the linkages between the information infrastructures and critical infrastructures have increased the potential of the information warfare threat. The report made several recommendations, such as increasing awareness, assessing dependencies and vulnerabilities, focusing research and development (R&D) and to participate fully in critical infrastructure protection.

Efforts by industry and academia have added to the magnitude of assessment of critical infrastructure protection. The Center for Strategic and International Studies at Stanford University has an Information Warfare/Information Assurance Task Force working on a report on critical infrastructure protection. Stanford Research Institutes International Information Integrity Institute (SRI - I4) an independent, non-profit membership organization provides forums, best practices with regard to information security and integrity programs, on-site clinics, a public awareness program, and various other programs aimed at addressing information security concerns for the private sector. The Manhattan Cyber Project, an initiative of War Room Research, LLC in cooperation with various organizations within industry, government and academia, was launched in June 1997 to gather data in on the cyber threat. Numerous other workshops and games/simulations run by academic institutions, such as the Sandia Institute, have contributed to the debate. In order to develop policy solutions, it is necessary to piece together commonalities between the various reports written with regard to the protection of the Nation's critical infrastructures. The next section begins to piece those commonalities together.

3.0 IDENTIFICATION OF POLICY SOLUTIONS

The efforts of the many organizations and individuals outlined in Phases I and II have led to important findings, conclusions, and recommendations. The purpose of this section is to highlight those commonalities that are evident from studying the documentation produced by these groups. The commonalities can be grouped into several categories: Industry/Government Partnerships, Coordinated Planning, Education and Awareness, Research and Development, Standards, Security Investment, Enhanced Law Enforcement Capabilities, and Global Perspective. Each category is fully addressed below.

[13] *Office of the Under Secretary of Defense for Acquisition & Technology.* Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D). *November 1996.*



3.1 Industry/Government Partnerships

Nothing is more recognized in any critical infrastructure policy discussion than the need for stronger partnerships among the public and private entities that are called upon to maintain the Nation's critical infrastructures. Infrastructure systems incorporate a mix of public and private ownership entities that bring to the table varying approaches with regard to security and protection. Stephen Lukasik of the Stanford University Center for International Security and Arms Control points to a dichotomy of public and private ownership of infrastructure systems. "Private owners, faced with loss of revenue and loss of confidence by their customers, regulators, investors, and insurers, will seek to restore revenue and customer confidence, satisfy regulators, document losses and avoid liability. Governments will focus on protecting national security, preventing future attacks, and identifying and punishing attackers."[14] Deputy Attorney General Jamie Gorelick, alluded to the varying interests of private and public concerns by noting that infrastructure protection is, "difficult because ownership of critical infrastructures is largely in private hands. Absent statutory authority to regulate a particular industry, the government has limited authority to require private companies to take protective measures; it can merely advise industry and urge it to 'do the right thing.'" [15]

As a result of the dichotomy of interests, there are differing definitions of what constitutes a threat. The private sector rationally concludes that it cannot invest to protect against all threats, a conclusion generally based on an analysis of the risks and a determination that response measures are generally more cost effective in dealing with significant outages. The current

---

[14] *Stephen J Lukasic.* Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure. Prepared for presentation at the Workshop on Protecting and Assuring Critical National Infrastructure, May 1997, *p. 2.*

[15] *Jamie Gorelick, U.S. Deputy Attorney General;* Statement Before the Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations, *July 16, 1996, p. 12.*

regulatory environment has fundamentally changed, relying more upon market forces and private decision making. As Lukasic claims, "In the face of needs to address system issues, we find ourselves having dismantled much of the regulatory machinery that could otherwise have been employed."[16]

While there is little question of the Government's role in protecting the Nation's infrastructure against physical attack, there is a lack of trust toward the Government in regard to its role. This mistrust is generally driven by fears of infringements of privacy, questions of free speech rights, and concerns about hampering economic competitiveness. As a result, the responsibility for regulating the infrastructures is fragmented among various levels of government, industries, and private companies. Joe Bankoff of King & Spalding summed up the mistrust as follows:

> Frequently the limitation on the use, development and protection of our technical resources is not a technology barrier. It is frequently a political and legal issue driven by economic and political interests and fueled by a healthy distrust and concern about change and uncertainty about the impact of new technologies.[17]

Any solution to the protection of the critical infrastructures requires the participation of private industry working in concert with Government. A great deal of the technological expertise resides in the private sector, and no analysis would be complete without thorough information regarding what attacks have been experienced by the private sector. Such cooperation and free flow of ideas are likely to engender trust and understanding between Government and industry that is absent in the current environment with the notable exception of the NSTAC/NCS partnership. In testimony before the PCCIP in Atlanta, Gary McConnell, director of the Georgia Emergency Management Agency (GEMA), stated:

> There is a tremendous void, we've found, in this area of any one central place for everybody to sit down and talk about those issues. The private corporations certainly know what their conditions are, what to be on the lookout for. Government on some level knows some of that. The information is there. It has been developed. I think our greatest challenge in actually doing it is providing the forum for everybody to sit down and share that information and to look at issues.[18]

The NSTAC/NCS partnership is an exceptional example of successful industry/Government partnership. Since 1982, the NSTAC has worked cooperatively with the NCS, an interagency consortium of Federal departments and agencies that serves

---

16 *Lukasic, p. 21.*

17 *Joe Bankoff*. Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Atlanta, GA, April 18, 1997, *p. 29.*

18 *Gary McConnell*. Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Atlanta, GA, April 18, 1997, *p. 18.*

as a focal point for industry-Government national security and emergency preparedness (NS/EP) planning.

- Cooperation and coordination among the various parties responsible for the protection of Nation's infrastructures have been widely recommended.

- At the PCCIP Strategic Simulation for Critical Infrastructure Protection held on June 29 through July 2, 1997, the concept of a National Infrastructure Coordination Center—a consortium with industry and Government, created to share information received substantial support from private sector participants in the game.[19]

- The NSTAC Information Assurance Task Force Electric Power Risk Assessment recommended the establishment of an NSTAC-like advisory committee to enhance Government/industry cooperation and provide a forum for information sharing for the electric power industry.[20]

- The NSTAC Financial Services Risk Assessment Report recommended that, "The President should assign to the appropriate department or agency the mission of identifying threats and risk mitigation to the financial services infrastructure and facilitating the sharing of meaningful and timely information between government and industry."[21]

- Findings of the National Information Infrastructure Risk Assessment included, "a need to establish a mechanism to support the information exchange process."[22]

- Robert Anderson of the RAND Corporation testified before the Senate Permanent Subcommittee on Investigations, "There are examples in which government and industry have worked and are now working together effectively, such as in improving the safety of automobiles and the commercial airline industry. Such continuing cooperation, focused on safety and security, is needed today across all aspects of our national information infrastructure, including energy distribution, transportation control systems, financial networks, the traditional telecommunications and inter-networking sectors."[23]

---

19 *Booz; Allen & Hamilton*, "PCCIP Strategic Simulation Briefing to the NSTAC Industry Executive Subcommittee Working Session," *August 19, 1997.*

20 *NSTAC.* Information Assurance Task Force Report, *March 1997, p. C.30.*

21 *NSTAC Information Infrastructure Group*. Financial Services Risk Assessment., *October 1997, p. 7.1.*

22 *NSTAC Reliability and Vulnerability Work Group,* A Nation's Information at Risk: National Information Infrastructure Risk Assessment, *February 29, 1996, p. 125.*

23 *Robert Anderson.*, Testimony before the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, 104th Congress, June 25, 1996, *p. 113.*

To fill the void caused by a lack of interaction between industry and Government, a cooperative partnership based upon trust and the two-way flow of information needs to be established. Robert Marsh, Chairman of the PCCIP, points out, "Cooperation between the public and private sectors is essential to the success of critical infrastructure protection."[24]

3.2 Coordinated Planning

Infrastructures have become more sophisticated and mutually dependent. This interdependence has brought to the forefront a need to coordinate infrastructure-wide consequence management for infrastructure protection and restoration in the event of natural disasters, criminal or terrorist actions. Such coordination needs to incorporate all levels of Government and private industry. Large-scale, infrastructure-wide emergency planning needs to be reexamined and updated. The last time such an examination took place was during the civil defense efforts that took place during the beginning of the Cold War.[25] The growing reliance upon the telecommunications system and the use of more automated systems suggest that a new approach needs to be investigated.

Currently, there is no single Government entity charged with coordinating the protection and emergency response to an attack on our critical infrastructures. Rather, there are various agencies, committees and organizations that have authority over certain parts of the infrastructure but which lack central responsibility to establish direction and coordinate emergency response planning. A similar lack of coordination exists in the private sector. As Deputy Attorney General Gorelick said, "While some individual companies have taken steps to secure their own information and communication systems from intrusion, few industries have taken an industry-wide approach to the problem."[26] An exception would be the telecommunications industry which has worked with the Federal Government in establishing emergency preparedness procedures through NSTAC.

There have been several circumstances where the resources of the Federal, State, and local emergency response organizations and private entities have been brought together to plan a coordinated emergency strategy. The latest example of such coordination came about in the planning for the 1996 Olympic Games in Atlanta. For the two years prior to the start of the Olympics, studies on the protection of critical infrastructures at the Olympic Games were conducted in coordination with the Federal Bureau of Investigation, various State and local agencies, and private entities, such as the Georgia Power Company. Mock exercises ranging from massive power outages, water supply poisonings, and bombings were conducted in order to craft a well-designed, carefully executed security plan. Major Jon Gordon of the Atlanta Police Department and the chairman of the committee on interagency preparations summed up the coordination

---

[24] *Robert Marsh*. Transcript of hearing held by the President's Commission on Critical Infrastructure Protection. Los Angeles, CA. March 13, 1997, *p. 4.*

[25] *Lukasik, p. 18.*

[26] *Gorelick, op. cit., p. 14.*

effort when he said, "The 1996 Summer Olympic Games was a showcase of interagency coordination between and among the Federal, State, and local public safety agencies and it was a showcase for public-private partnerships."[27]

New York City has also recognized the need for enhanced coordination and cooperation. Broad-based emergency planning across infrastructures has been consolidated under the mayor's Office of Emergency Management. The Office of Emergency Management developed a partnership with the Consolidated Edison Company of New York in order to bring about a coordinated communication protocol for emergencies and potential emergencies.[28] Other cities such as Los Angeles have developed a defense mechanism to address emergency situations such as earthquakes and fires, that involve coordination among Government and private entities. Los Angeles Department of Water and Power (DWP) recently developed an emergency control center to allow for a single point of coordination with the city's emergency operation center. Marcie Edwards of DWP comments that, "This particular entity provides us with the most rapid methodology to respond in an emergency to have an adequate infrastructure response in terms of management, dissemination of the media and prioritization of load restoration."[29]

The challenge is to bring about widespread, cross-infrastructure coordination at the national level. At the national level, the Government can investigate the nature of threats, vulnerabilities, and responses through research and analysis and coordinate exercises that bring public and private parties together to achieve a greater understanding of real-world threats, constraints, and limitations. Gaps in planning and knowledge can be pinpointed and actions can be taken. Local government officials and private companies, largely responsible for the daily operation of the Nation's critical infrastructures, would benefit from strong national level coordination of emergency planning. Deputy Attorney General Gorelick suggested a "Manhattan Project" for infrastructure protection.[30] This would involve a cooperative venture between the various levels of government and private companies in order to take advantage of the expertise brought to the table and devise solutions to infrastructure planning and the coordination of emergency response.

3.3 Education and Awareness

Coordinated ventures between Government and private companies, important in planning emergency response procedures, are also important in enhancing the awareness and knowledge of the threats facing the critical infrastructures. While awareness is

---

27 *Jon Gordon*, Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Atlanta, GA, April 18, 1997, *p. 27.*

28 *Lou Rana*. Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Boston, MA. June 6, 1997, *p. 19.*

29 *Marcie Edwards*, Transcript of hearing held by the President's Commission on Critical Infrastructure Protection. Los Angeles, CA., March 13, 1997, *p. 29.*

30 *Gorelick, op. cit., p.16.*

important, the Government must go about clearly defining what constitutes a threat. As Stephen Lukasic observed, "There are two ways to help people appreciate the magnitude of electronic and cyber threats. One learns by being burned, and inevitably much public appreciation will come the hard way. The other way is to learn through information and warnings."[31] There has been a widespread call for greater education and awareness about the risks facing critical infrastructures. In testimony during the Senate "Security in Cyberspace" hearings, a witness stated that, "There will not be a plateau with information system developments during which the existing problems can be solved. I believe the only viable solution is the development of a framework for a continuing partnership between government and industry within which new vulnerabilities and risks can be addressed as they are encountered."[32] Dr. Hugh Stevens of the University of Houston challenged the PCCIP to create, "An entity charged with extensive collection of detailed information necessary for comprehensive risk assessment associated with critical infrastructures."[33]

There is a growing need to raise consciousness within the entities charged with enhancing the infrastructure protection. A clearer definition of the threat to the infrastructures is necessary. Private entities and the Government clearly differ relative to the perceived magnitude of the threat to the critical infrastructures. In conducting research for the NSTAC Financial Services Risk Assessment, interviewers asked institutions, "What could the Federal Government do to help you improve the security of your systems?" A common response was, "Provide more information on threats."[34] Representatives of the financial services industry were unwilling to completely accept the notion of "an electronic Pearl Harbor" absent any credible evidence that such a threat existed. Institutions are asking, "Are there threats the government knows that I don't know about?"[35]

The NSTAC Financial Services Risk Assessment recommended that the President assign to an agency the duty of identifying threats and risk mitigation to the financial services infrastructure and facilitating the sharing of meaningful information between the Government and industry.[36] It is time to consider expanding the task of such an agency beyond the financial services infrastructure to embrace all of the critical infrastructures. In much the same way as threats against the President are documented and assessed, threats against components of the infrastructure should be.[37] Aided by this documentation, law enforcement, industry, and regulatory agencies can then apply their expertise and manage the response to the threats.

---

31 *Lukasic, op. cit., p. 8.*

32 *Robert Anderson,* Testimony before the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. 104th Congress, June 25, 1996, *p. 112.*

33 *Hugh Stephens.* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection. Houston, TX, May 13, 1997, *p. 55.*

34 *NSTAC,* Financial Services Risk Assessment, *p. 3.6.*

35 *Ibid., p. 3.6.*

36 *Ibid., p. 7.1.*

37 *Lukasic, op. cit., p. 6.*

It is essential to consider the rapid advancement in new technologies, the new vulnerabilities presented, and the increasing skill of potential adversaries taking advantage of the vulnerabilities. Enhanced awareness of potential vulnerabilities and early warning of potential attacks could diminish the potential for losses. For this awareness to be brought about, vigorous reporting of systems attacks is necessary. As Lukasic points out, "A benefit of such central reporting and analysis of real or suspected attacks on infrastructure information systems is that timely warning of other parts of the affected infrastructure becomes possible."[38]

Important parameters need to be established with regard to any type of central reporting mechanism. For such central reporting and analysis to work properly, the private sector and the Government need to be forthcoming in the reporting of incidents. It is essential that steps are taken to ensure that proprietary data are handled on a non-attribution basis and not released. Furthermore, all competitors must provide the same level of information.[39]

Increased awareness is essential in narrowing the gap between industry and Government with regard to the perceived threat to the infrastructures. Industry is not convinced there is a need to allocate additional resources toward protection. Only when the full range of incidents are reported, analyzed, and subsequently shared among Government and industry can the full nature of perceived threats to the infrastructure be understood.

The need for stronger education and awareness with regard to the threat to the Nation's infrastructures goes beyond the needs of Government and industry to share information. If the Government is looking to increase security awareness and training, it needs to give strong consideration to creating a career track for computer security professionals. Daniel Gelber, Chief Counsel to the Minority for the Senate Permanent Subcommittee on Investigations alluded to a concern that, "there is no security culture within the Government."[40] Gelber recommends that, "we (the Government) need to maintain a better pool of security professionals and generally improve the consciousness of users."[41] A concern within the government is that computer security professionals may be enticed to leave their government positions to accept higher paying positions with greater advancement in the private sector, thereby losing institutional and corporate knowledge. The Minority Report to the Senate Permanent Subcommittee on Investigations advocated

---

38 *Lukasic, op. cit., p. 14.*

39 *Booz, Allen & Hamilton.*, Briefing to the Industry Executive Subcommittee Working Session, *August 19, 1997.*

40 *Daniel Gelber,* Testimony before the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs. 104th Congress, June 5, 1996, *p. 53.*

41 *Ibid., p. 55.*

the creation of a Government Computer Security Specialist Career Field that included opportunities for career progression and provided specialized career training.[42]

In order to enhance the security culture with regard to the Nation's critical infrastructure, Government and industry could use help from academia in creating college-level programs that specialize in information security. As Wayne Clough, President of the Georgia Institute of Technology says, "We need to develop the means to protect our virtual systems and ensure access to education about infrastructure for the generations that are coming to our campus as well as those who come and then graduate."[43] Examples of comprehensive computer security training programs include the COAST program at Purdue University and the Software Engineering Institute at Carnegie Mellon University. Most universities have computer science departments. In order to increase the number of computer security professionals in Government and industry, more computer science departments need to offer programs that specialize in security training.

The public needs greater education in computer security and awareness of the potential cyber threats and how those threats affect our infrastructure systems. U.S. Attorney Richard Poehling told the PCCIP that computer crime is on the rise. As such, he pointed out a "need to advance educational initiatives to educate the public to the scope and nature of the problem."[44] Poehling advocates an idea of a C.A.R.E program for computer abuse, based upon the Drug Abuse Resistance Education (D.A.R.E) program used with respect to drug abuse. Most people know that it is illegal to open someone else's postal mail; however, the public awareness with regard to computer crime is lacking. A public awareness program could educate the public on improper conduct with computers, deter some people from breaking the law, and keep the public informed on security concerns. Mohammed Noori, a professor at Worcester Polytechnic Institute, recommends that public awareness exercises reach beyond computer education. He points to a need for "an educational paradigm for civil infrastructure systems, inclusive, that takes into account education at K2 through 12, education, undergraduate and graduate students."[45]

3.4 Research and Development

As the technology supporting the Nation's critical infrastructure has advanced, there has been a growing call for more R&D in the area of infrastructure defense. Hugh Stevens believes that, "It is clear that many of the solutions to infrastructure problems

---

42 *Staff Statement, U.S. Senate Permanent Subcommittee on Investigations (Minority Staff), Hearings on Security in Cyberspace, June 5, 1996, p. 33.*

43 *Wayne Clough,* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection. Atlanta, CA, April 18, 1997, *p. 17.*

44 *Richard Poehling.* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, St. Louis, MO, June 19, 1997, *p. 7.*

45 *Mohammed Noori,* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection. Boston, MA, June 6, 1997, *p. 38.*

require new ideas, research and perhaps new ways of looking at old solutions."[46] The National Science Foundation, in its report, *Technology for a Sustainable Future*, drew upon four key areas that should frame R&D efforts. These areas were an examination of deterioration science, an assessment of technologies, a look at renewal engineering, and an assessment of the economic and social aspects of civil infrastructure systems.[47] With the recent advances in information technology, it is also important that proper consideration be given to research into computer security, hacker techniques, and computer network intrusion detection.

Undertaking a new approach toward R&D requires joint efforts among Government, industry, and academia. Partnerships are becoming essential as the Federal government continues to downsize. Wayne Clough claims that, "There are serious issues facing this country if we're going to continue our research efforts because the Federal Government is downsizing its funding for research and development."[48] While a great deal of research can be undertaken by private industry, the Government plays a vital role in funding system level R&D through system simulation and testing. Mohammed Noori, professor at Worcester Polytechnic Institute, observes that, "Partnership can be a key element."[49] A leading example of Government and academia cooperation is the Computer Emergency Response Team (CERT) at the Software Engineering Institute, a federally-funded R&D center at the Carnegie Mellon University. The primary mission of the CERT is to respond to security emergencies on the Internet, identify problems with the technology, warn network security administrators of vulnerabilities to attack.[50] The Federal partnership with the Carnegie Mellon University's CERT is often looked at as an example of how the government can reach into the private sector to take advantage of R&D expertise not found in the public sector.

Another positive example of a partnership incorporating Government, industry and academia has been forged in Southern California with regard to creating innovations with the local transportation infrastructure. Representatives from the University of California—Los Angeles, University of Southern California, University of California—San Diego, Caltech, the U.S. Department of Transportation, Federal Highway Administration, Caltrans, Science Applications International Corporation and other industry partners have been brought together to conduct R&D with the goal of updating the transportation system in Southern California.[51] The example established by these partnerships could be expanded to include a broader range of infrastructures so that the necessary R&D of

---

46 *Stephens, p. 57.*

47 *Noori, op. cit., p. 37.*

48 *Clough, op. cit., p. 15.*

49 *Ibid. p. 38.*

50 *Richard Pethia,* Testimony before the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, 104th Congress, June 5, 1996, *p. 65.*

51 *Frieder Siebel,* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Los Angeles, CA, March 13, 1997, *p. 17.*

innovative technologies could be conducted to address the problems faced by the Nation's critical infrastructures.

William Mayfield and Ron Ross have recommended to the PCCIP that a National R&D Program for Infrastructure Assurance involving Government, industry, and academia should be established for the following reasons:

- Risks cut across the public and private sectors.
- Much of the relevant technical and empirical data on infrastructure operations, interdependencies, and vulnerabilities are held by the private sector.
- Training, education, and awareness programs are needed to develop a cadre of knowledgeable infrastructure assurance practitioners.
- Successful implementation will require closer cooperation between Government, industry, and academia.

Furthermore, it was recommended that Government departments and agencies be designated to manage infrastructure-specific R&D efforts. The National R&D Program for Infrastructure Assurance would promote the "science" of complex, interdependent systems and conduct in-depth research that addresses national infrastructure issues.[52]

Arguably, the most likely beneficiaries of coordinated infrastructure assurance R&D are the users of Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are ubiquitous in the electric power, transportation, and telecommunications industries. NSTAC risk assessments of electric power and transportation highlighted the need for specific attention to the importance of secure SCADA systems. In the electric power and rail industry, SCADA systems provide valuable data that are essential to regulate systems, ensure balance, and facilitate generation and transmission. The electric power SCADA system usually consists of a host or master computer, one or more field data-gathering and control units, and a collection of standard or custom software used to monitor and control remote field data elements. SCADA systems may have 30,000 to 50,000 data collection points and may transmit analog information as well as digital or status information (e.g., breaker open/close state).[53]

SCADA systems used by the pipeline industry also consist of sensors, computers, telecommunication links, and other servo-mechanisms that allow control centers to manage operating parameter throughout the system. These systems permit remote control of valves, compressors, and other critical pipeline components. In the pipeline industry,

---

[52] *William Mayfield and Ron Ross*, Evolving a National Information Assurance Research Agenda: Issues and Opinions from Commercial Information Technology Providers.

[53] *NSTAC*, Electric Power Information Assurance Risk Assessment Report, 1996.

dedicated microwave links are primarily used in SCADA systems due to the predominance of uninhabited and extremely rough terrain. The repeaters of these systems often reside on large towers that are susceptible to physical attack. Destruction of SCADA systems would result in serious damage to pipeline operations.[54] Although each industry has taken steps to enhance the reliability and robustness of SCADA systems, an opportunity clearly exists for coordinating R&D of such systems and their security. Such coordination should result in development cost savings and perhaps even lower production costs due to economies of scale.

3.5 Standards

A significant amount of work is being done regarding information security standards. However, consumers are often left with only the assurance of the manufacturers or systems integrators that their networks or systems are secure. At the PCCIP public meeting in Houston, Texas, Dr. Mitchell Morris of the Anderson Cancer Center expressed the concerns of the medical community as it increasingly deploys advanced information systems and technology.

> With a new paradigm of information technology, there are three major developments that expose Americans to risk, and these must be addressed. One is the computer-based patient record, another is telemedicine, and the third is health care networks…An area not completely evaluated is standards of electronics and physical characteristics of the data and systems that use it and transmit it. What are the standards to prevent hackers from getting in? What security measures should be in place? We need to define the required redundancy of systems such as the backups that need to be established and so forth.[55]

Ms. Roberta Croce, Director of Information Sciences of Boston University, also testified before the PCCIP for the need for certification and threshold security requirements for commercial information security products.[56] As mentioned previously, the NSTAC NII Task Force-led ISSB project and the independent ISEC have been focused on the concept of an entity to promote information systems security principles and standards to improve the reliability and trustworthiness of information products and services available in the commercial marketplace. The NII Task Force contacted more than 100 major information technology companies, industry associations, Government agencies, and major information technology users to solicit comments on the concept and determine the extent of support for the ISSB. The outreach effort revealed broad and general support for the ISSB among diverse industry groups and surfaced various questions and issues related to the ISSB implementation, such as the appropriate role of the

---

[54] *Reliability and Vulnerability Working Group,* NII Risk Assessment: A Nation's Information at Risk, *February 29, 1996.*

[55] *Dr. Mitchell Morris, Anderson Cancer Center*, Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Houston, TX, May 13, 1997.

[56] *Ms. Roberta Croce.* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Boston, MA, June 6, 1997.

Government, its relationship with ongoing standards activities, and the international implications of the ISSB. The task force determined that the private sector is capable of establishing and operating the ISSB, and the NSTAC recommended at NSTAC XIX in March 1997, that the President endorse the private sector ISSB initiative.[57]

The establishment and continued evolution of commercial information systems security best practices will facilitate education across infrastructures of the proper stewardship of computers and the networks they compose. Although there are many standards organizations, the decentralized nature of the activity also has a diluting effect in terms of recognition and consumer confidence. The concept of a commercial sector focal point should continue to be investigated.

3.6 Security Investment

It was pointed out earlier that Government has not adequately defined what constitutes a threat in order to convince industry to invest additional funds beyond what normal business case dictates. Industry may be unwilling to incur additional costs to protect its systems at a higher level against malicious attack if there is insufficient indications that such attacks will occur. The business pressures of operating in competitive environments will likely limit the funds available to secure their systems. Therefore, Government could follow two courses of action in the process of enhancing security— increase regulation or offer incentives. Richard Pethia pointed out, "It is going to be the marketplace that drives this process to a successful completion. In the meantime, some rules, policies, regulations and mechanisms might help, but I think that in the end, it is going to require the marketplace to respond to this problem. That means the people who need security are going to have to recognize that need and be willing to invest in it."[58] In gaming activities held by the PCCIP, industry leaders appeared to agree with the contention that investing in security needs to be market driven, with little Government regulation. If Government wants to raise the level of protection, industry looks for the Government to offer incentives, regulatory relief or loan guarantees.

3.7 Enhanced Law Enforcement Capabilities

U.S. attorneys are reporting a rising number of referrals from the FBI with regard to the use of computers to commit crimes. The increase in computer crime, coupled with the increasing dependence of the Nation's infrastructure upon computer technology brings forward a need to enhance law enforcement capabilities. Drawing upon a recurring theme of cooperation, Richard Poehling, Assistant United States Attorney says, "It is essential that we develop a period of intense cooperation between Government agencies, law enforcement community, and the potential victims of these crimes, whether they be private industry, educational institutions, government entities."[59] There is an apparent gap between law enforcement's knowledge and the expertise of the computer hackers

---

[57] NIITF Final Report to NSTAC XIX, *March 1997.*

[58] *Pethia, op. cit., p. 71.*

[59] *Poehling, op. cit., p. 7.*

attacking systems. The gap is exasperated by the number of hackers and the time and resource constraints of law enforcement. The gap has narrowed a bit with the creation of the FBI's National Computer Crime Squad and the Justice Department's Computer Telecommunications Coordination Program, which trains U.S. attorneys in computer and telecommunication issues.

Private industry can lend its expertise to law enforcement to assist in detecting potential infrastructure attacks. As U.S. Attorney Kent Alexander notes, "One reason why there have not been a lot of computer hacker prosecutions is that very few corporations report the attacks on their systems."[60] Clearly, a more trusting relationship needs to be forged between the private sector and law enforcement. While there are private sector concerns with regard to losing customer confidence if attacks are reported, hackers are taking advantage of these fears to break into systems without concern that the break-in will be reported.

3.8 Global Perspective

As the United States moves towards the 21st century, the nation is adjusting to the implications of the growing global economy. Although the United States leads in the development and use of information technology, the world is becoming more competitive. The transition of the NII toward the Global Information Infrastructure and the creation of multinational telecommunications corporations bring forward a need to expand U.S. perspective with regard to protecting the critical infrastructures. Although the changes wrought by these developments create a more dependable and robust worldwide telecommunications infrastructure, the changes create potential worldwide vulnerabilities. Hackers from foreign nations are just as able to crack into sensitive systems as hackers located in the United States. The challenge is to create an environment whereby international entities are included in addressing the vulnerabilities of the Global Information Infrastructure.

60 *Kent Alexander.* Transcript of hearing held by the President's Commission on Critical Infrastructure Protection, Atlanta, GA., April 18, 1997. *p. 11.*

4.0 NATIONAL COORDINATING MECHANISM

To address many factors involved in developing policy solutions, the PCCIP and many individuals within Government and industry have advocated the need for something resembling a National Coordinating Mechanism (NCM). An NCM and its organizational processes would provide senior Federal Government decision makers with real-time information from related components of critical national infrastructures to enhance NS/EP. The NCM would also provide a joint industry/Government infrastructure protection planning forum. The concept is driven primarily from the quickening realization that the nation's critical infrastructures are essential to the United States' economic and, therefore, national security. The need for an NCM is also shaped by the increased interdependency of infrastructures. For example, in 1996, the banking industry alone spent more than $4 billion on telecommunications services, placing the industry among the top consumers of communications systems.[61] In light of these factors, a coordinated approach to NS/EP planning for critical infrastructures should be investigated.

Several models exist upon which to base the NCM. The NSTAC is often put forth as an example or framework upon which to base the NCM. NSTAC was established by Presidential Executive Order 12382 in March 1982 in response to the anticipated deregulation of the telecommunications industry, divestiture of AT&T, and rapid changes in technology. In the early 1980s, the NSTAC first developed the idea for an industry/Government mechanism to coordinate planning, information sharing, and resources in response to NS/EP requirements.[62] Lessons from the NSTAC's experience are applicable to the NCM concept and provide an important historical context. Testimony before the Senate Permanent Subcommittee on Investigations that, "I think that the NSTAC is an example of various competitors getting together under a government aegis and that that has worked successfully. Perhaps that model might be replicated in other industries."[63]

As a result of NSTAC's effort and subsequent recommendation to the President, a joint industry/Government National Coordinating Center for Telecommunications (NCC) was created in 1984. The purpose of the NCC was to provide a single organization capable of responding to the Federal Government's NS/EP telecommunications service requirements. This approach provided continual access to a full range of industry representatives and to the operational arms of major U.S. telecommunications service providers to support national security leadership requirements and responsibilities in the event of an NS/EP emergency. Figure 1 is a notional representation of the NCC. In addition to the NCC construct, the NSTAC itself was envisioned to serve as a forum for coordinating industry-wide NS/EP telecommunications planning and activities.

---

61 *Tracey Tucker, "Telecommunications Spending Balloons as Banks Upgrade Systems and Services,* American Banker, October 16, 1996.

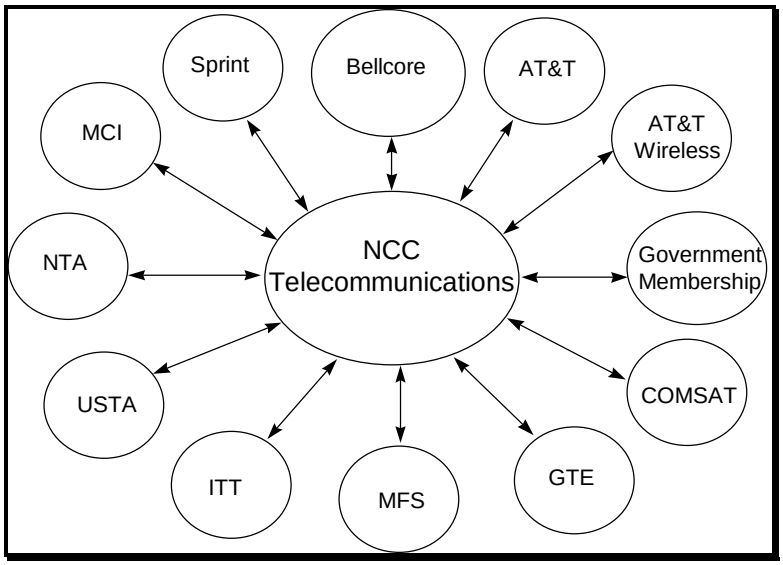
62 National Coordinating Mechanism Implementation Plan, January 30, 1984.

63 *Robert Anderson,* Testimony before the Senate Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, 104th Congress, June *25,* 1996, *p. 112.*

The primary need for such an overall NS/EP telecommunications national coordinating framework was twofold. First, the divestiture of AT&T disrupted an integrated, national telecommunications system and distributed control of the U.S. commercial telecommunications infrastructure. As a result, the Federal Government essentially lost a single point-of-contact for coordinating NS/EP telecommunications planning and response. Second, the Government realized that as part of the nation's deterrence strategy, the telecommunications infrastructure needed physical protection from the clear and predominant threat to the Nation, i.e., the Soviet Union's nuclear arsenal.

Although telecommunications divestiture and the Soviet threat were compelling causes for action in 1984, the current environment presents a new set of challenges. Specifically, the current business climate has created a much more diffuse and complex information-communications infrastructure. Technological advances and market deregulation have led to the evolution of an information infrastructure that is the critical in the day-to-day operations of many critical national infrastructures. In addition, pervasive interconnected networks and information systems have hastened infrastructure interdependence in general.

Figure 1. National Coordination Center for Telecommunications



A significant shift has also occurred in the strategic environment. Economic security concerns, including the maintenance of a strong socioeconomic base, have become a larger component of national security concerns. In such a context, a robust information infrastructure that connects other critical infrastructures is recognized as essential to the national interest. Consequently, the vulnerabilities inherent in the interrelationships of critical national infrastructures and the communications systems that underpin them could have a debilitating impact on the defense and economic vitality of the United States. Moreover, infrastructure protection is complicated by the fluidity and complexity of the threat environment. Military, intelligence, and law enforcement organizations have been frustrated in their efforts, both singularly and collectively, to provide an adequate defense or response to cyber-based national security threats.

In light of these developments, it is appropriate to investigate the utility and advisability of a cross-infrastructure NCM, and its potential organizational structure and functions, as a means to initiate discussion within the Federal Government and the private sector regarding a contemporary framework for infrastructure protection. The nature of infrastructure interdependency and its importance to the Nation's overall socioeconomic well being necessitate a national-level coordinating function that is broader in scope than telecommunications and includes all critical infrastructures. Nevertheless, the NSTAC-NCS partnership and its work in the NCC provide unique precedence for industry/Government planning and coordination with respect to one of the Nation's most critical infrastructures-telecommunications. As a result, important lessons can be drawn from the NSTAC-NCS experience. Moreover, because the telecommunications industry provides the backbone networks for many other critical infrastructures, the current role and functions of the NSTAC and NCS would need to be assessed in context of a proposed cross-infrastructure NCM.

4.1 Feasibility and Value

An NCM would require linking diverse sources of information within the private sector and the Government, including the intelligence and law enforcement communities. In addition, it would require developing new, trusted channels for information exchange and creating functional equivalents to the NCC within other critical infrastructures. The NSTAC's NCC Vision Subgroup along with the NCS NCC Implementation Team has begun to address these issues in the course of assessing the future mission, organization, and capabilities of the NCC.

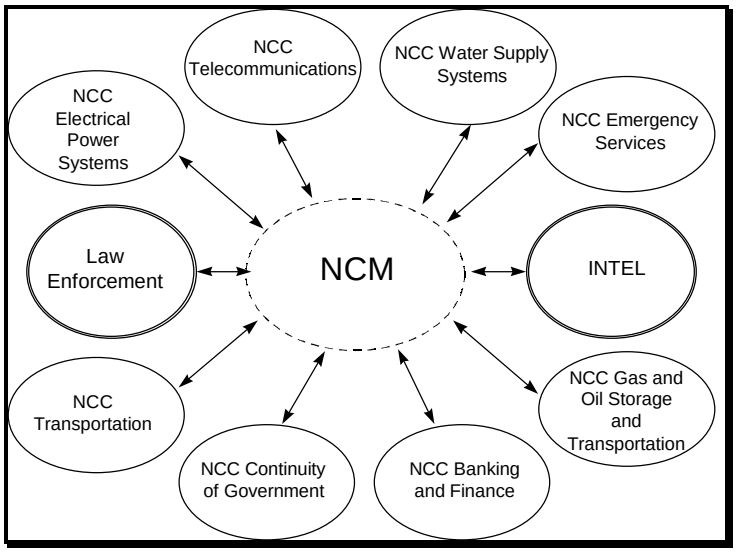
Operationally, the proposed NCM might best be envisioned as primarily an entity or process for sharing information among infrastructures and the Government. The success of the NCM would rest largely on the trusted relationships that would develop among all stakeholders. Information shared through the NCM would be used by the various stakeholders in accordance with their respective mission responsibilities. It is important to recognize that the feasibility of the NCM is dependent on the willingness of industry and Government to contribute meaningful information to the process. Participation in the NCM must be voluntary, and industry must never perceive itself to be subordinate to the Government. The NCM would be a cooperative partnership between industry and Government based on trusted relationships and the two-way flow of information.

Information channeled to and between stakeholders would be analyzed and available to appropriate decision makers in Government and industry. As shown in Figure 2, each infrastructure would have an NCC to address industry-specific issues. The NCM in turn would provide the means for coordinating infrastructure-wide consequence management to industry for infrastructure protection or restoration in the event of criminal, terrorist, or state-sponsored actions. In addition, an NCM would provide industry with a mechanism for identifying and addressing interdependency issues across infrastructures.

Both conceptually and operationally the NCM poses significant information management challenges. To effectively coordinate the flow of information, criteria for reporting information must be established and accepted by all participants. The identification of candidate participants

in an NCM must be based on the ability to affect NS/EP. In addition, an ongoing analysis of the providers of new and emerging technologies and services that could affect NS/EP would need to be conducted so that the NCM process and membership could be updated to ensure effective infrastructure protection planning and response. Lastly, the reporting and sharing of information raises important proprietary, antitrust, and security issues. The answers to questions regarding the handling and security of information are key enablers for industry participation in the NCM. Although, the private sector has significant concerns about Government and other private sector entities using reported information against individual companies, the success of the NSTAC has proven that acceptable solutions can be achieved.

Figure 2. National Coordinating Mechanism



4.2 Conclusion

A major point of this report has been that an extensive amount of work on critical infrastructure protection has been done in a relatively short amount of time by groups such as the CSSPAB, NSTISSC, and the PCCIP. In addition, numerous other groups, including the PCCIP Transition Team, will be concerned with further investigating infrastructure protection issues. The NCS and NSTAC process provides perhaps the best means to further investigate the NCM concept and coordinate the infrastructure protection activities outlined in this report. Since 1963, the NCS's interagency forum has effectively served as a focal point for industry-Government NS/EP telecommunications planning. Within this construct, the Government and the telecommunications industry have coordinated the appropriate policy and technical expertise to address the Nation's most critical telecommunications issues. Similarly, by expanding the scope of its outreach to address the changing national security environment the NSTAC and NCS are best positioned to coordinate individuals within the Government and industry that have the sufficient mission, policy, and management expertise across infrastructures to adequately address the Nation's critical infrastructure protection needs.

In short, while the NCM concept raises challenging implementation questions, it provides a framework for the Federal Government and the private sector to begin to discuss solutions to growing infrastructure protection concerns. Much work is needed to resolve the critical issues involved with the sometimes competing equities of the Government and private sector. Each community has its own interests, one driven by national security concerns and the other driven by business issues. However, the end goal¢ effective, secure, interoperable, and reliable operations¢ is mutual. This common interest in having and planning for functional networks in times of crisis is the foundation from which the NSTAC and other stakeholders can further investigate the issue of a national coordinating mechanism for critical infrastructure protection.

5.0 RECOMMENDATIONS

5.1 Recommendations for the President

- **Recommendations.** The President should direct appropriate departments and agencies to identify personnel within their respective department and agency that have the requisite policy, management, and mission expertise to work with the NCS and NSTAC in carrying out the following:

  - Continue to refine the NCM concept and postulate how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, R&D, standards, security investment, law enforcement capabilities, and the globalization of information systems.

  - Identify details of the NCM's initial formation and operation.

  - Explore the linkages within Government departments and agencies among infrastructures that will be essential to the NCM recommendation.

  - Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

5.2 Recommendations for the NSTAC

- **Recommendations.** The NSTAC should charge the Industry Executive Subcommittee to do the following:

  - Continue to refine the NCM concept and postulate how the NCM would address issues affecting the Nation's critical infrastructures such as industry/Government partnerships, coordinated NS/EP planning, education and awareness, R&D, standards, security investment, law enforcement capabilities, and the globalization of information systems.

- Identify details of the NCM's initial formation and operation.

- Explore the linkages with Government and between infrastructures that will be essential to the NCM recommendation.

- Ascertain support for the NCM concept through outreach to representative, appropriate industry, Government, academia, and other organizations, associations and institutions.

- Based on the outreach, develop a final recommendation as soon as possible, with interim status reports at intervening NSTAC meetings.