THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION INFRASTRUCTURE GROUP REPORT

December 1997

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In the spring of 1995, the President's National Telecommunications Advisory Committee's (NSTAC) Issues Group held a series of panel discussions to address concerns related to information warfare (IW) and information assurance (IA). As a result of these meetings, the Issues Group determined that it would be appropriate for NSTAC to address IA concerns regarding critical national infrastructures and recommended that the Information Assurance Task Force (IATF) be established to act as a focal point for NSTAC IA activities. Established on May 15, 1995, the IATF was charged to identify critical national infrastructures, determine their importance to the national interest, and, schedule several elements for assessment. The IATF defined three key infrastructures, electric power, financial services, and transportation. The IATF established three risk assessment subgroups to investigate the nature of each infrastructure, its dependence upon information technology and assess the IA risks to each infrastructure. Following NSTAC XIX, the Industry Executive Subcommittee (IES) restructured its organization to streamline its work to prevent a duplication of effort. As a part of this reorganization, the IATF and its charge were incorporated into the activities of the Information Infrastructure Group (IIG). A majority of the IIG's activities were completed by four subgroups.

Financial Services Risk Assessment Subgroup

The Financial Services Risk Assessment Subgroup conducted confidential interviews with institutions representing money center banks, securities credit firms, credit card associations, third-party processors, payment and industry utilities, industry associations and Federal regulatory agencies responsible for oversight of the industry. The subgroup found that security measures were treated as fundamental risk controls and that a system of independent, mutually-reinforcing checks and balances within critical systems and networks is unique to the financial services industry and provides a high level of integrity. The subgroup concluded that at the national level the industry is sufficiently protected and prepared to address a range of threats. However, there are security implications and potential vulnerabilities associated with the industry's dependence on a telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from mergers and acquisitions, and the introduction of web-based financial services.

The IIG made the following recommendations to the President and financial services industry.

Recommendations to the President:

- The President should assign to the appropriate department or agency the mission of identifying external threats and risk mitigation to the financial services infrastructure and facilitating the sharing of meaningful and timely information between the Government and industry.

- The President should assign the appropriate department or agency the task of working with the private sector to develop a mutually agreeable solution for effective background investigations for sensitive positions.
- The President, in consultation with the financial services industry, should assign the appropriate department or agency the task of monitoring the new/emerging areas of electronic money and commerce, including new payment services.
- The President should consider ensuring that the NSTAC continues to have at least one member from the financial services industry.

Recommendation to the Financial Services Industry:

- The financial services sector should consider identifying sensitive positions that require extensive screening and skill certification.

Transportation Risk Assessment Subgroup

In December 1996, the Transportation Risk Assessment Subgroup began its work analyzing the transportation infrastructure's dependency on information technology and the telecommunications industry. The subgroup met with transportation industry representatives and Government officials to collect data and to establish contacts within the industry and government. The subgroup also conducted a Transportation Information Risk Assessment Workshop on September 10, 1997, which provided a significant amount of information on the industry's use information technology and the security of major operations networks. The subgroup developed an interim report and made some preliminary conclusions; most notable was the need for improved or heightened awareness regarding the transportation industry's dependency on information technology and the telecommunications industry. The subgroup also realized that further discussions regarding intermodalism must involve a wider and more representative sample of transportation modes to complete the risk assessment. The subgroup will conduct additional events during the next NSTAC cycle to gain a more thorough understanding of the transportation industry.

Cyber Crime Subgroup

The IIG established the Cyber Crime Subgroup to examine the need for a cooperative approach between industry and Government. The subgroup discussed the need to establish an enhanced level of trust between industry and Government in detecting, investigating, and prosecuting cyber criminals. A point paper was developed to frame the issues to be discussed in proposed meetings between NSTAC principals and Attorney General Reno.

Information Assurance Policy Subgroup

The IA Policy Subgroup, working with the National Coordinating Mechanism (NCM) Subgroup of the NSTAC's Operations Support Group (OSG), developed a report that addresses a wide variety of information assurance policy issues and how those issues relate to the concept of

a NCM for coordinating the Nation's critical infrastructures. The report was based upon various NSTAC risk assessments and findings of various other groups, including the President's Commission on Critical Infrastructure Protection (PCCIP). The report identified pertinent issues regarding the interconnected nature of the Nation's critical infrastructures and how a coordinating mechanism could address these issues. The analysis of this report led the IIG and OSG to recommend that further research and outreach be conducted with regard to the NCM concept. The full report is part of the OSG Report to NSTAC XX.

Information Systems Security Board (ISSB)

During the NSTAC XIX Business Session, the NSTAC principals voted to recommend that the President should endorse the private sector ISSB initiative. The IES subsequently charged the IIG to track the progress of subsequent and related private sector activity. A result of the National Information Infrastructure Task Force's outreach efforts has been the development of a private sector entity-the Information Security Exploratory Committee (ISEC) to explore issues regarding the establishment of the ISSB. The Information Technology Industry Council, a private, nonprofit association, is serving as the host organization for the ISEC. Comprising predominantly non-NSTAC private sector interests, the ISEC has met regularly since December 1996, and has developed a draft final report. The report will be finalized by the end of 1997.

1.0 BACKGROUND AND APPROACH

On January 16, 1995, Vice Admiral Mike McConnell, Director of the National Security Agency (NSA), briefed the 17th meeting of the NSTAC on threats to U.S. information systems and the need to improve the security of the Nation's critical infrastructures. The NSTAC principals discussed those issues and drafted a letter to the President in March of that year 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 control, power, etc., also depend on reliable and secure information systems and could be at risk."[1] In July 1995, President Clinton replied to the NSTAC letter, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications systems."[2] The President further asked "the NSTAC's principals-with input from the full range of NII users-to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information infrastructure."[3]

In the spring of 1995, the NSTAC's Issues Group held a series of panel discussions to address concerns related to IW and IA. Representatives from the U.S. Government and the private sector were invited to those meetings to contribute their perspectives. The Issues Group determined that it would be appropriate for NSTAC to address IA considerations for critical national infrastructures and recommended that a new task force be established to serve as the focal point for NSTAC information assurance activities. On May 15, 1995, the NSTAC's IES established the IATF.

The IATF was charged to cooperate with the U.S. Government in identifying critical national infrastructures, determining their importance to the national interest, and scheduling several elements for assessment. Working with representatives from the national security community, law enforcement, civil departments and agencies, and the private sector, the task force narrowed an initial list of critical infrastructures to three for study-electric power, financial services, and transportation. These three infrastructures were selected based on the strong interdependencies depicted in Figure 1. Furthermore, the task force members agreed that each of those infrastructures was growing more dependent on telecommunications and information systems to perform their key business functions.

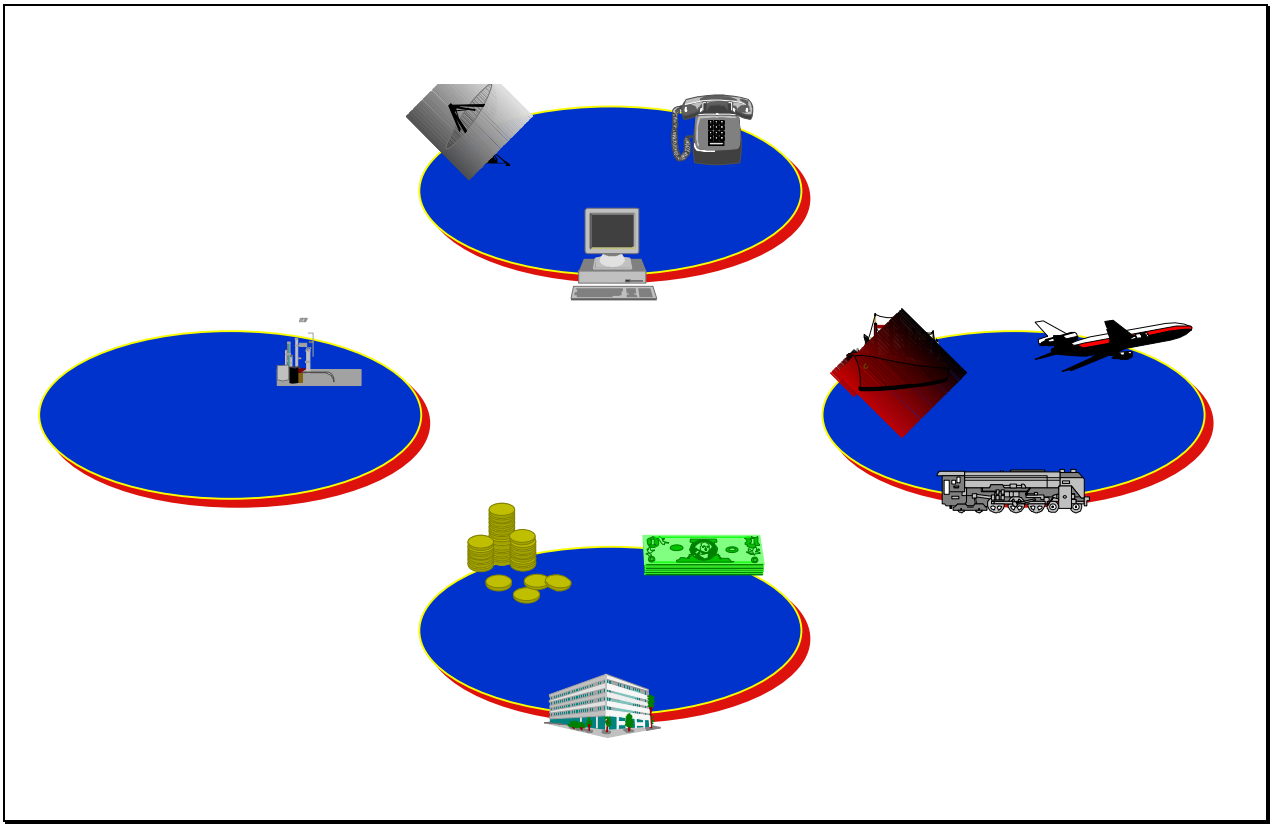
---

1 Letter from Mr. William T. Esrey, Sprint Corporation and Chair of the President's NSTAC, to President of the United States, dated March 20, 1995.

2 *Letter from the President of the United States to the Chair of NSTAC,* dated *July 7, 1995.*

3 Ibid.

Figure 1. Interdependencies of Critical Infrastructures

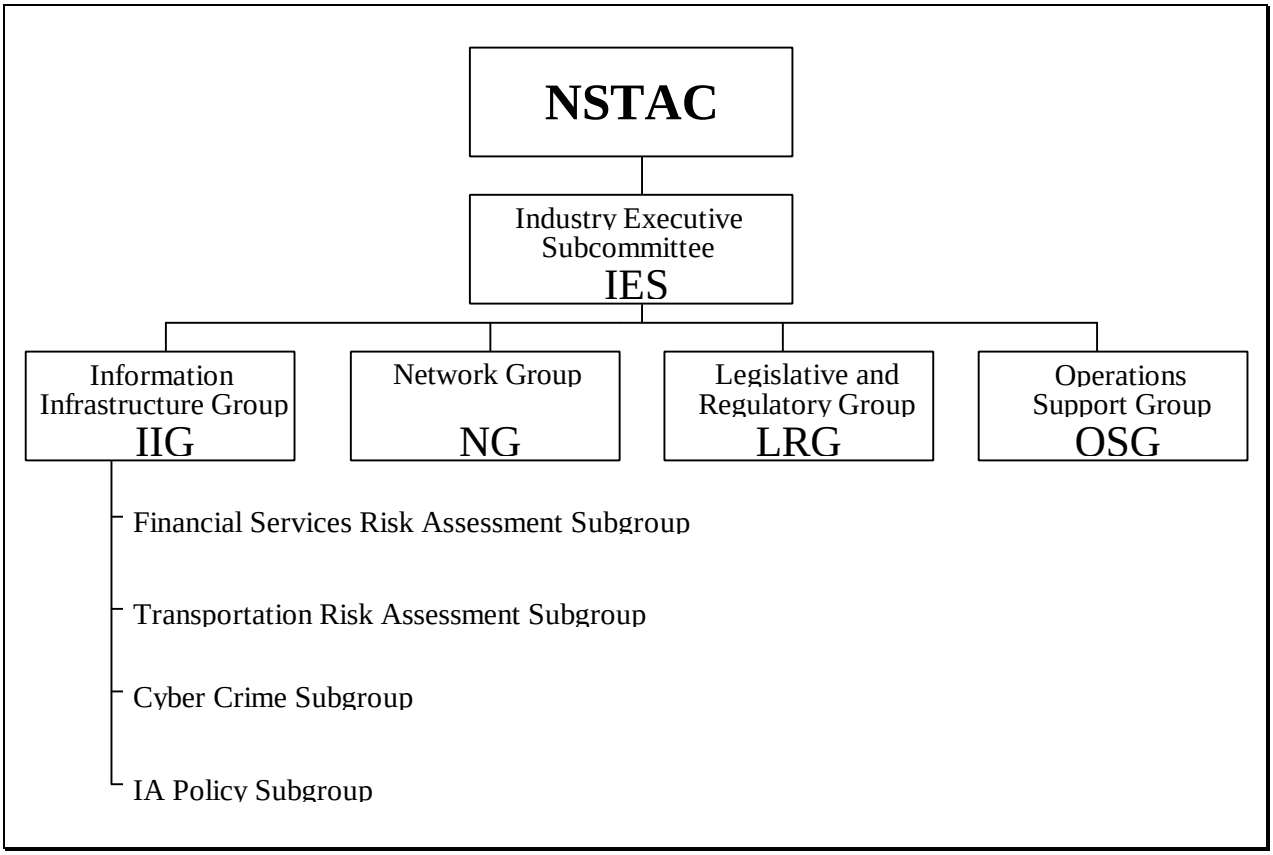


The task force developed a generic risk assessment methodology to be applied to each infrastructure and subsequently formed three risk assessment subgroups to address the distinct characteristics and concerns of each infrastructure. A time-phased schedule for completing the risk assessments was developed to maximize the use of resources by the NSTAC and the Office of the Manager, National Communications System. The first risk assessment was completed by the Electric Power Risk Assessment Subgroup in September 1996, and its report and recommendations were approved by the principals prior to NSTAC XIX.

In their endeavors, the task force and its subgroups have worked closely with the Government, industry, and professional associations in scoping their activities, identifying organizations for interview, and conducting interviews. In examining information assurance risks to each infrastructure, the task force and subgroups worked diligently to avoid duplicating the efforts of other organizations conducting similar analyses. In particular, they coordinated with the PCCIP and the Infrastructure Protection Task Force (IPTF).

Following NSTAC XIX, the IES restructured its organization to streamline its processes and prevent duplicative effort. To that end, the IATF and its charge were incorporated into the activities of the IIG. Figure 2 depicts this new organizational structure and the subgroups of the IIG.

Figure 2. NSTAC Organization and IIG Subgroups



2.0 IIG CHARGE AND APPROACH

The IES charged the IIG to serve as the focal point for NSTAC IA activities:

- Conduct IA risk assessments
- Consider the implications of IA risks for overall infrastructure protection
- Investigate a cooperative industry-Government approach to enhance cyber security and crime
- Provide advice and assistance to the electric power industry in establishing an NSTAC-like organization
- Track the progress of the ISSB initiative
- Propose policy recommendations to the NSTAC for presentation to the President.

The majority of these activities were completed by four IIG subgroups:

- Financial Services Risk Assessment Subgroup
- Transportation Risk Assessment Subgroup
- Cyber Crime Subgroup
- IA Policy Subgroup.

While the subgroups undertook work, the IIG approved reports and developed recommendations by the subgroups. Subgroup activities are described in the following section. It should also be noted that the IIG monitored the progression of the recommendations from the Electric Power Risk Assessment report. The National Information Infrastructure Task Force (NIITF) progression was also monitored by the IIG with respect to the ISSB. The current status of the ISSB recommendations is summarized in Section 3.5.

3.0 IIG FINDINGS AND RECOMMENDATIONS

3.1 Financial Services Risk Assessment Subgroup

3.1.1 Actions

From December 1996 to April 1997, the subgroup conducted more than 25 confidential interviews with institutions representing money center banks, securities firms, credit card associations, third-party processors, and payment and industry utilities. To augment interview data, the subgroup also met with industry associations and Federal regulatory agencies responsible for oversight and supervision of the industry. The subgroup identified three primary objectives for its effort:

- Assess the security and robustness of the financial services infrastructure at a national level relative to the identified threats to its networks and information systems

- Determine the risks to the financial services industry that derive from its dependence on information technology and the telecommunications infrastructure

- Examine the implications of trends regarding the industry's use of information technology and networks.

3.1.2 Findings

The subgroup concluded that at the national level the financial services industry is sufficiently protected and prepared to address a broad range of current threats, from natural disasters to electronic intrusions. However, there are security implications and potential vulnerabilities associated with the industry's dependence on a telecommunications infrastructure being subjected to deregulation, the integration of dissimilar information systems and networks resulting from mergers and acquisitions, and the introduction of web-based financial services.

These conclusions were based primarily on the data gathered from the extensive interview process. During each interview, the subgroup reviewed the policy, personnel, information systems, telecommunications, and disaster recovery risk controls in place at the institution. In general, the subgroup observed that security was considered and integral element of an overall program of risk management accountable to the most senior levels of an institution. The industry has a long-established practice of risk management, which factored into every investment decision. Security measures were treated as fundamental risk controls. And the extent of independent, mutually-reinforcing checks and balances in place within most critical systems and networks is unique to the financial services industry and provides an exceptional level of integrity and resilience. The Financial Services Risk Assessment Report is attached as Annex B.

- **Recommendations to the President:**

  - The President should assign to the appropriate department or agency the mission of identifying external threats and risk mitigation to the financial services infrastructure and facilitating the sharing of meaningful and timely information between the Government and industry.
  - The President should assign the appropriate department or agency the task of working with the private sector to develop a mutually agreeable solution for effective background investigations for sensitive positions.
  - The President, in consultation with the financial services industry, should assign the appropriate department or agency the task of monitoring the new/emerging areas of electronic money and commerce, including new payment services.
  - The President should consider ensuring that the NSTAC continues to have at least one member from the financial services industry.

- **Recommendations to the Financial Services Industry:**

  - The financial services sector should consider identifying sensitive positions that require extensive screening and skill certification.

3.2 Transportation Risk Assessment Subgroup

3.2.1 Actions

Since December 1996, the Transportation Risk Assessment Subgroup has analyzed the dependencies of the transportation infrastructure on telecommunications and information systems. To discern those transportation modes that may be exposed to increased risk through these dependencies, the subgroup met with representatives from the transportation industry, the Department of Transportation (DOT), and the PCCIP. The scope and complexity of the transportation infrastructure necessitated a step by step approach to accurately assess risks. The first step was to conduct a Transportation Information Risk Assessment Workshop at the U.S. Army Reserve Command Headquarters, Ft. McPherson, Atlanta, Georgia, on September 10, 1997. The workshop included briefings from representatives of NSTAC, DOT, and the Federal

Bureau of Investigation, which stimulated participant discussion using a transportation infrastructure threat scenario prepared by the subgroup.

3.2.2 Findings

The subgroup research efforts and workshop discussions revealed that other infrastructures, most notably power and telecommunications, are instrumental to the transportation infrastructure in carrying out both normal and emergency operations. Subgroup outreach also identified a general need for improved awareness in the transportation industry of infrastructure interdependencies, cyber threats, and the overall implications of these issues on information systems security. At the workshop, industry representatives expressed an interest in gaining greater access to threat information. The subgroup identified a need for further discussion with industry representatives from transportation modes that were underrepresented at the workshop. It was also noted that these discussions should include industry associations and attempt to focus on a more thorough examination of intermodal transportation issues. The subgroup will conduct future events during the next NSTAC cycle to gain a more thorough transportation industry perspective for the completion of the risk assessment. The Interim Transportation Information Risk Assessment report is attached as Annex C.

- **Recommendation to the IIG:**

  - A second transportation infrastructure workshop should be held to facilitate information exchange, further investigate intermodal transportation and transportation infrastructure dependency issues, and finish the data collection effort to complete the subgroup's task
  - The workshop should involve national transportation industry representatives, including relevant industry associations.

3.3 Cyber Crime Subgroup

3.3.1 Actions

At the NSTAC XIX Executive Session, Attorney General Janet Reno expressed concerns about cyber security and crime issues and stated that Government could not solve the associated problems without forging a stronger partnership between industry and Government. In response, the IIG established the Cyber Crime Subgroup to examine the need for a cooperative approach between industry and Government. The subgroup discussed the need to establish an enhanced level of trust between industry and Government in detecting, investigating, and prosecuting cyber criminals. A point paper was developed to frame the issues to be discussed in proposed meetings between NSTAC principals and Attorney General Reno. In addition, that point paper was intended to serve as a guideline for discussion at the NSTAC XX Executive Session. The point paper is attached as Annex D.

3.4 Information Assurance Policy Subgroup

3.4.1 Actions

In the spring of 1997, the IIG established the IA Policy Subgroup to examine the findings of the NSTAC risk assessments, lessons learned from other NSTAC outreach activities, the findings and recommendations of the PCCIP, and several other information assurance and infrastructure protection reports to identify common sets of issues, findings, and recommendations. The subgroup worked closely with the NCM Subgroup of the NSTAC's Operations Support Group to develop a report that examined IA policy issues and related them to the concept of an NCM for coordinating responses among the Nation's critical infrastructures.

3.4.2 Findings

Extensive work on critical infrastructure protection has been done in a short period of time. The level of effort undertaken by government policy-makers, law enforcement officials, the defense and intelligence communities, academia, and the private sector reflects the important role that the Nation's critical infrastructures play in national security. The subgroup report outlined the major milestones in critical infrastructure protection awareness and identified the pertinent issues surrounding a possible mechanism or process to coordinate industry/Government information sharing between critical infrastructures and the Federal Government.

The most important issues identified by the report included a need for more industry/Government partnerships, coordinated national security/emergency preparedness (NS/EP) planning, enhanced education and awareness, more attention to R&D, standards, security investment, augmented law enforcement capabilities, and the realization of the global nature of information systems. The analysis of these issues led the IIG and OSG to recommend that further research be conducted with regard to the NCM concept. An NCM is best envisioned as a cooperative partnership that would create a process or entity whereby government and industry could confidently share regarding threats to the Nation's critical infrastructures as well as sensitive industry information. The full Joint Report of the IA Policy subgroup and the NCM Subgroup is attached in the OSG report.

3.5 Information Systems Security Board (ISSB)

3.5.1 Actions

During the NSTAC XIX Business Session, the NSTAC principals voted to recommend that the President should endorse the private sector ISSB initiative. The IES subsequently charged the IIG to track the progress of subsequent and related private sector activity. A result of the National Information Infrastructure Task Force's outreach efforts has been the development of a private sector entity "the ISEC" to explore issues regarding the establishment of the ISSB. The Information Technology Industry Council, a private, nonprofit association, is serving as the host organization for the ISEC. Comprising predominantly non-NSTAC private sector interests, the ISEC has met regularly since December 1996, and has developed a draft final report. The report will be finalized by the end of 1997.

ANNEX A

Information Infrastructure Group Members

Information Infrastructure Group Members

CSC	Mr. Guy Copeland, Chair
Unisys	Dr. Dan Wiener, Vice Chair
AT&T	Mr. Larry Nelson
Boeing	Mr. Bob Steele
Bellcore	Mr. Carl Ripa
COMSAT	Mr. Ernie Wallace
CTC	Mr. John Grimes
EDS	Mr. Bob Donahue
GTE	Mr. Lowell Thomas
MCI	Mr. Micheal McPadden
NORTEL	Dr. Jack Edwards
SAIC	Mr. Bernie Ziegler
Sprint	Dr. Sushil Munshi
U S West	Mr. Jon Lofstedt