THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION INFRASTRUCTURE GROUP REPORT

SEPTEMBER 1998

INFORMATION INFRASTRUCTURE GROUP REPORT
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the last meeting of the President's National Security Telecommunications Advisory Committee (NSTAC), December 1997, the Information Infrastructure Group (IIG) has concentrated its efforts on issues related to information assurance, infrastructure protection, electronic commerce, and cyber security. The IIG established two subgroups to investigate these topics, the Transportation Information Infrastructure Risk Assessment Subgroup and the Electronic Commerce (EC)/Cyber Security Subgroup.

The Transportation Information Infrastructure Risk Assessment Subgroup conducted a workshop for the transportation industry on telecommunications and information systems dependencies on September 10, 1997. On the basis of findings from that event, the subgroup submitted an interim report to the December 1997 NSTAC XX meeting. The report recommended that more information be gathered, particularly in the area of intermodal transportation, and concluded that broader participation from the transportation industry was desirable. The subgroup anticipates completing the risk assessment in the beginning of the NSTAC XXII cycle.

The EC/Cyber Security Subgroup was established in response to a briefing the Deputy Secretary of Defense gave at the December 1997 NSTAC XX meeting. The subgroup agreed to examine national security and emergency preparedness (NS/EP) implications of EC because both industry and Government incorporate EC into their business practices. After meeting with key officials in industry and Government on security issues related to EC, the subgroup developed an issue paper that focused on one aspect of EC—cyber security training and forensics. That paper centers on the importance of industry and Government cooperation in addressing cyber security. The subgroup is also developing further analyses of EC to be completed in preparation for the NSTAC XXII meeting.

The following recommendations result from deliberations and assessments of the group on cyber security issues.

Recommendation to the President

The President should direct the appropriate departments and agencies to continue working with the NSTAC for the development of policies, procedures, techniques, and tools to facilitate joint industry–Government cooperation on cyber security.

Recommendation to the NSTAC

The NSTAC should continue to work with the presidentially directed departments and agencies in the development of policies, procedures, techniques, and tools to facilitate joint industry-Government cooperation on cyber security.

1.0 INTRODUCTION

The President's National Security Telecommunications Advisory Committee (NSTAC) has directly addressed information assurance and information infrastructure protection issues since 1995. At the January 16, 1995, NSTAC XVII meeting, the Director of the National Security Agency discussed with the NSTAC principals threats to U.S. information systems and the need to improve the security of the Nation's critical infrastructures. The NSTAC chair 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] 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]

On May 15, 1995, the NSTAC's Industry Executive Subcommittee (IES) established the Information Assurance Task Force (IATF) 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 on the basis of their strong interdependencies and their growing reliance on telecommunications and information systems for performing key functions.

The IATF developed a risk assessment methodology and subsequently formed three risk assessment subgroups to address the distinct characteristics and concerns of each infrastructure. The first assessment was completed by the Electric Power Risk Assessment Subgroup in September 1996, and its report and recommendations were approved by the principals before NSTAC XIX. The Financial Services Risk Assessment Subgroup completed its risk assessment in 1997, and the NSTAC approved its report and recommendations in advance of NSTAC XX. The Transportation Information Infrastructure Risk Assessment Subgroup conducted a risk assessment workshop in September 1997 and delivered its findings in an interim report to NSTAC XX.

Following NSTAC XIX, the IES restructured its organization, and the IATF's activities were incorporated into the newly formed Information Infrastructure Group (IIG). The IIG's charge was also broadened to include, among other things, a consideration of cyber security and crime issues. That set of issues gained focus at NSTAC XIX, where the U.S. Attorney General

[1] Letter from Mr. William T. Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States, March 20, 1995.
[2] Letter from the President of the United States to the Chair of NSTAC, July 7, 1995.
[3] Ibid.

initiated a dialogue with the NSTAC principals on the need to develop a more cooperative industry-Government approach to cyber crime. The IIG's current charge is outlined below.

2.0 CHARGE

The IES charged the IIG to serve as a focal point for NSTAC information assurance and infrastructure protection activities along multiple dimensions:

- continue to assess the implications of transportation information assurance risks;
- examine inter-infrastructure protection and coordination issues among the telecommunications, transportation, electric power, and financial services industries;
- consider the national security and emergency preparedness (NS/EP) implications associated with electronic commerce;
- monitor any Information Systems Security Board (ISSB) related activity; and
- stand ready to assist the electrical power industry in forming an NSTAC-like body.

The major IIG activities were completed by two IIG subgroups the Transportation Information Infrastructure Risk Assessment Subgroup and the Electronic Commerce (EC)/Cyber Security Subgroup.

3.0 ACTIVITIES

At NSTAC XIX, the principals recommended that the President endorse a private sector ISSB initiative. Subsequently, the IES charged the IIG to monitor any ISSB-related activities. On the basis of previous outreach efforts by the NSTAC's National Information Infrastructure Task Force, a private sector group called the Information Security Exploratory Committee (ISEC) further investigated issues regarding the establishment of the ISSB. (The Information Technology Industry Council, a private nonprofit association, serves as the host organization for the ISEC.) Since December 1996, the ISEC has met regularly, and it issued a final report in December 1997. The IIG believed that the NSTAC was misrepresented in the final ISEC report and on two occasions notified the ISEC of the misrepresentation. The IIG plans to continue to work with the ISEC to clarify the issue.

In addition, the IIG monitored the progression of the recommendations from the Electric Power Risk Assessment Report and the Financial Services Risk Assessment Report. The IIG's focus on issues regarding the transportation infrastructure and the NS/EP implications associated with electronic commerce are discussed below.

3.1 Transportation Risk Assessment

On September 10, 1997, the Transportation Information Infrastructure Risk Assessment Subgroup conducted a Transportation Risk Assessment Workshop to gather data about the industry's dependency on information technology and telecommunications. The findings of this workshop were included in an interim report presented during NSTAC XX. The subgroup

recommended that further discussions with the industry be conducted to gain information from a wider sample of transportation modes, and that future efforts capture data relating to intermodal transportation trends. The subgroup has contacted the Department of Transportation as a result of Presidential Decision Directive 63 (PDD-63), to jointly ensure the success and relevance of the risk assessment. The Transportation Information Infrastructure Risk Assessment Subgroup has developed a strategy to encourage involvement by key associations to ensure strong participation by all transportation modes so this task can be completed during the next NSTAC cycle.

3.2 Electronic Commerce/Cyber Security

3.2.1 Analysis

On December 11, 1997, the Honorable John Hamre, Deputy Secretary of Defense, briefed the 20th meeting of the NSTAC on steps that the Department of Defense (DOD) is taking to prepare for potential cyber attacks against the Nation. In his remarks, Dr. Hamre expressed the intent of the DOD to move forward with a paperless operation, utilizing EC technologies, and state-of-the-art security tools and strategies while expecting organizations that work with the DOD to adhere to the same level of protection. The IIG established the EC/Cyber Security Subgroup to examine any NS/EP implications associated with the movement to EC as the DOD, other Federal agencies, financial institutions, and a growing number of corporations incorporate EC into their business practices. Toward that end, the subgroup has scoped the issue and has received briefings from key officials in Government and industry on security issues related to EC. The subgroup will develop an issue analysis of the NS/EP implications of EC, which will be presented at NSTAC XXII.

In the course of scoping the EC issue, the subgroup determined that cyber crime concerns might be a long-term impediment to widespread use of emerging EC technologies. The subgroup also acknowledged that those concerns were related to issues raised by the NSTAC and the U.S. Attorney General at NSTAC XIX, where a dialogue was initiated on the need to develop a more cooperative industry-Government approach to cyber security. The subgroup agreed that there were emerging and timely issues related to the investigative community's ability to address evolving cyber security concerns. Officials from the National Infrastructure Protection Center, the Federal Bureau of Investigation Computer Analysis and Response Team, and the Department of Justice Computer Crime and Intellectual Property Section met with members of the subgroup to assist them in determining what timely NS/EP recommendations the IIG can make regarding cyber crime investigation. On the basis of findings from those discussions and previous IIG scoping of the cyber security problem, the subgroup produced an issue paper that presents findings and recommendations on cyber security. The issue paper is attached as Annex B.

3.2.2 Conclusions

In its investigation of cyber security issues, the EC/Cyber Security Subgroup concluded that a stronger partnership between industry and Government is required for the following reasons:

- The NS/EP implications of cyber security necessitate developing a partnership with industry, law enforcement, national security communities, and PDD-63 lead departments and agencies.

- The size and complexity of the cyber crime caseload, coupled with the growing sophistication and proliferation of computer-based tools used to attack information systems, challenge traditional policies, procedures, and protocols for investigating crimes and collecting evidence.

- Cyber investigators also face the challenge of staying abreast of industry's continuous introduction of new and innovative technologies.

- These new technologies introduce additional vulnerabilities that are being exploited by intruders.

- Industry possesses knowledge, tools, and expertise that investigators could leverage as they respond to increasingly complex and sophisticated cyber crimes.

A key element in this partnership will be establishing the appropriate levels of trust and understanding to spur cooperation in addressing cyber security issues. This partnership will also need to foster a dialogue that allows representatives from industry and investigative communities to develop a unique understanding of the perspectives and issues faced by their counterparts. The Government and NSTAC Network Security Information Exchanges and the National Coordinating Center for Telecommunications are examples of effective partnerships between the telecommunications industry and Government. The principles of cooperation exercised in these forums could be applied in efforts to address cyber crime.

With its years of experience working with the Government on NS/EP telecommunications, network security, and information assurance issues, NSTAC is positioned to build on this experience in developing a partnership with the law enforcement and national security communities to address cyber security issues.

3.2.3 Recommendations

Based on the findings of the EC/Cyber Security Subgroup, the IIG proposes the following recommendations.

3.2.3.1 Recommendation to the President

The President should direct the appropriate departments and agencies to continue working with the NSTAC for the development of policies, procedures, techniques, and tools to facilitate joint industry□Government cooperation on cyber security.

3.2.3.2 Recommendation to the NSTAC

The NSTAC should continue to work with the presidentially directed departments and agencies in the development of policies, procedures, techniques, and tools to facilitate joint industry-Government cooperation on cyber security.

ANNEX A

INFORMATION INFRASTRUCTURE GROUP MEMBERS

INFORMATION INFRASTRUCTURE GROUP MEMBERS

CSC	Mr. Guy Copeland, Chair
Unisys	Dr. Dan Wiener, Vice-Chair
AT&T	Dr. Larry Nelson
Boeing	Mr. Bob Steele
COMSAT	Mr. Ernie Wallace
EDS	Mr. Bob Donahue
GTE	Mr. Lowell Thomas
MCI	Mr. Michael McPadden
Nortel	Dr. Jack Edwards
Raytheon	Mr. John Grimes
SAIC	Mr. Bernie Ziegler
Sprint	Dr. Sushil Munshi
U S WEST	Mr. Jon Lofstedt

ACTIVE PARTICIPANTS

CSC	Mr. Richard Swanson
CSC	Ms. Deborah Jacobs
EDS	Mr. Richard Parodi
GTE	Ms. Ernie Gormsen
ITT	Mr. Joe Gancie
Lockheed Martin	Ms. Dena Kisala
NTA	Mr. Bob Burns
Raytheon	Mr. Bob Tolhurst
SAIC	Mr. Bill Deaver
SAIC	Ms. Rosemary Dew
TRW	Mr. Bob Lentz
Unisys	Mr. Fred Tompkins
DOT	LCDR Tim Custer
NASA	Mr. Art Sigust
NTIA	Mr. Bill Belote
SAIC	Mr. Hank Kluepfel

ANNEX B

CYBER SECURITY TRAINING AND FORENSICS ISSUE PAPER

THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

INFORMATION INFRASTRUCTURE GROUP

Cyber Security Training and Forensics Issue Paper

SEPTEMBER 1998

1.0 INTRODUCTION

Since 1990, the President's National Security Telecommunications Advisory Committee (NSTAC) has addressed network security issues affecting the U.S. telecommunications infrastructure. Those issues include vulnerabilities introduced into telecommunications networks by new technologies, the growing number of cyber intrusions as networks become more pervasive and open, and the changing threat environment characterized by linkages between national and economic security. National security and emergency preparedness (NS/EP) telecommunications rely heavily on information systems for transmission and network control. Historically, these information systems have been high-value targets for intrusions. Cyber security—the act of protecting sensitive computers and networked systems from misuse, exploitation, and intrusion—involves initiating a number of policies and tools to protect the Nation's security interests from a growing cyber threat.

At the 19th meeting of the President's NSTAC, Attorney General Janet Reno initiated a dialogue with the NSTAC principals on the need to develop a more cooperative industry–Government approach to cyber security. Because of the Nation's increasing dependence on the information systems that support the telecommunications and other critical infrastructures, the NSTAC views cyber security as an important NS/EP telecommunications issue. Subsequent discussions between industry and Government officials focused on issues of mutual concern. Based on these discussions, the following objectives were identified:

- an investigative community composed of intelligence and criminal investigators and prosecutors at the Federal, State, and local level who are sufficiently trained and resourced to respond to the cyber threats of the 21st century,

- an industry that is aware of the potential vulnerabilities in a networked society and is actively taking steps to address cyber security, and

- a partnership that incorporates a mutually beneficial dialogue between industry and the investigative community.

The NSTAC recognizes that industry and the investigative community need a cooperative dialogue in order to ensure that the investigative community has ready access to better tools, techniques, capabilities, and training. This is particularly important as society transitions to an information-based economy. Specifically, the NSTAC's Electronic Commerce/Cyber Security Subgroup determined that cyber crime concerns might be a long-term impediment to widespread adoption and use of emerging electronic commerce technologies.

2.0 THE CHANGING ENVIRONMENT

2.1 National and Economic Security

Proliferation and sophistication of information technologies, coupled with the growing use of the Internet, have dramatically transformed how our society communicates and conducts business. The use of the Internet is rapidly growing. The number of Americans using the Internet has

grown from less than 5 million in 1993 to nearly 62 million in 1997.[1] UUNET estimates that Internet traffic doubles every 100 days.[2] Corporations are looking toward the Internet as a tool for commerce. Many Government agencies, including the Department of Defense (DOD), are beginning to use electronic commerce technologies to streamline business practices. The growth of electronic commerce, the deregulation of the telecommunications industry, and the interconnection of the Public Switched Network (PSN) and the Internet have blurred traditional barriers and opened the door to an "Information Age." This has tremendous security implications for the Nation, as President Clinton stated, "As borders open and the flow of information, technology, money, trade and people across borders increases, the line between domestic and foreign policy continues to blur." [3]

The risks associated with cyber intrusions into critical systems have risen over the past decade. Networked systems supporting our national security community and our national economy have become increasingly reliant on cyber-based information systems. Vital control systems that support the information infrastructure and other critical infrastructures depend upon network connectivity through the use of the PSN.

These factors introduce vulnerabilities that can be exploited by a wide spectrum of perpetrators: disgruntled insiders, recreational and institutional hackers, organized crime, terrorist groups, or hostile nations. The inability to determine the intentions of an intruder attacking or exploiting a networked system makes addressing this threat more difficult. As a result, "by their nature, developments in cyberspace blur the distinction between crime and warfare, thereby 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."[4] In February 1998, the DOD faced widespread intrusions into its networks in a case that became known as Solar Sunrise. The case highlights the complicated nature of cyber intrusions, especially with the challenge of determining whether an intrusion is a national security or law enforcement issue. The intrusion occurred as the United States was facing heightened hostilities with Iraq. However, the perpetrators turned out to be two juveniles in California and a juvenile in Israel. Investigators from the Federal Bureau of Investigation (FBI) and DOD were called on to work together to investigate the intrusion.

2.2 The Cyber Security Challenge

Computers can be used by criminals and other nefarious actors in the cyber arena in two broad areas the computer may be used as a tool to commit the offense (e.g., an intrusion into a network system), or it may be incidental to the crime but act as a repository of evidence (e.g., drug traffickers using encrypted computer information to hide evidence). In some cases, the computer may serve both functions. For example, hackers use their computers as tools to intrude into the networked systems of others as well as to store tools and information that could be used as evidence against them (e.g., hacker software, stolen files, and log information).

[1] *Morgan Stanley U.S. Investment Research: Internet Retail.* Morgan Stanley, May 1997.
[2] Inktomi Corporation White Paper. 1997.
[3] President William J. Clinton, "A National Security Strategy for a New Century," May 1997.
[4] 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.

In fact, hacker intrusion cases represent a troubling percentage of the total cyber crime caseload. In 1997, the FBI investigated 408 cyber intrusion incidents, a 133 percent increase from 1996. In 1996, the Defense Information Systems Agency (DISA) estimated that nearly 250,000 attacks on DOD systems may have taken place in 1995.[5] In cases where the computer contained evidence of a crime rather than being the tool used to commit the crime, the FBI Computer Analysis and Response Team (CART) conducted forensic examinations in almost 2,200 cases. The FBI reports that nearly 70 percent of those cases were instances of white-collar crime; the remaining cases involved organized crime, violent crime, terrorism, and cyber crime investigative programs.

Complicating matters, cyber security initiatives face several constraints. The cyber crime casework has grown exponentially in size and complexity. The Computer Emergency Response Team (CERT) at Carnegie Mellon University's Software Engineering Institute warned that intruders are using sophisticated techniques for analyzing source code vulnerabilities, have compromised a variety of operating systems, and are using complex denial of service attacks.[6] The General Accounting Office (GAO) noted the threat posed by cyber intrusion is rapidly increasing, and protection mechanisms have failed to keep pace with the threat.[7] Investigators require ready access to the full range of special tools and resources needed to keep pace with the increasing technical sophistication of cyber criminals. Investigative agencies are also faced with the difficult task of training their staff to investigate crime in nontraditional environments. Within these constraints, management must also balance the immediate need to investigate cases against long-term efforts to train employees. These managers, already faced with tight resources and a shortage of investigators to handle a growing caseload, may not be able to spare a key investigator for a prolonged period of time for cyber investigative training.

3.0 FEDERAL INITIATIVES

The Federal Government has recognized the cyber threats to critical networked systems and the potential national security implications. On May 22, 1998, President Clinton announced the signing of Presidential Decision Directive (PDD) 63, which expressed his intent to develop a national system to protect critical infrastructures from these types of attacks.

Federal, State, and local law enforcement agencies have initiated a number of programs to address the investigation and prosecution requirements of this threat. On February 26, 1998, the National Infrastructure Protection Center (NIPC) was established to create an interagency and public-private partnership to combat physical and cyber threats. The NIPC will provide centralized support, planning, and response capability to deal with domestic cyber crime and potential attacks on infrastructures. To provide a unified, comprehensive response to the cyber crime threat, the NIPC will be staffed with cyber investigators from the FBI and other representatives from the Department of Defense, the intelligence community, other Federal

[5] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO-AIMD-96-84, Washington, DC: USGPO, May 1996.
[6] CERT Coordination Center, "Increasing Sophistication of Intruder Community Expertise," CERT Summary CS-96.04, World Wide Web, info.cert.org/pub/cert_summaries/,July 23, 1996.
[7] United States General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO-AIMD-96-84, Washington, DC: USGPO, May 1996.

departments, state and local law enforcement, and private industry.

The Department of Justice Computer Crime and Intellectual Property Section (CCIPS) represents another strong Federal initiative on cyber crime. The CCIPS attorneys work with other Government officials and industry to develop a global response to cyber attacks. They litigate cyber crime cases, provide litigation support to other prosecutors, and train Federal law enforcement personnel. Other notable initiatives to address cyber crime include efforts within the Department of Treasury and NASA, as well as statewide cyber crime efforts in Florida and New York.

The national security community has undertaken a number of programs to secure its systems from the cyber threat. As the Manager of the Defense Information Infrastructure (DII), the Defense Information Systems Agency (DISA) initiated critical programs to protect against, detect and react to threats to both its information infrastructure and information sources. The DISA has undertaken a number of initiatives to transform the way DOD users move, share, and use information on critical systems such as the Defense Information System Network, the Defense Message System, the Global Command and Control System, and the Global Combat Support System.

Other DOD initiatives on cyber security include steps taken by the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD/C3I) to assist Defense Criminal Investigative Organizations (DCIO) and Military Counterintelligence Agencies to respond to the growing number of cyber intrusions and cases involving computer evidence. On June 28, 1996, OASD/C3I established the Defense Computer Forensics Laboratory (DCFL) to develop state-of-the-art cyber forensics tools and provide forensics analysis to DCIOs. In addition, the DOD Computer Training Program (DCITP) was created to develop and provide computer investigation training to cyber investigators within DOD.

4.0 CYBER FORENSICS

Cyber forensics is a discipline that includes computer forensics techniques by law enforcement investigators and the national security community to investigate potential criminal or national security events that involve the use of information systems. Federal, State, and local government agencies of all sizes and jurisdictional responsibilities are increasingly finding critical investigative information stored on computers. These computers range in size from microcomputers to mainframes and in complexity from simple stand-alone desktop computers to complex networked systems with data distributed worldwide. Computers can be huge electronic filing cabinets containing vast amounts of data, instruments of the crime in cases such as hacker intrusions, or containers of contraband such as stolen passwords and user identification. Given the proliferation and sophistication of information technologies, there is an increasing probability that crucial evidence in the form of computers and related items will play a significant role in future criminal and national security investigations. Cyber forensics is the discipline of acquiring, preserving, retrieving, and presenting data for review from this unique evidence.

Cyber forensics relies on detailed, documented, and certified sets of policies and practices, i.e., protocols, that describe the examination processes in technical detail and that are legally defensible. Protocols are discoverable in both criminal and civil trials. Because these

examinations will likely become issues before a court, the cyber forensics process must serve two masters. First it must be technically robust to address questions of complete recovery of probative information without altering the original material. It must then meet the legal requirements of acquisition, storage, examination, and distribution in a manner that is entirely consistent with the rules of evidence. In criminal cases, there may be specific limits on the information that may be recovered and examined (privilege and e-mail issues, for example) and who may be party to the examination (grand jury material, for example). It is unlikely that any informal or ad hoc approach to cyber forensic examination will meet these requirements and produce admissible evidence.

The ideal situation places the computer examination process in a laboratory environment; however, practical issues often require that computer forensic experts travel on site in support of investigations. This requirement is typical of investigations of financial crimes in which seizure of computer systems would interfere with legitimate business operations, health care fraud investigations where computer systems are considered part of the health care delivery system, and investigations where privileged information is likely to be encountered. An attack against national security systems presents a similar challenge. Policies and practices must also be in place for these remote efforts to assure that these on-site requirements are met with the same high degree of technical competence and professionalism as would be expected in the laboratory.

The software utilities necessary to conduct these examinations include disk imaging, restoration of erased and deleted files, slack and free space data recovery, text string search, known file filters, and data integrity checks such as CRC and MD-4 and 5. For these software utilities to be acceptable to the court, any special-use (i.e., not COTS) utilities should be certified by an objective third party. Likewise, protocols should receive thorough peer review and represent the state of the art in good laboratory practice.

The FBI reports that the number of criminal cases for which computer evidence was submitted has grown exponentially in the past few years to nearly 2,200 cases in 1997. An even larger number of cases in which computer evidence is recovered exist at the civil or administrative inquiry level throughout Government and the private sector. All cases, criminal, civil, and administrative, deserve to be handled competently and professionally. The volume of material stored on computers, and the litigious nature of many civil and administrative inquiries, combine to require that plans and policies be prepared, in place, and understood before they are needed. With a growing cyber crime caseload, it is clear that industry, law enforcement, and the national security community need to work together to ensure that all parties involved with investigating cyber-based events have ready access to the needed tools, techniques, and capabilities.

5.0 EDUCATION, TRAINING, AND AWARENESS

Providing the best tools to cyber investigators is only one step in responding to the rising cyber security threat. With the frequency and sophistication of cyber crime rapidly rising, defense against the threat demands thorough training for investigative officers and systems administrators to prevent, detect, and respond to cyber intrusions. Any successful initiative to address the threat must not only provide investigators with the comprehensive training needed to

respond to and investigate intrusion incidents but should also make systems administrators aware

of their key roles and responsibilities in responding to cyber intrusions.

The electronic nature of this threat is troublesome for investigators because cyber crime challenges traditional policies, procedures, and protocols for investigating crimes and collecting evidence. A cyber investigator must use traditional investigative skills combined with knowledge of network systems to conduct an investigation in an automated environment. Investigators need comprehensive training to understand the operation of an information system and the type of crimes that target information systems or use computers as an instrument of the crime, as well as provide the context of the interconnected environment in which these crimes are committed. This training requires basic knowledge of computer hardware and software technology, network operating systems, Internet and intranet protocols, and intrusion techniques and tools. Law enforcement agencies have recognized the need to train their cyber investigators and have integrated programs to augment their cyber investigation capability; however, the resources allocated for training, while growing, are not sufficient to keep pace with the rapid growth and sophistication of the cyber security threat. This problem is further exacerbated by the fact that many of the "first responders" to a crime scene are likely to be local law enforcement officers or field agents not trained in cyber investigative techniques. For this reason, training programs need to be extended to the full range of investigators.

System administrators are responsible for maintaining information systems and are often the first responders to an electronic intrusion. System administrators need proper training to be able to help in investigating intrusions. NSTAC concluded in the *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, "There is a lack of guidance to employees as to how to respond to intrusions and capture the information required to conduct a law enforcement investigation."[8] Training materials and guidelines must be established to make system administrators aware of what information investigators need and what procedures they must follow to collect evidence on an intrusion.

6.0 FINDINGS

In its investigation of cyber security issues, the Electronic Commerce/Cyber Security Subgroup concluded that a stronger partnership between industry and Government is required for the following reasons:

- The NS/EP implications of cyber security necessitate developing a partnership with industry, law enforcement, and national security communities, and PDD-63 lead departments and agencies.

- The size and complexity of the cyber crime caseload coupled with the growing sophistication and proliferation of computer-based tools used to attack information systems challenges traditional policies, procedures, and protocols for investigating crimes and collecting evidence.

[8] NSTAC Network Group, *Report on the NS/EP Implications of Intrusion Detection Technology Research and Development*, December 1997.

- Cyber investigators also face the challenge of staying abreast of industry's continuous introduction of new and innovative technologies.

- These new technologies introduce additional vulnerabilities that are being exploited.

- Industry possesses knowledge, tools, and expertise investigators could leverage as they respond to increasingly complex and sophisticated cyber crimes.

A key element in a dialogue with industry and Government will involve establishing the appropriate levels of trust and understanding that spur cooperation to address cyber security issues. This dialogue will allow representatives from industry and investigative communities to develop a unique understanding of the perspectives and issues faced by their counterparts. The Government and NSTAC Network Security Information Exchanges (NSIE) and the National Coordinating Center for Telecommunications (NCC) are examples of effective partnerships between the telecommunications industry and Government. The principles of cooperation exercised in these forums could be applied in efforts to address cyber crime.

With its years of experience of working with the Government on NS/EP telecommunications, network security, and information assurance issues, NSTAC is positioned to build on this experience in developing a partnership with the law enforcement and national security communities to address cyber security issues.

7.0 RECOMMENDATIONS

Based on the findings of the Electronic Commerce/Cyber Security Subgroup, the following recommendations are proposed.

7.1 Recommendation to the President

The President should direct the appropriate departments and agencies to continue working with the NSTAC for the development of policies, procedures, techniques, and tools to facilitate joint industry□Government cooperation on cyber security.

7.2 Recommendation to the NSTAC

The NSTAC should continue to work with the presidentially directed departments and agencies in furtherance of the recommendation above.