

FOIA MARKER

This is not a textual record. This is used as an administrative marker by the Clinton Presidential Library Staff.

Folder Title:

NII Security 1995 Report [National Information Infrastructure Security Group]

Staff Office-Individual:

Strategic Planning-Bobbitt, Philip

Original OA/ID Number:

1750

Row:	Section:	Shelf:	Position:	Stack:
49	1	11	2	V

NII SECURITY: THE FEDERAL ROLE

June 5, 1995

I. INTRODUCTION

The National Information Infrastructure (NII) is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits.

Security is critical to the development and operation of a viable NII. In fact, one of the goals stated in "The National Information Infrastructure: Agenda for Action," is to ensure information security and network reliability. Without the confidence that information will go where and when it is supposed to go, and nowhere else, the NII will not be used to support health, education, commerce, public services, and advanced communications to the fullest extent. In the NII, security¹ means:

- . integrity -- assuring that information will not be accidentally or maliciously altered or destroyed;
- . reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and
- . availability -- assuring that information and communications services will be ready for use when expected.
- . confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons;

To articulate and implement the Administration's vision for the NII, the Vice President formed the Information Infrastructure

¹ The discussion of security in this report encompasses a number of substantive issues which are tangential to security, such as protecting intellectual property rights. The report does not attempt to set the underlying norms for these areas, but rather discusses protection of such information.

Task Force (IITF). The IITF is chaired by Secretary of Commerce Ron Brown and is comprised of senior Administration officials having expertise in technical, legal, and policy areas pertinent to the NII. The NII Security Issues Forum was established within the IITF to address the important cross-cutting issue of security in the NII. The Forum is chaired by Sally Katzen, the Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget, and includes representatives from each of the IITF's committees as well as representatives from each Executive branch organization with significant information security responsibilities.

In addition to the IITF, the President has established the U.S. Advisory Council on the National Information Infrastructure. The Advisory Council includes representatives from industry, labor, State and local governments, and public interest groups, and advises the Secretary of Commerce on issues relating to the NII. Mega-Project III, one of three work groups of the Advisory Council, is addressing security, intellectual property, and privacy issues as they relate to the NII.

To better understand what will be needed to make the NII adequately secure, the NII Security Issues Forum and members of the U.S. Advisory Council on the NII held seven public meetings to discuss the security needs of likely users of the NII. Based on the first several meetings, the Forum proposed a set of five security tenets (set forth below) for public comment, which characterize in layman's terms the security needs of users of the NII.²

The purpose of this report is to expand on those tenets and begin to articulate security expectations for the NII in order to develop a broad consensus of the appropriate Federal role. Specifically, this report:

- . Summarizes the Forum's findings concerning security needs in the NII;
- . Presents an analysis of the institutional, legal, and technical issues surrounding security of the NII; and
- . Proposes Federal actions to address these issues.

PUBLIC PARTICIPATION

² Although Mega-Project III co-sponsored the public meetings, this draft report is the product of the NII Security Issues Forum, a Federal organization. The Forum looks forward to receiving advice about this report from Mega-Project III through the NII Advisory Council.

Over the past year, the Forum, in cooperation with Mega-Project III of the U.S. Advisory Council on the National Information Infrastructure, conducted seven public meetings between government officials and members of the private and public interest sectors.

A general meeting was held on July 15, 1994, at which individuals representing business, manufacturing, banking, health, entertainment, publishing, education, libraries, and government services discussed their views of security needs in the NII. Subsequent meetings addressed the needs of various sectors using the NII. The subjects of the meetings were:

- (1) "Commercial Security on the NII," which focused on the need for intellectual property rights protection in the entertainment, software, and computer industries;
- (2) "Security of Insurance and Financial Information";
- (3) "Security of Health and Education Information";
- (4) "Security of the Electronic Delivery of Government Services and Information";
- (5) "Security for Intelligent Transportation Systems and Trade Information"; and
- (6) "The NII: Will It Be There When You Need It?" addressing the availability and reliability of the Internet, the public switched network, and cable, wireless, and satellite communications services.

In order to continue and expand this public dialogue, this draft report, "NII Security: The Federal Role," is being issued for public comment. In addition to receiving comments, the Forum will sponsor two public meetings this Summer to discuss the Report.

This report includes a set of proposed government action items in section IV. This is intended to articulate the areas in which the government will act to improve the security of the NII. The next step is to receive and respond to public comment on the report in order to develop consensus regarding the Federal role and its proposed actions.

II. FINDINGS

Based on the initial dialogue, the Forum is proposing three actions: (1) adoption of proposed NII Security Tenets, (2)

adoption of Organization of Economic Cooperation and Development (OECD) Security Principles for use on the NII, and (3) implementation of the Federal role described at the end of this report.

A. SECURITY TENETS

On February 10, 1995 [see Vol. 60 No. 28 of the Federal Register, p. 8100], the IITF proposed five security tenets for public comment, based on the general proposition that people who use the NII want to know that their information goes where and when they want it to and nowhere else. The tenets are comprised of five common propositions that emerged from the early public meetings about what NII participants expect. Clearly, the details of implementation of the tenets will vary by user -- whether teachers, doctors, or tax preparers -- and by application -- whether communicating over a two-way multi-media conference, sharing data between doctors and patients, or calculating a tax return. Participants expect:

- 1) The ability to control who sees (or cannot see) their information and under what terms.
- 2) The ability to know who they are communicating with.
- 3) The ability to know that information stored or transmitted is unaltered.
- 4) The ability to know when information and communication services will (or will not be) available.
- 5) The ability to block unwanted information or intrusions.

Two conditions attach to these security tenets:

- 1) None of these tenets is absolute. For each tenet there may be valid societal reasons -- such as an emergency or a need to protect another's rights -- that cause the tenet to be conditioned in some manner.
- 2) Each tenet requires NII participants to take responsibility for establishing the terms and conditions under which they will exchange information. The distributed and empowering nature of this technology demands a greater level of personal responsibility from participants than when communications systems were more limited in scope and scale. Education of NII participants is thus a critical task.

B. OECD PRINCIPLES

The U.S. is not alone in addressing security concerns in the evolving global information infrastructure. The organization for Economic Cooperation and Development (OECD) has adopted Security Guidelines. The U.S. and 23 other member nations of the OECD have endorsed these Guidelines. The Guidelines encompass nine Security Principles, which articulate high-level needs, such as the need for explicit accountability for security, the need for awareness of security practices and procedures, and the need to respect the rights and legitimate interests of other users. These Principles are included as Appendix A. The IITF proposes to adopt those Principles for use in the NII.

The OECD Principles are being incorporated into two National Institute of Standards and Technology (NIST) publications, "An Introduction to Computer Security: The NIST Handbook," and "Federal Computer Security Principles and Practices" (working title). These two publications complement each other -- the Principles and Practices publication will provide a quick reference to accepted security practices. The Handbook explains the Principles and Practices and provides a bibliography and extended examples.

C. PROVIDER AND USER SECURITY CONCERNS

The public meetings solicited discussion with a broad range of NII participants, both users and providers of NII services. Regardless of the commercial, industrial, or public interest use represented, the participants shared a number of concerns. These concerns included: the potential inability to control secondary uses of information; questions of liability for loss or inappropriate access to or use of information; a mistrust of government's use of information; the desire to protect one's own system from outsiders, whether by hostile attacks or junk mail; and risk of system failure at times of critical need. The most-heard concern was that personal information, such as information pertaining to an individual's finances, health, or purchasing habits, could be disclosed to or manipulated by an unauthorized user. These shared concerns were generalized in developing the security tenets described above.

In addition, some participants seemed to desire a greater government role, such as censorship of defamatory or pornographic information transmitted over the NII, or additional funding for national security and emergency preparedness programs. Other participants seemed to desire a lesser government role. For example, some participants desired open access to and use of virtually all information and systems without interference. Other participants criticized the Federal government's export control policy, which limits the export of powerful cryptographic systems.

Still others were suspicious of the technology underlying the NII and how it would be used. Some witnesses were also concerned that government's involvement could create greater inefficiencies, increase susceptibility to invasions of privacy and risk of fraud, and contribute to the depersonalization of society.

The following summarize the concerns and needs heard at each of the public meetings. Transcripts are available on the NII bulletin board at the Department of Commerce. (For Internet access, gopher, telnet, or anonymous ftp to iitf.doc.gov. Access is also available over the World-Wide Web. Dial-up access by modem is available at (202) 501-1920. Set parameters at no parity, 8 data bits, and one stop. Speeds of up to 14,400 baud are supported.)

1. Entertainment, Software, and Computer Services

Images, movies, music, software, and a variety of products that can be transmitted in digital form can be easily altered or copied. The protection of intellectual property rights in an electronic age requires technology, legal protection, and institutions that promote fair use, support licensing and payment, and prevent unauthorized copying, alteration, or distribution. There was considerable discussion about effective legal protection and institutions. A thorough treatment of intellectual property on the NII will be found in the IITF White Paper.³

A number of possible technological approaches were described at the meeting, including software that is programmed to be disabled after a span of time if the software is not paid for. Another technique described was to distribute an encrypted movie with a key that can decrypt it (for viewing) one time only. One intellectual property entrepreneur electronically distributed his work -- visual images -- in encrypted form and then sold the decryption key through the regular mail. This solution allowed him to distribute digital images electronically, but it did not prevent the buyer from redistributing the work after they decrypted it. Generally, participants indicated that adequate technical capability was being developed to protect their own products. Technical challenges remain, however, including the need for an automated copyright management system for digital works. In addition, several witnesses raised a concern about government barriers to the development and sale of technologies such as export control laws.

³ The report is expected to be issued in June, 1995. For a copy of the report, contact the U.S. Patent and Trademark Office, Washington, D.C. 20231, or call (703) 305-9300.

2. Health and Education Information and Services

Health care will be improved by computer-based patient records, on-line databases, consumer health information, and remote treatment and advice. However, improved access to information also brings with it a risk of improper disclosure, alteration, or use of highly personal information. Patients' well-being will become dependent on the integrity and reliability of such information in the NII. In particular, the reliability of such computerized medical records systems will be of critical importance as the health care system shifts away from paper. Similarly, educational records can have a substantial effect on individuals' economic well-being.

Participants suggested that the technology will need to promote information integrity, and to ensure that access is provided on a need to know basis, that records that serve different functions are separated, and that the records are destroyed when they no longer serve their function. Concern was also raised about the availability of pornographic material on the Internet and the need to protect children from exposure to it.

3. Financial, Insurance, and Commercial Services

The financial and insurance sectors have relied for decades on closed networks in order to reliably transfer funds and share information. As their networks become more open, new security tools and techniques will be needed to protect the confidentiality and integrity of valuable commercial information. Questions of liability will also arise if improper disclosure of customer information occurs while it is being transmitted over the public switched network.

As consumers use the NII to conduct business, they will want to verify that a payment or order was received correctly. Without a face-to-face transaction to verify the authenticity of the customer and of the vendor, the potential for fraud increases for both parties, requiring methods of electronic notarization, digital signatures, and date-stamping.

The advent of so-called digital cash involves a different challenge. It requires a technical method to avoid forgery and authenticate the current owner. On the other hand, some witnesses favored the ability to anonymously execute transactions. A number of products are already being tested to provide "electronic cash" on the NII.

One witness pointed out that the vast majority of technical solutions address the issue of protecting an organization's data

from individuals, while little attention has been paid to the problem of how the individual's data can be protected from organizations. This situation is illustrated by the way in which data about an individual's purchasing habits is bought and sold in private markets. Other personal information which is generally publicly available, such as marital status, home ownership, and status in legal proceedings, is collected by the private sector and sold as a commodity. Some individuals expressed a desire to exercise greater control over the use of this information, or to be reimbursed for its use. The IITF's Privacy Working Group is developing principles to guide policy development in this area.⁴

4. Intelligent Transportation

Intelligent transportation systems include applications such as electronic toll collection, in which a toll payment is automatically deducted from a card with a computer chip so that cars won't have to stop as they pass through toll booths. Such systems may also help monitor traffic patterns and road conditions through cameras or other sensors, and provide drivers with information in their cars about the quickest route.

A basic security concern with electronic toll collection is funds control and integrity. In addition, there are concerns that the information collected in these transactions, including information about the owner of the vehicle, how fast he or she was driving, and where he or she was headed, could be used inappropriately. Access to this information could disclose commercial proprietary information or compromise personal privacy. Furthermore, as transportation becomes more dependent on automated control systems, the movement of people becomes subject to security risks. For example, a security breach could allow mischief such as switching all the traffic lights to green, thus promoting accidents.

5. Government Information and Services

Use of the NII is becoming integral to virtually every Federal program, and Federal agencies are becoming dependent upon that use for execution of their missions. The NII will support programs as varied as air traffic control, compilation of the decennial census, response to natural disasters, and delivery of social security benefits.

⁴ "National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary;" January 20, 1995; 60 FR 4362.

This use of the NII in Federal operations promises improved efficiency of governmental program delivery. However, it also introduces new and varied security vulnerabilities, not unlike those faced by other users of the NII. The difference, of course, is that addressing these security vulnerabilities is a direct responsibility of the Federal government, since such vulnerabilities could degrade Federal program effectiveness and resource safeguards, and affect the integrity, confidentiality, and/or availability of government information.

At the meeting, the use of "smart cards" or electronic debit cards for delivering food stamps was discussed in depth. Smart cards provide the advantage of on-time payment, increased dignity, and improved efficiency in program administration. However, cards can be lost, and there are opportunities for fraud by converting the credits to cash. Other concerns include the potential for counterfeiting such cards or otherwise manipulating the value of the cards. Unauthorized access to individual purchasing records could violate personal privacy. Users of these cards need confidence that the benefits will be available when they expect them to be, and that associated information will not be abused by those with access to it.

6. The Public Switched Network and the Internet

As new technologies are integrated into the public network, new vulnerabilities are introduced. Some technologies are more vulnerable than others. For example, wireless communications are particularly vulnerable to eavesdropping, while cable and satellite television providers face an ongoing battle to protect the commercial information they are sending to consumers.

As individuals and organizations become more reliant on the NII to conduct personal and business transactions, the availability and reliability of the network is of greater importance. These concerns vary from the risk of major network outages to the minor irritant of slow or noisy network connections. Users need assurances that the NII will be there when they need it. If it isn't, they want meaningful recourse. For certain transactions, users also desire an assurance that information was received by the intended recipient, analogous to "certified mail."

Users will depend not just on the availability and reliability of the information itself and of the system on which it resides, but indirectly on the availability and reliability of the network which transports the information between systems. From the perspective of the providers of network services, security threats include natural disasters such as fires, floods, or hurricanes; physical attacks, such as bombs; electronic attacks, such as computer viruses; and unintentional errors, such

as design flaws, software bugs, and human error. Network services providers are addressing these threats as an integral part of their business. During the public meetings, some participants were open to appropriate Federal involvement in this area, while others were more cautious about the Federal role in this area.

Other concerns include the risk that hackers may intentionally compromise the security of personal or organizational computer systems, or maliciously gain access to information while it is moving from place to place within the NII. These fears are grounded in well-publicized incidents on the Internet and public switched network, but actually comprise only a small fraction of computer security incidents. The majority of incidents are caused by authorized individuals doing unauthorized activities. There was some discussion of the need to share information among providers concerning the outside threats to networks, as well. Other security concerns included the need to verify whether information was altered accidentally and the need to ensure availability of networks in the event of natural disasters.

III. ANALYSIS

The NII security needs expressed above can be organized into three areas: (1) coordinating functions, (2) oversight and enforcement for public safety, and (3) technical security needs. The three areas are interrelated. For example, for Federal computer crime law to be enforceable against a system trespasser, security measures must have been in place and a record made of the trespass. Similarly, civil liability standards of due care require that effective technical security be in place. At the same time, overall security is enhanced if there are criminal or civil legal sanctions which act as deterrents.

The following section addresses the functions necessary to support a secure NII, as heard in the public meetings. The section on oversight and enforcement for public safety addresses how existing oversight organizations need to adapt to the oversight of NII related activities, as well as whether current laws are sufficient and enforceable in the context of the NII. The discussion on technical security addresses the technical ability to protect information and systems in the NII.

A. COORDINATING FUNCTIONS

The National Research Council's (NRC) report, "Realizing the Information Future," notes that while security needs can be addressed to some extent by technological methods and a legal framework, structures must be in place to make them work. This

section is intended in part to contribute to the dialogue about and development of such an architecture, by describing the coordinating functions which emerged based on public discussions of security of the NII. Some of these functions will be fulfilled by the private sector, some by government, and others in partnership.

If the NII is to succeed, a structure or a collection of structures -- a security architecture -- must exist to ensure security. The NRC report states: "This security architecture must include technical facilities, recommended operational procedures, and means for recourse within the legal system." This architecture will be based on a variety of public and private institutions and policies. Although an architecture will define how institutions, policies, and technologies interconnect, a sound security architecture will consist not of rigidly prescribed technologies or solutions, but must be able to flexibly adapt to change. The report also notes that such an architecture will require research and development over time.

1. National and Economic Security

As the United States as a whole becomes increasingly reliant on the NII for communications and information, other key components of the U.S. infrastructure will become dependent on it. For example, the power grid, transportation systems, financial institutions, and economic transaction data will all be dependent on the NII. Security weaknesses in the NII can place those infrastructure elements at risk. Hence a significant attack on the NII would be a threat to our national security in addition to the significant personal and economic harm it would cause.

From the Federal government's perspective, public safety and the national defense call for a secure NII. All Federal entities that oversee various parts of the U.S. economic infrastructure must be aware of the changing risk that increasing reliance on the NII entails. They also must be aware of the various types of threats to the NII and their magnitude.

2. Ethics and Education

There was a general concern at the public meetings about the lack of regard that many participants in today's Internet had for others' intellectual property and privacy. This was often characterized as youth in its search for knowledge and disdain for bounds of ownership of electronic information. Several presenters noted that often young persons have tremendous technological savvy, but little understanding of the ethical responsibilities that such knowledge entails.

Witnesses at the public meetings specifically suggested a need for training and awareness in the general area of computer ethics. The basic principle should be a respect for others' rights on the NII. Whether in the office, university, elementary school, or at home -- where today's children are learning to use computers -- parents, teachers and supervisors should emphasize that it is not only wrong, but illegal, to copy copyrighted software or other materials or to break into someone else's file or computer system. It was noted that the Education Department, in cooperation with the Intellectual Property Rights Working Group of the IITF, has begun to develop a model curriculum on the importance of protecting intellectual property. Participants at several meetings described the need for ongoing dialogue on this subject among all users.

A final issue where more dialogue is needed is the protection of children from exposure to inappropriate materials on the NII. As President Clinton has stated:

"I believe that insofar as governments have the legal right to regulate obscenity that has not been classified as speech under the First Amendment, and insofar as the American public widely supports, for example, limiting access of children to pornographic magazines, I think it is folly to think that we should sit idly by when a child who is a computer whiz may be exposed to things on that computer, which in some ways are more powerful, more raw and more inappropriate than those things from which we protect them when they walk into a 7-Eleven." ⁵

3. Emergency Preparedness and Response

Three types of emergency preparedness and response roles were described during various meetings: (a) the need for an entity analogous to the Computer Emergency Response Team (CERT), which currently acts as an Internet "911," (b) a system for planning and recovery during and after an emergency which sets, among other things, a priority of restoration, and (c) a need to exchange information concerning mutual vulnerabilities.

(a) Emergency response. As the Internet is evolving from a research and development experiment to a widely used public communications medium, the need for an emergency response entity to coordinate the community's response to security threats has become apparent. In the Internet the entity that currently performs that function is the Computer Emergency Response Team (CERT). It is likely that function will need to continue in the

⁵ Remarks to the American Society of Newspaper Editors, Dallas, Texas, April 7, 1995.

NII.

(b) Emergency planning and recovery. In order to maintain a state of readiness or respond to and manage an emergency or crisis, an emergency preparedness capability is required. The government has established the National Communications System (NCS) to ensure the availability of communications services required to support emergency planning and response functions. The NCS's National Coordinating Center for Telecommunications is staffed full-time by both government and telecommunications industry representatives, whose mission is to respond to both military and civil emergencies, e.g., Operations Desert Shield/Desert Storm, Hurricane Andrew, the Northridge earthquake, and more recently, the bombing of the Federal building in Oklahoma City. A similar function is likely to be needed to ensure the availability of NII services to support emergency planning and response functions.

All users have an interest in having service restored in the event of an emergency or disaster such as an earthquake or flood. In the public switched network, telephone service is restored based upon governmentally established priorities, with the highest priority given to organizations whose function it is to respond to such emergencies, such as the Federal Emergency Management Agency (FEMA). As users rely more on the NII for critical functions, a similar need for setting priorities for restoration on a broader level will arise.

(c) Exchanging information concerning vulnerabilities. Participants at several meetings discussed the need to exchange information about mutual vulnerabilities in the NII as it evolves. They indicated that improved security resulted from meaningful communications among users and providers. If a problem is identified, it can be quickly solved. In describing this role, some pointed to CERT bulletins as a model. Others pointed to the NCS's program to facilitate appropriate sharing of security vulnerability information. Others described different possible mechanisms, such as industry newsletters and trade publications, engaging in mutual assistance agreements with other parties in the private sector, and on-line news groups.

4. Quality Assurance

Some participants in the public meetings asked how they could be sure that the security products they chose were as good as they claimed to be. Testing by independent third parties such as nationally recognized testing laboratories, organizations that certify that products meet or exceed the requirements of a specific standard, may be useful for those trying to evaluate the effectiveness of security products. Such third party testers may evolve into a system for evaluating security products. A

certification procedure could be useful for both producers and users of security products who may be trying to be more competitive and to protect against the threat of lawsuits. Utilization of the trademark system may also operate to provide assurance of performance. The trademark system may be useful in allowing consumers to develop confidence in a particular trademark that could result in continued purchase of both a particular product and of others bearing the same trademark.

Additionally, an independent entity representing consumers' interests such as a "Better Business Bureau" could provide a place to file complaints and answer questions about various NII service providers. Either government, trade associations, industry groups, or private sector consultants could fulfill this need.

Related to the issue of accreditation is that of standards. Security products and services can be tested as meeting either a performance standard or a technical standard. Standards in the United States are developed primarily by private standards development organizations representing industry, trade, and professional organizations. For example, the American National Standards Institute (ANSI), the Institute for Electrical Engineering and Electronics (IEEE), and others are active in this area. Sometimes a Federal government standard becomes the accepted international standard. Many of these organizations work together through the International Standards Organization (ISO). Internet standards have been developed somewhat more informally and quickly by the Internet Engineering Task Force (IETF).

Alternatively, any group of users can define a set of security standards and agree among themselves to be bound by them. Such "affinity groups" design or decide on standards to meet the specific needs of their members. During the public meetings, participants described unique problems such as the need for a particular database to increase the integrity of information, or to help their industry improve its use of electronic processing and networking. These standards may become de jure standards formally accepted by industry, or they may remain de facto standards. In addition, de facto standards are often set by dominant industry participants. Quality assurance and other security standards must be developed in full recognition of the complex standards-setting environment.

B. OVERSIGHT AND ENFORCEMENT

There is a need for effective law and oversight of both the NII itself and of public safety-related uses of the NII. A sound legal system that applies civil remedies and criminal penalties is essential to fulfilling this need. In the public meetings,

participants focused primarily on civil remedies and litigation, rather than criminal issues. In addition, considerable activity is occurring in State, local, and Tribal governments, particularly regarding criminal computer law.

1. Law and Regulation

Various activities are overseen by government because they affect the well-being of the nation. For example, some sectors of the economy are regulated to ensure the public health or safety. As these activities become increasingly reliant upon the NII for communications and information, a security weakness in the NII can become a threat to the public health or safety. To effectively manage risk in their public safety oversight role, Federal agencies will need to ensure the secure use of the NII by their overseen sector. Thus, for example, the Transportation Department may need to adjust its regulatory oversight of aircraft to account for the risks involved in aircraft's use of the NII. Similarly, the Securities and Exchange Commission may need to adapt its oversight of securities exchanges, and the Treasury Department and the Federal Reserve Board their oversight of the nation's banking system.

2. Civil Law

Civil litigation includes specialized or statutory suits, contract actions, tort actions, and injunctive relief. Several participants in the meetings stated that issues of liability must be resolved before widespread use of the NII occurs. In reality, however, a range of accepted solutions and practices concerning information security will be decided in increments through the court system as a body of case law develops over time.

Civil law addresses the issue of liability. In every public meeting, users and providers of NII services questioned how the current system of liability for damages would affect their use. For instance, concerns were raised that unknown exposure to liability could prevent potential providers from offering services.

Specialized suits can be used to protect intellectual property rights against copyright, patent and trademark infringement, or other violations of established statutory rights. Whether a particular statute extends to activities on the NII when Congress did not specify the statute's application in a networked environment may be subject to litigation on a case-by-case basis.

Contract actions are law suits contesting provisions in express or implied contracts. Tort actions resolve disputes for

money damages alleging a breach of a duty which caused harm to the plaintiff. Injunctions involve obtaining a court order to prevent specific actions or require certain activities. For example, such an order might prohibit use of the Internet in a certain way or require a user to make certain disclosures before using the Internet. Other forms of civil action and novel theories of liability involving all aspects of the NII continue to evolve.

Civil liability is likely to create incentives for improving security of information systems.⁶ If users, system managers, and service providers face liability in contract for failure to perform a contractual duty, or liability in tort for negligence, they will have an incentive to take reasonable steps to secure their systems, ensure accuracy of their data, and limit unauthorized access and use. A presenter at one public meeting noted that some private parties currently protect their proprietary information by simply not putting it on networks. Attaching legal consequences for the unauthorized or improper use of electronic data will increase the likelihood that the NII will be a trustworthy, reliable system.

Courts are beginning to be confronted with cases that test the effects that civil liability practices will have on the security of the NII. Until a settled body of law develops, various parties' responsibilities and potential liability for negligent security will be uncertain. Legislation that would impose criminal and/or civil penalties for security violations such as blocking, tampering, masquerading, or denying service in the network environment is, of course, possible. However, consensus about what constitute reasonable standards for information security will be difficult to achieve. Because security requirements greatly vary in different contexts, such as finance, law enforcement, medicine, national security, research, and education, there may be a need for context-specific standards that can evolve as requirements change.

3. Criminal Law

Traditionally, laws have focused explicitly on the computer, since it could be easily recognized as the venue where a crime occurred. The laws were intended to protect the information

⁶ Lost or scrambled files, system downtime, invasion of privacy, and economic or physical injury can be foreseen as a result of sloppy security of networks. For example, liability for system managers can be envisioned for failure to enforce password expiration, eliminate access by former employees, replace default configurations, or implement technical solutions to prevent or reduce breaches in security.

contained in computers. Technology, however, has evolved so that proscribing conduct with regard to computers does not adequately protect information. Today, information can be intercepted and modified in transit between computers, or when it is present in devices not typically thought of as computers, such as telephones, cable systems, satellite and cellular channels, etc.

Many actions that would compromise security of the NII are already criminal violations. For example, it is illegal to conduct a wiretap without a court order. Fraud, whether perpetrated electronically or not, is a criminal offense. In other areas, laws may need to be amended.

Legislative efforts to protect computers and information suffer, on the one hand, from having to exhaustively yet clearly define these terms in order to make the laws meaningful. On the other hand, the laws must be sufficiently broad and adaptable that the statute will not be rendered obsolete by rapid technological change. For example, current law may not deal well with the problem of intrusive code, also known as a computer virus or worm. That is, it may be difficult to prosecute the distributor of these destructive instructions if that individual never actually "accessed or used" the affected computer.

Although existing laws provide some protection, new laws will be needed to insure that the NII is protected adequately. For example, 18 U.S.C. Sec. 1030(a)(5) should be extended to protect all United States Government and financial institution computers, even if the computer is not used in interstate commerce or communications. Additionally, the statute should specifically apply to computers used in foreign communications, not just interstate communications. These and other changes must be made to ensure that laws keep pace with new technologies.

In order for the NII to be secure, laws must be enforceable. Hence, law enforcement officials such as police officers must maintain the ability to enforce laws effectively in it. Future crimes are likely to be planned and coordinated using the NII. The NII will also be used by criminals to smuggle stolen corporate information, engage in the transmission of child pornography, engage in industrial sabotage, or electronically stalk, terrorize, or threaten other NII users. In all of these cases, law enforcement must be able to protect citizens.

4. International Issues

International computer offenses are easier to commit than traditional international crimes, because they do not necessarily require additional manpower or physical transportation. Someone can ship information covertly via telephone and data networks. They need no passport and pass no checkpoint, but cross borders

simply by typing a command.

Second, computer crime has not received the emphasis given other international crimes. Until relatively recently the United States, probably the most computerized nation, has not mobilized against computer criminals, even though it is the frequent target of such computerized attacks. Although the U.S. now recognizes the seriousness of the threat, it is not surprising that less computerized countries do not yet fully share this awareness.

Many countries have weak or no laws against breaking into computers. Those with strong laws find it difficult to engage in fruitful cooperation with those without. The vulnerability of both modern and modernizing nations has been highlighted by recent events:

- . A Christmas card message sent over BitNet, the international academic computer network, landed in 2,800 machines on five continents including IBM's internal network. It took only two hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.
- . Pirate bulletin boards contain information regarding computer vulnerabilities and are being used to develop and perfect new computer viruses. Such bulletin boards have been found throughout the United States as well as in Bulgaria, Italy, Sweden, and the Soviet Union.
- . In China, computer criminals recently stole \$235,000 from a bank in Chengdu.
- . Recent reports indicate highly prolific virus writers are working in Bulgaria.

In order to improve international cooperation in the prosecution of computer crimes, the United States has joined international efforts to raise public consciousness about computer crime and encourage other countries to enact or strengthen their computer crime laws. In fact, other countries have been working both domestically and internationally in this area, particularly Denmark, England, Australia and Germany.

Consistent with this international effort, the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems require prompt assistance by all parties in cases where information security has been breached. Additionally, the Council of Europe is currently addressing procedural problems that arise in information technology crimes, such as how to quickly get international trap and trace information.

C. TECHNOLOGY

At the heart of information security in the NII is the technical ability for individuals to protect their information and systems. At every security meeting technical approaches in use or being developed to protect systems or information were discussed. These varied from techniques being used by firms to protect their intellectual property rights, to protection being designed into systems of electronic cash, to "firewall" techniques for protecting firms' networks when connected to the Internet. These public discussions indicated that the marketplace, to the extent that users are demanding security, is responding with both specific security products as well as general NII products and services that incorporate security protection.

At the same time, the security technology challenges of the NII are formidable. Information and services will need to be protected, yet also available to communities of interest. Much of the technology that will be used to provide security in future use of the NII is yet to be developed. The discussion in this section that follows summarizes today's technological approaches to security, based on the public meetings. It should not be read as a complete description of the security technology needs of the future NII, nor to minimize the complexity of fulfilling those needs.

Security products and methods are necessary for individuals and organizations to be able to protect their systems and information in the NII. The many products and techniques that exist approach security from one of two principal strategies -- protecting a system from outside attack (e.g., firewalls), or protecting the information itself regardless of where it resides, normally through some form of cryptography. In addition, the networks themselves should be protected.

1. Protecting Systems

Like criminal laws, technical security measures have traditionally focused on controlling access to the system. As today's processing environment becomes more open, however, that task becomes significantly more difficult.

Participants in the public meetings demonstrated an understanding of a wide array of technical security techniques used to protect their systems. Moreover, a consensus view emerged that incentives exist for the marketplace to provide appropriate security techniques. A number of participants expressed surprise that the government was taking an interest in this issue, other than as a user. Most felt that their technical

security needs would be satisfactorily addressed by the private sector.

a. Access Control to Systems

Today, individual access to and accountability on systems is controlled largely by password management. That is, an individual is required to identify some unique piece of information known only to the individual and the system in order to identify himself to the system. Over the years, password schemes have become more complex to make systems more secure, and the ability of those trying to penetrate systems by obtaining passwords has become substantially better. For example, a large number of sophisticated password "sniffers" -- software programs designed to capture passwords as they are sent across hosts -- were recently detected on the Internet.

Stronger schemes for protecting systems include timed password-changing mechanisms. These mechanisms change acceptable passwords at timed intervals previously agreed upon between the system and a device held by individuals desiring to remotely access the network. Other methods are being developed to substitute for password schemes. They identify individuals to a system by the rhythm of their keystrokes or by biometrics such as fingerprints or a retinal scan.

b. Secure Gateways

Participants at the public meetings that use Internet noted that they were using secure gateways or "firewalls" to help protect their systems by limiting outside access to internal system capabilities. It was often noted at the meetings that, despite recent publicity about break-ins and breakdowns, strong technical measures exist that afford protection. Where break-ins have occurred, they normally exploit known weaknesses which have not been fixed, even though fixes are readily available.

A different concern raised by a number of participants at the public meetings is the need to block the reception of unwanted information. This can be a security risk because unwanted messages could overwhelm a receiver's ability to handle them and effectively shut down the receiver's system.

A view that was often presented was that individuals and organizations are responsible for making reasonable efforts to secure their systems, in the same way they have a responsibility to lock their doors to deter burglars from entering. Private sector firms are responding to the need for secure gateways by developing increasingly sophisticated commercial products. However, like seat belts in cars, they only work when they are

used.

c. Protecting Networks

Related to the security of systems is the security of networks. Networks, comprising a variety of technologies, are what connect systems with each other. The most common threats are breakdowns in the availability and reliability of the networks, resulting in slow or noisy connections, network outages, or loss of data. These threats can be caused by natural disasters such as fires, floods, or earthquakes, but also can include a physical attack, such as a bomb, or an electronic attack, such as a virus. Procedural errors such as design errors, software bugs, and operational mistakes can also place a network at risk.

Basic physical security precautions can help, such as fire protection systems and doors with locks. Back-up equipment enables a network provider to quickly restore service, while quality assurance software can minimize design errors, and technical security measures can warn about an impending breakdown or prevent an outage or loss of data.

2. Protecting Information

Protecting information requires different technology than protecting a system. Once information is outside a controlled system, there is little control over who can gain access to it. Therefore technology which can provide assurance that information itself can not be read, copied, or modified is critically important in an open processing environment such as the NII.

a. Cryptography

Cryptographic mechanisms already widely used are unique in that they directly protect information from being compromised or altered without authorization. It is envisioned that use of encryption and digital signatures will continue to grow rapidly. Cryptography is used by banks to assure the integrity of financial transactions, by computer operating systems to conceal passwords, by users of the Internet to protect the privacy and confidentiality of their communications, and by holders of smart cards to protect information contained on the card. There is no doubt that in the future there will be widespread use of this technology, which will be virtually transparent to end-users. Cryptography is also used in other security services, such as digital signatures and passwords.

Some participants noted that many hurdles remain to easy use

of cryptography. For example, one problem is the awkwardness of handling encrypted information. Also, the lack of a public key infrastructure makes it difficult for individuals and organizations to manage keys efficiently and to use public key cryptography. Another factor which has limited cryptography is the risk of unmanaged cryptography for business -- whether it be a disgruntled employee who encrypts corporate financial records before departing, an employee who is absent when critical files are needed, or merely someone who forgets the keys. Finally, the lack of agreement on cryptographic standards is slowing the proliferation of cryptography.

1. Confidentiality

Cryptography is essential to protecting the confidentiality of automated information. It provides the protection of information being undecipherable, even if someone gains access to it. It is this use that crystallizes a conflict between citizens' needs to protect confidential information and the societal need for justice and safety. Strong cryptography can be used to thwart law enforcement's legitimate ability to understand the contents of lawful wiretaps. On the other hand, weak cryptography will not provide effective protection of confidentiality of citizens' sensitive communications.

A number of alternative approaches to resolve this dilemma are being proposed. Many involve a key escrow approach whereby, keys to strong encryption are escrowed with a trusted entity. Under this approach, the keys would be provided to law enforcement authorities upon presentation of a duly-executed wiretap warrant. Some of these approaches could also assist firms in recovering lost data, where, for example, a key has been lost. Private sector approaches being developed to meet the needs of corporate key escrow may also benefit government, both as a user and in its law enforcement responsibilities.

As a user, government has its own needs for security. In order to protect its voice and low-speed telephonic data communications, the government has developed and fielded a technology to meet these needs, known as the Escrowed Encryption Standard, or "Clipper" chip. It is available for voluntary use by the private sector, but individuals may continue to choose to use any encryption technique domestically.

The private sector has reacted strongly to this initiative, objecting to the key escrow feature, to the fact that the technology is hardware-based, and to its use of a classified algorithm. However, this technology gives government no new authority or abilities. Instead, it enables government to protect its own information while supporting effective law enforcement.

2. Digital Signatures

In an open digital environment, verifying the source of a message or document and assuring that it has not been changed was mentioned as a concern in a number of different meetings. For example, in electronic payments there is concern that the correct payment is made to the correct individual. As noted at the meetings, the private sector is actively working on providing this capability and assuring effective protection. The underlying technology for such protection is digital signature.

A digital signature is created by applying an encryption algorithm to the information, resulting in a unique "signature" associated with the information. This signature is encrypted and sent with the information, which may or may not itself be encrypted. By verifying the signature and comparing it with the information, the receiver can verify that the contents of the message were not altered in transit. Of course, such a technique does not prevent or correct alterations, it only detects them.

While there are a number of different technical approaches to digital signatures, two are prevalent in the current environment. One, based on the RSA encryption algorithm, is coming into wide use in the private sector. A second, based on the El Gamal algorithm, has been adopted as the Federal standard for signature and is coming into use in the Federal government. Both require a public key infrastructure to provide a trusted third party, which will allow verification that the signer of a given document is indeed who he or she claims to be.

3. Public Key Infrastructure

In tomorrow's open networks, cryptography will help to verify the identity of a message sender, assure the integrity of a message, and protect information from unauthorized readers. Without some means of verifying where and to whom their information is going, people may hesitate to do business electronically. A Public Key Infrastructure (PKI) uses two keys, one public, like a phone number, and the other private, like a personal identification number (PIN) or password. The public key is listed in a public electronic directory, while the private key is kept secret by the individual.

The primary application of a PKI is to verify the identity of a message sender through creation of a digital signature. To create a digital signature, a sender of information uses her private key to sign the message. The receiver uses the sender's public key to verify the signature.

A PKI can also support confidentiality of messages. A sender of information obtains the receiver's public key and encrypts the data. The receiver uses his private key to decrypt

the information.

A public key infrastructure has great potential to encourage new activity on the NII because it provides a means to do business among parties without prior arrangements. For example, a mail order company posts its public key in an on-line catalogue. Customers send in their order with their credit card number in encrypted format. The company uses its private key to decrypt the information.

b. Protecting Against Copying

A more difficult technical problem that is being addressed by the private sector is protecting information against unauthorized copying. Technology using encryption to prevent data from being read by individuals who are not authorized to read it is readily available. However, preventing individuals from making unauthorized use of data they have been authorized to read is a more difficult technical problem to solve.

Once someone possesses a document in electronic form, it is easy to copy and redistribute it. If the information is copyrighted or protected by non-disclosure agreements, there is little more that the owner of the information can effectively do. Intellectual property owners are concerned that if they disseminate information with commercial value such as software, music, books, or video images, it will be widely pirated. Many of these property holders have traditionally disseminated in other media, such as paper or film.

Efforts to protect copyrighted software from unauthorized reproduction provide an interesting case study of the various approaches -- both legal and technical -- used to protect intellectual property rights. Some software developers have used cryptography to prevent illegal reproduction of their software. Alternatively, the Software Publishers Association (SPA) has a two-fold approach to this issue: it sues corporations that make illegal copies of copyrighted software, and it is also conducting a campaign to educate the public on software copyright issues. However, the international component of this problem makes legal and educational remedies difficult.

IV. GOVERNMENT ROLE AND RESPONSIBILITIES

The NII will be designed, built, owned, and operated by private citizens and private organizations. It will primarily be used by individuals and organizations, but it will also be used by Federal, State, local, and Tribal governments in support of their missions. The Federal government has an important role in the continued development and growth of the NII as a leader, facilitator, a promoter of the general welfare, a catalyst, and a

model user.

Based on information generated from the public meetings, the private sector is addressing many of the security needs of the NII. NII security, like other aspects of the NII, will be developed, built, and used by the private sector. Products and services that can be used to secure information on the NII will be designed and provided by the private sector in response to market demands. This section of the security report proposes the role of the Federal government in supporting a secure NII.

The Federal government will undertake four main activities for improving NII Security. The first three involve the government's responsibilities to ensure the sound development and use of the NII. The fourth is the government's responsibility as a user of the NII.

First, the Federal government will serve as a facilitator and a catalyst for promoting private sector activity.

Second, in its role as guardian of the public interest and general welfare, the Federal government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules for security in the NII.

Third, the Federal government can support the private sector's development of needed technology by funding research and development in critical areas.

Fourth, as a model user of the NII, the Federal government has a responsibility to ensure that its own automated information is secure.

A. As facilitator and catalyst for private sector activity, the Federal government will (1) adopt the NII Security Tenets and the OECD Security Principles for use on the NII; (2) stimulate dialogue and awareness about security risks, needs, and solutions; (3) make Federal security products and techniques available for use in the NII; and (4) promote private sector development of high quality security products and services.

1. Adopt the NII Security Tenets and the OECD Security Principles for use on the NII.

Sound security must be based on a common understanding of what is entailed. The NII Security Tenets previously proposed and the internationally-recognized OECD Security Principles [Appendix A] form a solid foundation for developing security products, services, and practices on the NII and internationally.

Furthermore, security is needed to protect privacy and intellectual property rights. Principles on privacy and on intellectual property rights have been released by both the U.S. Advisory Council on the NII and by the Information Infrastructure Task Force.

Proposed Action 1: Promulgate the Tenets and Principles in the final version of this report by September, 1995.

2. Stimulate dialogue and awareness of security risks, needs, and solutions.

The series of public meetings co-sponsored by the Security Issues Forum and members of the NII Advisory Council is the beginning of an on-going dialogue concerning NII security. This report is designed to further that dialogue.

As the NII interconnects U.S. participants into a global information infrastructure, it introduces new threats to U.S. systems and information. Some of these threats (e.g., sophisticated "crackers" in a foreign country) may be difficult for individual participants to fully perceive. In the course of its international relations, the Federal government may learn about the prevalence and magnitude of this type of threat. This information should be shared with participants in the NII.

During the public meetings, there was considerable discussion about assuring appropriate behavior on the part of participants in the NII. One part of that discussion pointed out that many of those who break into others' systems believe such behavior is acceptable. To begin countering this incorrect perception, it was suggested that the Federal government should promote inclusion of ethical computing in educational courses.

Proposed Action 1: Develop data on threat and risk assessment for the NII and appropriately make it available to the public. Promote awareness of the existence of different threats to the NII with an understanding that there is no "one size fits all" solution, and that different threats must be treated differently. Ongoing.

Proposed Action 2: Stimulate dialogue and broad awareness of the national and economic security concerns related to the NII through public meetings and other outreach methods. Ongoing.

Proposed Action 3: Promote educational programs (along with the private sector and state, local, and tribal governments) to teach ethical behavior and awareness of security issues and risks on the NII. March 1996.

Proposed Action 4: Address the issue of minors gaining access to

adult materials on NII. September, 1995.

3. Make Federal security products and techniques available for use in the NII.

This report recognizes that strong, effective security is important to users of the NII in protecting their information. In the past, when private sector products were not available, the Federal government has developed security products for its own use that other NII users have found useful. The Data Encryption Standard (DES) (Federal Information Processing Standard Publication 46), originally developed for government use, has become a worldwide standard for protecting financial information on the world's banking system. Similarly, the Digital Signature Standard (Federal Information Processing Standard Publication 186), provides a strong, efficient, and economical means of assuring the integrity of electronic documents and the authenticity of the sender. The extent to which government-developed technologies will be adopted by the private sector is dependent on a variety of factors. The government does not intend to mandate security products for private sector use, but instead to depend on the marketplace to select those products that best meet the needs of the various NII participants.

Proposed Action 1: *Compile a list of security technologies developed for or used by the Federal government, evaluate them for appropriate and applicable use in the private sector, and make them generally available to the public. Ongoing.*

4. Promote private sector development of high quality security products and services.

NII users are demanding high quality security products and services. Flexible and responsive standards and accreditation processes can assist in the development of those products.

Some security products may provide confidentiality of information that is so strong that it can frustrate law enforcement's authorized ability to listen to communications where criminal activity is suspected. As Vice President Gore has written:

"The Administration has committed itself to cooperating with industry representatives and privacy advocates towards the goal of developing a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address national security needs as well. Such a system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be

exportable. . . .

We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrow services for their own products. Having a number of escrow agents would give individuals and businesses more choices and flexibility in meeting their needs for secure communications." (Letter to Representative Maria Cantwell and others, July 20, 1994)

In addition, the Federal government has for years regulated the export of products based on critical technologies for national security reasons. Although the U.S. has relaxed many of its export controls for advanced computing and communications technologies, certain encryption technologies remain restricted. Nevertheless, the U.S. has committed to allowing the overseas use of encryption for personal use by Americans.

Proposed Action 1: Promote the development of private certification processes through private, nationally and internationally recognized entities such as the American National Standards Institute, the International Standards Organization, nationally recognized testing laboratories, Underwriter's Laboratories, and other private sector communities of interest, such as the health, entertainment, and financial sectors. June, 1996.

Proposed Action 2: Continue to work with industry to develop alternative key escrow technologies, to make available standards and technology for public use, to develop methods for providing compatibility among different key escrow technologies, and to consider ways to promote use of such technologies overseas. December, 1995.

Proposed Action 3: Work with industry and the private sector to foster development of a public key infrastructure. December, 1995.

Proposed Action 4: Encourage the private sector to develop technology vulnerability and risk management guidance in accordance with the requirements for their communities. December, 1995.

Proposed Action 5: Review technology policy for the NII to ensure support for cooperative Federal-industry approaches in the development of security technology. January, 1996.

Proposed Action 6: Issue a proposed rule to establish a personal use exemption for overseas use of encryption. July, 1995.

B. In its role as protector of the public interest, the government will: (1) assure adequate emergency response capability on the NII; (2) adapt current oversight processes to meet the challenges of the NII; (3) review criminal law; and (4) promote international cooperation.

1. Assure adequate emergency response capability on the NII.

Today the Federal government sets priorities and procedures for service on the public switched network in the event of an emergency in order to meet critical communication needs and to assist in an orderly recovery. This role should be extended to establishment of priorities and procedures to support a robust emergency response capability comparable to that provided by CERT, the Computer Emergency Response Team. An extension of this role to assure that priority communications in the NII when emergencies occur will be necessary.

Proposed Action 1: Review emergency communications and network services requirements and priorities, to include the Telecommunications Service Priority program, to assure that appropriate priorities for the NII are established in times of emergency. September, 1995.

Proposed Action 2: Cooperate with private sector and State, local, and Tribal governments to ensure that vital government and civil infrastructure security needs are being addressed. January, 1995.

2. Adapt current oversight processes to meet the challenges of the NII.

The government does not regulate the NII as a whole, although it does regulate different pieces, including providers such as common carriers and users such as financial institutions. As discussed above, virtually every sector of the economy, from health care to aviation, is growing to depend on the NII. Security failures in the supporting information infrastructure could jeopardize the U.S. economic well-being, national security, and public safety. Thus the current oversight processes must be adapted to meet the challenges of the NII.

Proposed Action 1: Examine whether current banking regulations are adequate in the areas of electronic banking, electronic payment systems, and "digital cash," in order, for example, to protect consumers from counterfeiting and fraud. November, 1995.

Proposed Action 2: Ensure that all Federal agencies evaluate their current oversight mechanisms and practices in light of the growing need to address the growing dependence on the NII.

December, 1995.

3. Review Criminal Law.

A review of current law is timely, particularly in the areas of intellectual property rights and computer crime. The Federal government has such reviews underway and will propose its views for public discussion in mid-1995. For example, the Intellectual Property Rights Working Group has proposed that selling software designed to defeat copy protection of copyrighted materials be deemed contributory infringement under the Copyright Act. The Federal government will continue to work with private sector and State, local, and Tribal governments to ensure that proposed changes in criminal law are appropriate.

Proposed Action 1: *Propose legislation to enable prosecution of computer-related crime. June, 1995.*

4. Promote International Cooperation.

In recognition of the increasingly global nature of the information infrastructure, the U.S. has been active in putting computer and communications security issues on the table in international fora. At the G-7 Ministerial Conference on the Information Society in Brussels in February 1995, the U.S. proposed, and the G-7 partners agreed, to increase efforts to find creative, technological and policy solutions to increase "the reliability and security of national and international networks by developing security principles that are commensurate with the risk and magnitude of harm." The OECD has been a leading international organization in the area of information and communications security.

Proposed Action 1: *Stimulate consideration of security issues at the OECD and other international fora. Ongoing.*

C. The government will promote research and development in critical and high-risk areas.

Although the private sector will continue to respond to market pressures and opportunities to create technical security products, services, and techniques, there may be a need for government to encourage private sector research and development in high risk or critical technologies. Some technologies developed by the government which are suitable for adaption for industry applications sector may become available through technology transfer programs. In other situations, government supports the private sector through funding pre-commercial, pre-competitive technology through various grant programs,

cooperative research and development agreements (CRADAs), and other technology development programs. For example, the Advanced Research Projects Agency (ARPA) and the NIST Advanced Technology Program are currently funding research into advanced technology that could be used to support an automated copy management system.

Proposed Action 1: Promote research and development through the High Performance Computing and Communications Program, ARPA, NIST, and others, of security technology that supports agencies' missions. Ongoing.

D. As a user, the government has a responsibility to protect the information in its possession and to act as a model user. Thus, it has the obligation to support all elements of a secure NII as it procures and manages its own portion of the NII. The Federal government will: (1) protect its own security requirements through good management processes; (2) improve its national security/emergency preparedness capabilities; (3) ensure that the products and services it uses meet its needs; and (4) develop a security infrastructure for its own use.

1. Protect its own information through good management practices.

The Computer Security Act of 1987 provides the framework within which Federal agencies will manage the security of the vast majority of their use of the NII. Through that mechanism, they will work to assure the confidentiality, integrity, and availability of their information as they use the NII. In March, the Office of Management and Budget (OMB) issued a draft revision to OMB Circular A-130, Appendix III, "Security of Federal Automated Information" to re-orient Federal implementation of the Act. The proposal will guide agencies in securing information as they increasingly rely on the open and interconnected NII. It stresses management controls such as individual accountability and awareness and training, rather than technical controls.

Similarly, the military will use and be dependent on the security and reliability of the NII. This may require using technologies especially designed for government use, such as advanced firewalls and encryption devices.

Proposed Action 1: Release final guidance to agencies to assure adequate security of Federal automated information through education, training, and awareness programs across agencies. September, 1995.

Proposed Action 2: Continue development of security technologies

to support unique government requirements. Ongoing.

Proposed Action 3: Develop and implement a program to ensure the security of Federal automated information consistent with guidance. January, 1996.

2. Improve its national security/emergency preparedness capabilities.

The National Communications System is a government entity that seeks to effect coordination among Federal government agencies and between the government and the telecommunications industry in order to support the government's emergency response mission. Through its efforts to promote the sharing of information between the private sector and government, the NCS promotes greater cooperation in securing networks for both the civil and private sectors.

Proposed Action 1: Review and validate national security and emergency preparedness (NS/EP) requirements for the nation's information infrastructure. December, 1995.

3. Ensure that the products and services it uses meet its needs.

The Federal government will adopt voluntary, consensus based standards wherever practicable. Where an appropriate standard developed in the private sector is not available, government will develop a standard for its own use. These standards will be available for other parties to use on voluntary basis. These standards are developed and promulgated by the National Institute of Standards and Technology (NIST) of the Department of Commerce.

The Federal government has traditionally accredited many of its standards through government laboratories. Increasingly, however, private sector evaluations are encouraged, as in "Security Requirements for Cryptographic Modules" (Federal Information Processing Standards Publication 140-1). The government also publicly issues lists of commercial products that it has accredited for its use.

Proposed Action 1: Rely, where possible, on security products which are based on industry standards. However, where commercial security services and standards are insufficient for government's needs in the NII, the government should develop security standards and use products built to those standards. Ongoing.

4. Develop a security infrastructure for its own use.

Under the auspices of the NII Security Issues Forum, the General Services Administration has established a Security Infrastructure Program Management Office. This office is coordinating the development of a public key infrastructure to meet the Federal government's needs for digital signature and confidentiality purposes. The U.S. Postal Service is pursuing complementary efforts.

Proposed Action 1: *Develop a public key infrastructure for government use. Demonstrate interoperability with multiple agencies and with industry. June, 1996.*

V. CONCLUSION

Users of the NII require reasonable confidence about the confidentiality, integrity, reliability, and availability of their communications. While the Federal government has a role in supporting a secure NII by facilitating private sector activity, ensuring public safety by protecting against abuses that result in harm to others, and supporting research and development in critical areas, much of the responsibility lies with the private sector. It is neither appropriate nor realistic to expect the Federal government to provide the security solution for the NII. Not only is the NII too complex for a one-size-fits-all solution, but without demand from users, the market in appropriate security tools and services will not succeed.

Ultimately, users must realize that no system is completely free of risk. Users of the NII must make informed choices about an acceptable level of risk for a particular transaction. While laws, policies, and technology can contribute to a secure NII, awareness of risk is the foundation upon which a secure NII will stand.

NII SECURITY: THE FEDERAL ROLE

June 5, 1995

I. INTRODUCTION

The National Information Infrastructure (NII) is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits.

Security is critical to the development and operation of a viable NII. In fact, one of the goals stated in "The National Information Infrastructure: Agenda for Action," is to ensure information security and network reliability. Without the confidence that information will go where and when it is supposed to go, and nowhere else, the NII will not be used to support health, education, commerce, public services, and advanced communications to the fullest extent. In the NII, security¹ means:

- . integrity -- assuring that information will not be accidentally or maliciously altered or destroyed;
- . reliability -- assuring that systems will perform consistently and at an acceptable level of quality; and
- . availability -- assuring that information and communications services will be ready for use when expected.
- . confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons;

To articulate and implement the Administration's vision for the NII, the Vice President formed the Information Infrastructure

¹ The discussion of security in this report encompasses a number of substantive issues which are tangential to security, such as protecting intellectual property rights. The report does not attempt to set the underlying norms for these areas, but rather discusses protection of such information.

Task Force (IITF). The IITF is chaired by Secretary of Commerce Ron Brown and is comprised of senior Administration officials having expertise in technical, legal, and policy areas pertinent to the NII. The NII Security Issues Forum was established within the IITF to address the important cross-cutting issue of security in the NII. The Forum is chaired by Sally Katzen, the Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget, and includes representatives from each of the IITF's committees as well as representatives from each Executive branch organization with significant information security responsibilities.

In addition to the IITF, the President has established the U.S. Advisory Council on the National Information Infrastructure. The Advisory Council includes representatives from industry, labor, State and local governments, and public interest groups, and advises the Secretary of Commerce on issues relating to the NII. Mega-Project III, one of three work groups of the Advisory Council, is addressing security, intellectual property, and privacy issues as they relate to the NII.

To better understand what will be needed to make the NII adequately secure, the NII Security Issues Forum and members of the U.S. Advisory Council on the NII held seven public meetings to discuss the security needs of likely users of the NII. Based on the first several meetings, the Forum proposed a set of five security tenets (set forth below) for public comment, which characterize in layman's terms the security needs of users of the NII.²

The purpose of this report is to expand on those tenets and begin to articulate security expectations for the NII in order to develop a broad consensus of the appropriate Federal role. Specifically, this report:

- . Summarizes the Forum's findings concerning security needs in the NII;
- . Presents an analysis of the institutional, legal, and technical issues surrounding security of the NII; and
- . Proposes Federal actions to address these issues.

PUBLIC PARTICIPATION

² Although Mega-Project III co-sponsored the public meetings, this draft report is the product of the NII Security Issues Forum, a Federal organization. The Forum looks forward to receiving advice about this report from Mega-Project III through the NII Advisory Council.

Over the past year, the Forum, in cooperation with Mega-Project III of the U.S. Advisory Council on the National Information Infrastructure, conducted seven public meetings between government officials and members of the private and public interest sectors.

A general meeting was held on July 15, 1994, at which individuals representing business, manufacturing, banking, health, entertainment, publishing, education, libraries, and government services discussed their views of security needs in the NII. Subsequent meetings addressed the needs of various sectors using the NII. The subjects of the meetings were:

- (1) "Commercial Security on the NII," which focused on the need for intellectual property rights protection in the entertainment, software, and computer industries;
- (2) "Security of Insurance and Financial Information";
- (3) "Security of Health and Education Information";
- (4) "Security of the Electronic Delivery of Government Services and Information";
- (5) "Security for Intelligent Transportation Systems and Trade Information"; and
- (6) "The NII: Will It Be There When You Need It?" addressing the availability and reliability of the Internet, the public switched network, and cable, wireless, and satellite communications services.

In order to continue and expand this public dialogue, this draft report, "NII Security: The Federal Role," is being issued for public comment. In addition to receiving comments, the Forum will sponsor two public meetings this Summer to discuss the Report.

This report includes a set of proposed government action items in section IV. This is intended to articulate the areas in which the government will act to improve the security of the NII. The next step is to receive and respond to public comment on the report in order to develop consensus regarding the Federal role and its proposed actions.

II. FINDINGS

Based on the initial dialogue, the Forum is proposing three actions: (1) adoption of proposed NII Security Tenets, (2)

adoption of Organization of Economic Cooperation and Development (OECD) Security Principles for use on the NII, and (3) implementation of the Federal role described at the end of this report.

A. SECURITY TENETS

On February 10, 1995 [see Vol. 60 No. 28 of the Federal Register, p. 8100], the IITF proposed five security tenets for public comment, based on the general proposition that people who use the NII want to know that their information goes where and when they want it to and nowhere else. The tenets are comprised of five common propositions that emerged from the early public meetings about what NII participants expect. Clearly, the details of implementation of the tenets will vary by user -- whether teachers, doctors, or tax preparers -- and by application -- whether communicating over a two-way multi-media conference, sharing data between doctors and patients, or calculating a tax return. Participants expect:

- 1) The ability to control who sees (or cannot see) their information and under what terms.
- 2) The ability to know who they are communicating with.
- 3) The ability to know that information stored or transmitted is unaltered.
- 4) The ability to know when information and communication services will (or will not be) available.
- 5) The ability to block unwanted information or intrusions.

Two conditions attach to these security tenets:

- 1) None of these tenets is absolute. For each tenet there may be valid societal reasons -- such as an emergency or a need to protect another's rights -- that cause the tenet to be conditioned in some manner.
- 2) Each tenet requires NII participants to take responsibility for establishing the terms and conditions under which they will exchange information. The distributed and empowering nature of this technology demands a greater level of personal responsibility from participants than when communications systems were more limited in scope and scale. Education of NII participants is thus a critical task.

B. OECD PRINCIPLES

The U.S. is not alone in addressing security concerns in the evolving global information infrastructure. The organization for Economic Cooperation and Development (OECD) has adopted Security Guidelines. The U.S. and 23 other member nations of the OECD have endorsed these Guidelines. The Guidelines encompass nine Security Principles, which articulate high-level needs, such as the need for explicit accountability for security, the need for awareness of security practices and procedures, and the need to respect the rights and legitimate interests of other users. These Principles are included as Appendix A. The IITF proposes to adopt those Principles for use in the NII.

The OECD Principles are being incorporated into two National Institute of Standards and Technology (NIST) publications, "An Introduction to Computer Security: The NIST Handbook," and "Federal Computer Security Principles and Practices" (working title). These two publications complement each other -- the Principles and Practices publication will provide a quick reference to accepted security practices. The Handbook explains the Principles and Practices and provides a bibliography and extended examples.

C. PROVIDER AND USER SECURITY CONCERNS

The public meetings solicited discussion with a broad range of NII participants, both users and providers of NII services. Regardless of the commercial, industrial, or public interest use represented, the participants shared a number of concerns. These concerns included: the potential inability to control secondary uses of information; questions of liability for loss or inappropriate access to or use of information; a mistrust of government's use of information; the desire to protect one's own system from outsiders, whether by hostile attacks or junk mail; and risk of system failure at times of critical need. The most-heard concern was that personal information, such as information pertaining to an individual's finances, health, or purchasing habits, could be disclosed to or manipulated by an unauthorized user. These shared concerns were generalized in developing the security tenets described above.

In addition, some participants seemed to desire a greater government role, such as censorship of defamatory or pornographic information transmitted over the NII, or additional funding for national security and emergency preparedness programs. Other participants seemed to desire a lesser government role. For example, some participants desired open access to and use of virtually all information and systems without interference. Other participants criticized the Federal government's export control policy, which limits the export of powerful cryptographic systems.

Still others were suspicious of the technology underlying the NII and how it would be used. Some witnesses were also concerned that government's involvement could create greater inefficiencies, increase susceptibility to invasions of privacy and risk of fraud, and contribute to the depersonalization of society.

The following summarize the concerns and needs heard at each of the public meetings. Transcripts are available on the NII bulletin board at the Department of Commerce. (For Internet access, gopher, telnet, or anonymous ftp to iitf.doc.gov. Access is also available over the World-Wide Web. Dial-up access by modem is available at (202) 501-1920. Set parameters at no parity, 8 data bits, and one stop. Speeds of up to 14,400 baud are supported.)

1. Entertainment, Software, and Computer Services

Images, movies, music, software, and a variety of products that can be transmitted in digital form can be easily altered or copied. The protection of intellectual property rights in an electronic age requires technology, legal protection, and institutions that promote fair use, support licensing and payment, and prevent unauthorized copying, alteration, or distribution. There was considerable discussion about effective legal protection and institutions. A thorough treatment of intellectual property on the NII will be found in the IITF White Paper.³

A number of possible technological approaches were described at the meeting, including software that is programmed to be disabled after a span of time if the software is not paid for. Another technique described was to distribute an encrypted movie with a key that can decrypt it (for viewing) one time only. One intellectual property entrepreneur electronically distributed his work -- visual images -- in encrypted form and then sold the decryption key through the regular mail. This solution allowed him to distribute digital images electronically, but it did not prevent the buyer from redistributing the work after they decrypted it. Generally, participants indicated that adequate technical capability was being developed to protect their own products. Technical challenges remain, however, including the need for an automated copyright management system for digital works. In addition, several witnesses raised a concern about government barriers to the development and sale of technologies such as export control laws.

³ The report is expected to be issued in June, 1995. For a copy of the report, contact the U.S. Patent and Trademark Office, Washington, D.C. 20231, or call (703) 305-9300.

2. Health and Education Information and Services

Health care will be improved by computer-based patient records, on-line databases, consumer health information, and remote treatment and advice. However, improved access to information also brings with it a risk of improper disclosure, alteration, or use of highly personal information. Patients' well-being will become dependent on the integrity and reliability of such information in the NII. In particular, the reliability of such computerized medical records systems will be of critical importance as the health care system shifts away from paper. Similarly, educational records can have a substantial effect on individuals' economic well-being.

Participants suggested that the technology will need to promote information integrity, and to ensure that access is provided on a need to know basis, that records that serve different functions are separated, and that the records are destroyed when they no longer serve their function. Concern was also raised about the availability of pornographic material on the Internet and the need to protect children from exposure to it.

3. Financial, Insurance, and Commercial Services

The financial and insurance sectors have relied for decades on closed networks in order to reliably transfer funds and share information. As their networks become more open, new security tools and techniques will be needed to protect the confidentiality and integrity of valuable commercial information. Questions of liability will also arise if improper disclosure of customer information occurs while it is being transmitted over the public switched network.

As consumers use the NII to conduct business, they will want to verify that a payment or order was received correctly. Without a face-to-face transaction to verify the authenticity of the customer and of the vendor, the potential for fraud increases for both parties, requiring methods of electronic notarization, digital signatures, and date-stamping.

The advent of so-called digital cash involves a different challenge. It requires a technical method to avoid forgery and authenticate the current owner. On the other hand, some witnesses favored the ability to anonymously execute transactions. A number of products are already being tested to provide "electronic cash" on the NII.

One witness pointed out that the vast majority of technical solutions address the issue of protecting an organization's data

from individuals, while little attention has been paid to the problem of how the individual's data can be protected from organizations. This situation is illustrated by the way in which data about an individual's purchasing habits is bought and sold in private markets. Other personal information which is generally publicly available, such as marital status, home ownership, and status in legal proceedings, is collected by the private sector and sold as a commodity. Some individuals expressed a desire to exercise greater control over the use of this information, or to be reimbursed for its use. The IITF's Privacy Working Group is developing principles to guide policy development in this area.⁴

4. Intelligent Transportation

Intelligent transportation systems include applications such as electronic toll collection, in which a toll payment is automatically deducted from a card with a computer chip so that cars won't have to stop as they pass through toll booths. Such systems may also help monitor traffic patterns and road conditions through cameras or other sensors, and provide drivers with information in their cars about the quickest route.

A basic security concern with electronic toll collection is funds control and integrity. In addition, there are concerns that the information collected in these transactions, including information about the owner of the vehicle, how fast he or she was driving, and where he or she was headed, could be used inappropriately. Access to this information could disclose commercial proprietary information or compromise personal privacy. Furthermore, as transportation becomes more dependent on automated control systems, the movement of people becomes subject to security risks. For example, a security breach could allow mischief such as switching all the traffic lights to green, thus promoting accidents.

5. Government Information and Services

Use of the NII is becoming integral to virtually every Federal program, and Federal agencies are becoming dependent upon that use for execution of their missions. The NII will support programs as varied as air traffic control, compilation of the decennial census, response to natural disasters, and delivery of social security benefits.

⁴ "National Information Infrastructure; Draft Principles for Providing and Using Personal Information and Commentary;" January 20, 1995; 60 FR 4362.

This use of the NII in Federal operations promises improved efficiency of governmental program delivery. However, it also introduces new and varied security vulnerabilities, not unlike those faced by other users of the NII. The difference, of course, is that addressing these security vulnerabilities is a direct responsibility of the Federal government, since such vulnerabilities could degrade Federal program effectiveness and resource safeguards, and affect the integrity, confidentiality, and/or availability of government information.

At the meeting, the use of "smart cards" or electronic debit cards for delivering food stamps was discussed in depth. Smart cards provide the advantage of on-time payment, increased dignity, and improved efficiency in program administration. However, cards can be lost, and there are opportunities for fraud by converting the credits to cash. Other concerns include the potential for counterfeiting such cards or otherwise manipulating the value of the cards. Unauthorized access to individual purchasing records could violate personal privacy. Users of these cards need confidence that the benefits will be available when they expect them to be, and that associated information will not be abused by those with access to it.

6. The Public Switched Network and the Internet

As new technologies are integrated into the public network, new vulnerabilities are introduced. Some technologies are more vulnerable than others. For example, wireless communications are particularly vulnerable to eavesdropping, while cable and satellite television providers face an ongoing battle to protect the commercial information they are sending to consumers.

As individuals and organizations become more reliant on the NII to conduct personal and business transactions, the availability and reliability of the network is of greater importance. These concerns vary from the risk of major network outages to the minor irritant of slow or noisy network connections. Users need assurances that the NII will be there when they need it. If it isn't, they want meaningful recourse. For certain transactions, users also desire an assurance that information was received by the intended recipient, analogous to "certified mail."

Users will depend not just on the availability and reliability of the information itself and of the system on which it resides, but indirectly on the availability and reliability of the network which transports the information between systems. From the perspective of the providers of network services, security threats include natural disasters such as fires, floods, or hurricanes; physical attacks, such as bombs; electronic attacks, such as computer viruses; and unintentional errors, such

as design flaws, software bugs, and human error. Network services providers are addressing these threats as an integral part of their business. During the public meetings, some participants were open to appropriate Federal involvement in this area, while others were more cautious about the Federal role in this area.

Other concerns include the risk that hackers may intentionally compromise the security of personal or organizational computer systems, or maliciously gain access to information while it is moving from place to place within the NII. These fears are grounded in well-publicized incidents on the Internet and public switched network, but actually comprise only a small fraction of computer security incidents. The majority of incidents are caused by authorized individuals doing unauthorized activities. There was some discussion of the need to share information among providers concerning the outside threats to networks, as well. Other security concerns included the need to verify whether information was altered accidentally and the need to ensure availability of networks in the event of natural disasters.

III. ANALYSIS

The NII security needs expressed above can be organized into three areas: (1) coordinating functions, (2) oversight and enforcement for public safety, and (3) technical security needs. The three areas are interrelated. For example, for Federal computer crime law to be enforceable against a system trespasser, security measures must have been in place and a record made of the trespass. Similarly, civil liability standards of due care require that effective technical security be in place. At the same time, overall security is enhanced if there are criminal or civil legal sanctions which act as deterrents.

The following section addresses the functions necessary to support a secure NII, as heard in the public meetings. The section on oversight and enforcement for public safety addresses how existing oversight organizations need to adapt to the oversight of NII related activities, as well as whether current laws are sufficient and enforceable in the context of the NII. The discussion on technical security addresses the technical ability to protect information and systems in the NII.

A. COORDINATING FUNCTIONS

The National Research Council's (NRC) report, "Realizing the Information Future," notes that while security needs can be addressed to some extent by technological methods and a legal framework, structures must be in place to make them work. This

section is intended in part to contribute to the dialogue about and development of such an architecture, by describing the coordinating functions which emerged based on public discussions of security of the NII. Some of these functions will be fulfilled by the private sector, some by government, and others in partnership.

If the NII is to succeed, a structure or a collection of structures -- a security architecture -- must exist to ensure security. The NRC report states: "This security architecture must include technical facilities, recommended operational procedures, and means for recourse within the legal system." This architecture will be based on a variety of public and private institutions and policies. Although an architecture will define how institutions, policies, and technologies interconnect, a sound security architecture will consist not of rigidly prescribed technologies or solutions, but must be able to flexibly adapt to change. The report also notes that such an architecture will require research and development over time.

1. National and Economic Security

As the United States as a whole becomes increasingly reliant on the NII for communications and information, other key components of the U.S. infrastructure will become dependent on it. For example, the power grid, transportation systems, financial institutions, and economic transaction data will all be dependent on the NII. Security weaknesses in the NII can place those infrastructure elements at risk. Hence a significant attack on the NII would be a threat to our national security in addition to the significant personal and economic harm it would cause.

From the Federal government's perspective, public safety and the national defense call for a secure NII. All Federal entities that oversee various parts of the U.S. economic infrastructure must be aware of the changing risk that increasing reliance on the NII entails. They also must be aware of the various types of threats to the NII and their magnitude.

2. Ethics and Education

There was a general concern at the public meetings about the lack of regard that many participants in today's Internet had for others' intellectual property and privacy. This was often characterized as youth in its search for knowledge and disdain for bounds of ownership of electronic information. Several presenters noted that often young persons have tremendous technological savvy, but little understanding of the ethical responsibilities that such knowledge entails.

Witnesses at the public meetings specifically suggested a need for training and awareness in the general area of computer ethics. The basic principle should be a respect for others' rights on the NII. Whether in the office, university, elementary school, or at home -- where today's children are learning to use computers -- parents, teachers and supervisors should emphasize that it is not only wrong, but illegal, to copy copyrighted software or other materials or to break into someone else's file or computer system. It was noted that the Education Department, in cooperation with the Intellectual Property Rights Working Group of the IITF, has begun to develop a model curriculum on the importance of protecting intellectual property. Participants at several meetings described the need for ongoing dialogue on this subject among all users.

A final issue where more dialogue is needed is the protection of children from exposure to inappropriate materials on the NII. As President Clinton has stated:

"I believe that insofar as governments have the legal right to regulate obscenity that has not been classified as speech under the First Amendment, and insofar as the American public widely supports, for example, limiting access of children to pornographic magazines, I think it is folly to think that we should sit idly by when a child who is a computer whiz may be exposed to things on that computer, which in some ways are more powerful, more raw and more inappropriate than those things from which we protect them when they walk into a 7-Eleven." ⁵

3. Emergency Preparedness and Response

Three types of emergency preparedness and response roles were described during various meetings: (a) the need for an entity analogous to the Computer Emergency Response Team (CERT), which currently acts as an Internet "911," (b) a system for planning and recovery during and after an emergency which sets, among other things, a priority of restoration, and (c) a need to exchange information concerning mutual vulnerabilities.

(a) Emergency response. As the Internet is evolving from a research and development experiment to a widely used public communications medium, the need for an emergency response entity to coordinate the community's response to security threats has become apparent. In the Internet the entity that currently performs that function is the Computer Emergency Response Team (CERT). It is likely that function will need to continue in the

⁵ Remarks to the American Society of Newspaper Editors, Dallas, Texas, April 7, 1995.

NII.

(b) Emergency planning and recovery. In order to maintain a state of readiness or respond to and manage an emergency or crisis, an emergency preparedness capability is required. The government has established the National Communications System (NCS) to ensure the availability of communications services required to support emergency planning and response functions. The NCS's National Coordinating Center for Telecommunications is staffed full-time by both government and telecommunications industry representatives, whose mission is to respond to both military and civil emergencies, e.g., Operations Desert Shield/Desert Storm, Hurricane Andrew, the Northridge earthquake, and more recently, the bombing of the Federal building in Oklahoma City. A similar function is likely to be needed to ensure the availability of NII services to support emergency planning and response functions.

All users have an interest in having service restored in the event of an emergency or disaster such as an earthquake or flood. In the public switched network, telephone service is restored based upon governmentally established priorities, with the highest priority given to organizations whose function it is to respond to such emergencies, such as the Federal Emergency Management Agency (FEMA). As users rely more on the NII for critical functions, a similar need for setting priorities for restoration on a broader level will arise.

(c) Exchanging information concerning vulnerabilities. Participants at several meetings discussed the need to exchange information about mutual vulnerabilities in the NII as it evolves. They indicated that improved security resulted from meaningful communications among users and providers. If a problem is identified, it can be quickly solved. In describing this role, some pointed to CERT bulletins as a model. Others pointed to the NCS's program to facilitate appropriate sharing of security vulnerability information. Others described different possible mechanisms, such as industry newsletters and trade publications, engaging in mutual assistance agreements with other parties in the private sector, and on-line news groups.

4. Quality Assurance

Some participants in the public meetings asked how they could be sure that the security products they chose were as good as they claimed to be. Testing by independent third parties such as nationally recognized testing laboratories, organizations that certify that products meet or exceed the requirements of a specific standard, may be useful for those trying to evaluate the effectiveness of security products. Such third party testers may evolve into a system for evaluating security products. A

certification procedure could be useful for both producers and users of security products who may be trying to be more competitive and to protect against the threat of lawsuits. Utilization of the trademark system may also operate to provide assurance of performance. The trademark system may be useful in allowing consumers to develop confidence in a particular trademark that could result in continued purchase of both a particular product and of others bearing the same trademark.

Additionally, an independent entity representing consumers' interests such as a "Better Business Bureau" could provide a place to file complaints and answer questions about various NII service providers. Either government, trade associations, industry groups, or private sector consultants could fulfill this need.

Related to the issue of accreditation is that of standards. Security products and services can be tested as meeting either a performance standard or a technical standard. Standards in the United States are developed primarily by private standards development organizations representing industry, trade, and professional organizations. For example, the American National Standards Institute (ANSI), the Institute for Electrical Engineering and Electronics (IEEE), and others are active in this area. Sometimes a Federal government standard becomes the accepted international standard. Many of these organizations work together through the International Standards Organization (ISO). Internet standards have been developed somewhat more informally and quickly by the Internet Engineering Task Force (IETF).

Alternatively, any group of users can define a set of security standards and agree among themselves to be bound by them. Such "affinity groups" design or decide on standards to meet the specific needs of their members. During the public meetings, participants described unique problems such as the need for a particular database to increase the integrity of information, or to help their industry improve its use of electronic processing and networking. These standards may become de jure standards formally accepted by industry, or they may remain de facto standards. In addition, de facto standards are often set by dominant industry participants. Quality assurance and other security standards must be developed in full recognition of the complex standards-setting environment.

B. OVERSIGHT AND ENFORCEMENT

There is a need for effective law and oversight of both the NII itself and of public safety-related uses of the NII. A sound legal system that applies civil remedies and criminal penalties is essential to fulfilling this need. In the public meetings,

participants focused primarily on civil remedies and litigation, rather than criminal issues. In addition, considerable activity is occurring in State, local, and Tribal governments, particularly regarding criminal computer law.

1. Law and Regulation

Various activities are overseen by government because they affect the well-being of the nation. For example, some sectors of the economy are regulated to ensure the public health or safety. As these activities become increasingly reliant upon the NII for communications and information, a security weakness in the NII can become a threat to the public health or safety. To effectively manage risk in their public safety oversight role, Federal agencies will need to ensure the secure use of the NII by their overseen sector. Thus, for example, the Transportation Department may need to adjust its regulatory oversight of aircraft to account for the risks involved in aircraft's use of the NII. Similarly, the Securities and Exchange Commission may need to adapt its oversight of securities exchanges, and the Treasury Department and the Federal Reserve Board their oversight of the nation's banking system.

2. Civil Law

Civil litigation includes specialized or statutory suits, contract actions, tort actions, and injunctive relief. Several participants in the meetings stated that issues of liability must be resolved before widespread use of the NII occurs. In reality, however, a range of accepted solutions and practices concerning information security will be decided in increments through the court system as a body of case law develops over time.

Civil law addresses the issue of liability. In every public meeting, users and providers of NII services questioned how the current system of liability for damages would affect their use. For instance, concerns were raised that unknown exposure to liability could prevent potential providers from offering services.

Specialized suits can be used to protect intellectual property rights against copyright, patent and trademark infringement, or other violations of established statutory rights. Whether a particular statute extends to activities on the NII when Congress did not specify the statute's application in a networked environment may be subject to litigation on a case-by-case basis.

Contract actions are law suits contesting provisions in express or implied contracts. Tort actions resolve disputes for

money damages alleging a breach of a duty which caused harm to the plaintiff. Injunctions involve obtaining a court order to prevent specific actions or require certain activities. For example, such an order might prohibit use of the Internet in a certain way or require a user to make certain disclosures before using the Internet. Other forms of civil action and novel theories of liability involving all aspects of the NII continue to evolve.

Civil liability is likely to create incentives for improving security of information systems.⁶ If users, system managers, and service providers face liability in contract for failure to perform a contractual duty, or liability in tort for negligence, they will have an incentive to take reasonable steps to secure their systems, ensure accuracy of their data, and limit unauthorized access and use. A presenter at one public meeting noted that some private parties currently protect their proprietary information by simply not putting it on networks. Attaching legal consequences for the unauthorized or improper use of electronic data will increase the likelihood that the NII will be a trustworthy, reliable system.

Courts are beginning to be confronted with cases that test the effects that civil liability practices will have on the security of the NII. Until a settled body of law develops, various parties' responsibilities and potential liability for negligent security will be uncertain. Legislation that would impose criminal and/or civil penalties for security violations such as blocking, tampering, masquerading, or denying service in the network environment is, of course, possible. However, consensus about what constitute reasonable standards for information security will be difficult to achieve. Because security requirements greatly vary in different contexts, such as finance, law enforcement, medicine, national security, research, and education, there may be a need for context-specific standards that can evolve as requirements change.

3. Criminal Law

Traditionally, laws have focused explicitly on the computer, since it could be easily recognized as the venue where a crime occurred. The laws were intended to protect the information

⁶ Lost or scrambled files, system downtime, invasion of privacy, and economic or physical injury can be foreseen as a result of sloppy security of networks. For example, liability for system managers can be envisioned for failure to enforce password expiration, eliminate access by former employees, replace default configurations, or implement technical solutions to prevent or reduce breaches in security.

contained in computers. Technology, however, has evolved so that proscribing conduct with regard to computers does not adequately protect information. Today, information can be intercepted and modified in transit between computers, or when it is present in devices not typically thought of as computers, such as telephones, cable systems, satellite and cellular channels, etc.

Many actions that would compromise security of the NII are already criminal violations. For example, it is illegal to conduct a wiretap without a court order. Fraud, whether perpetrated electronically or not, is a criminal offense. In other areas, laws may need to be amended.

Legislative efforts to protect computers and information suffer, on the one hand, from having to exhaustively yet clearly define these terms in order to make the laws meaningful. On the other hand, the laws must be sufficiently broad and adaptable that the statute will not be rendered obsolete by rapid technological change. For example, current law may not deal well with the problem of intrusive code, also known as a computer virus or worm. That is, it may be difficult to prosecute the distributor of these destructive instructions if that individual never actually "accessed or used" the affected computer.

Although existing laws provide some protection, new laws will be needed to insure that the NII is protected adequately. For example, 18 U.S.C. Sec. 1030(a)(5) should be extended to protect all United States Government and financial institution computers, even if the computer is not used in interstate commerce or communications. Additionally, the statute should specifically apply to computers used in foreign communications, not just interstate communications. These and other changes must be made to ensure that laws keep pace with new technologies.

In order for the NII to be secure, laws must be enforceable. Hence, law enforcement officials such as police officers must maintain the ability to enforce laws effectively in it. Future crimes are likely to be planned and coordinated using the NII. The NII will also be used by criminals to smuggle stolen corporate information, engage in the transmission of child pornography, engage in industrial sabotage, or electronically stalk, terrorize, or threaten other NII users. In all of these cases, law enforcement must be able to protect citizens.

4. International Issues

International computer offenses are easier to commit than traditional international crimes, because they do not necessarily require additional manpower or physical transportation. Someone can ship information covertly via telephone and data networks. They need no passport and pass no checkpoint, but cross borders

simply by typing a command.

Second, computer crime has not received the emphasis given other international crimes. Until relatively recently the United States, probably the most computerized nation, has not mobilized against computer criminals, even though it is the frequent target of such computerized attacks. Although the U.S. now recognizes the seriousness of the threat, it is not surprising that less computerized countries do not yet fully share this awareness.

Many countries have weak or no laws against breaking into computers. Those with strong laws find it difficult to engage in fruitful cooperation with those without. The vulnerability of both modern and modernizing nations has been highlighted by recent events:

- . A Christmas card message sent over BitNet, the international academic computer network, landed in 2,800 machines on five continents including IBM's internal network. It took only two hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.
- . Pirate bulletin boards contain information regarding computer vulnerabilities and are being used to develop and perfect new computer viruses. Such bulletin boards have been found throughout the United States as well as in Bulgaria, Italy, Sweden, and the Soviet Union.
- . In China, computer criminals recently stole \$235,000 from a bank in Chengdu.
- . Recent reports indicate highly prolific virus writers are working in Bulgaria.

In order to improve international cooperation in the prosecution of computer crimes, the United States has joined international efforts to raise public consciousness about computer crime and encourage other countries to enact or strengthen their computer crime laws. In fact, other countries have been working both domestically and internationally in this area, particularly Denmark, England, Australia and Germany.

Consistent with this international effort, the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems require prompt assistance by all parties in cases where information security has been breached. Additionally, the Council of Europe is currently addressing procedural problems that arise in information technology crimes, such as how to quickly get international trap and trace information.

C. TECHNOLOGY

At the heart of information security in the NII is the technical ability for individuals to protect their information and systems. At every security meeting technical approaches in use or being developed to protect systems or information were discussed. These varied from techniques being used by firms to protect their intellectual property rights, to protection being designed into systems of electronic cash, to "firewall" techniques for protecting firms' networks when connected to the Internet. These public discussions indicated that the marketplace, to the extent that users are demanding security, is responding with both specific security products as well as general NII products and services that incorporate security protection.

At the same time, the security technology challenges of the NII are formidable. Information and services will need to be protected, yet also available to communities of interest. Much of the technology that will be used to provide security in future use of the NII is yet to be developed. The discussion in this section that follows summarizes today's technological approaches to security, based on the public meetings. It should not be read as a complete description of the security technology needs of the future NII, nor to minimize the complexity of fulfilling those needs.

Security products and methods are necessary for individuals and organizations to be able to protect their systems and information in the NII. The many products and techniques that exist approach security from one of two principal strategies -- protecting a system from outside attack (e.g., firewalls), or protecting the information itself regardless of where it resides, normally through some form of cryptography. In addition, the networks themselves should be protected.

1. Protecting Systems

Like criminal laws, technical security measures have traditionally focused on controlling access to the system. As today's processing environment becomes more open, however, that task becomes significantly more difficult.

Participants in the public meetings demonstrated an understanding of a wide array of technical security techniques used to protect their systems. Moreover, a consensus view emerged that incentives exist for the marketplace to provide appropriate security techniques. A number of participants expressed surprise that the government was taking an interest in this issue, other than as a user. Most felt that their technical

security needs would be satisfactorily addressed by the private sector.

a. Access Control to Systems

Today, individual access to and accountability on systems is controlled largely by password management. That is, an individual is required to identify some unique piece of information known only to the individual and the system in order to identify himself to the system. Over the years, password schemes have become more complex to make systems more secure, and the ability of those trying to penetrate systems by obtaining passwords has become substantially better. For example, a large number of sophisticated password "sniffers" -- software programs designed to capture passwords as they are sent across hosts -- were recently detected on the Internet.

Stronger schemes for protecting systems include timed password-changing mechanisms. These mechanisms change acceptable passwords at timed intervals previously agreed upon between the system and a device held by individuals desiring to remotely access the network. Other methods are being developed to substitute for password schemes. They identify individuals to a system by the rhythm of their keystrokes or by biometrics such as fingerprints or a retinal scan.

b. Secure Gateways

Participants at the public meetings that use Internet noted that they were using secure gateways or "firewalls" to help protect their systems by limiting outside access to internal system capabilities. It was often noted at the meetings that, despite recent publicity about break-ins and breakdowns, strong technical measures exist that afford protection. Where break-ins have occurred, they normally exploit known weaknesses which have not been fixed, even though fixes are readily available.

A different concern raised by a number of participants at the public meetings is the need to block the reception of unwanted information. This can be a security risk because unwanted messages could overwhelm a receiver's ability to handle them and effectively shut down the receiver's system.

A view that was often presented was that individuals and organizations are responsible for making reasonable efforts to secure their systems, in the same way they have a responsibility to lock their doors to deter burglars from entering. Private sector firms are responding to the need for secure gateways by developing increasingly sophisticated commercial products. However, like seat belts in cars, they only work when they are

used.

c. Protecting Networks

Related to the security of systems is the security of networks. Networks, comprising a variety of technologies, are what connect systems with each other. The most common threats are breakdowns in the availability and reliability of the networks, resulting in slow or noisy connections, network outages, or loss of data. These threats can be caused by natural disasters such as fires, floods, or earthquakes, but also can include a physical attack, such as a bomb, or an electronic attack, such as a virus. Procedural errors such as design errors, software bugs, and operational mistakes can also place a network at risk.

Basic physical security precautions can help, such as fire protection systems and doors with locks. Back-up equipment enables a network provider to quickly restore service, while quality assurance software can minimize design errors, and technical security measures can warn about an impending breakdown or prevent an outage or loss of data.

2. Protecting Information

Protecting information requires different technology than protecting a system. Once information is outside a controlled system, there is little control over who can gain access to it. Therefore technology which can provide assurance that information itself can not be read, copied, or modified is critically important in an open processing environment such as the NII.

a. Cryptography

Cryptographic mechanisms already widely used are unique in that they directly protect information from being compromised or altered without authorization. It is envisioned that use of encryption and digital signatures will continue to grow rapidly. Cryptography is used by banks to assure the integrity of financial transactions, by computer operating systems to conceal passwords, by users of the Internet to protect the privacy and confidentiality of their communications, and by holders of smart cards to protect information contained on the card. There is no doubt that in the future there will be widespread use of this technology, which will be virtually transparent to end-users. Cryptography is also used in other security services, such as digital signatures and passwords.

Some participants noted that many hurdles remain to easy use

of cryptography. For example, one problem is the awkwardness of handling encrypted information. Also, the lack of a public key infrastructure makes it difficult for individuals and organizations to manage keys efficiently and to use public key cryptography. Another factor which has limited cryptography is the risk of unmanaged cryptography for business -- whether it be a disgruntled employee who encrypts corporate financial records before departing, an employee who is absent when critical files are needed, or merely someone who forgets the keys. Finally, the lack of agreement on cryptographic standards is slowing the proliferation of cryptography.

1. Confidentiality

Cryptography is essential to protecting the confidentiality of automated information. It provides the protection of information being undecipherable, even if someone gains access to it. It is this use that crystallizes a conflict between citizens' needs to protect confidential information and the societal need for justice and safety. Strong cryptography can be used to thwart law enforcement's legitimate ability to understand the contents of lawful wiretaps. On the other hand, weak cryptography will not provide effective protection of confidentiality of citizens' sensitive communications.

A number of alternative approaches to resolve this dilemma are being proposed. Many involve a key escrow approach whereby, keys to strong encryption are escrowed with a trusted entity. Under this approach, the keys would be provided to law enforcement authorities upon presentation of a duly-executed wiretap warrant. Some of these approaches could also assist firms in recovering lost data, where, for example, a key has been lost. Private sector approaches being developed to meet the needs of corporate key escrow may also benefit government, both as a user and in its law enforcement responsibilities.

As a user, government has its own needs for security. In order to protect its voice and low-speed telephonic data communications, the government has developed and fielded a technology to meet these needs, known as the Escrowed Encryption Standard, or "Clipper" chip. It is available for voluntary use by the private sector, but individuals may continue to choose to use any encryption technique domestically.

The private sector has reacted strongly to this initiative, objecting to the key escrow feature, to the fact that the technology is hardware-based, and to its use of a classified algorithm. However, this technology gives government no new authority or abilities. Instead, it enables government to protect its own information while supporting effective law enforcement.

2. Digital Signatures

In an open digital environment, verifying the source of a message or document and assuring that it has not been changed was mentioned as a concern in a number of different meetings. For example, in electronic payments there is concern that the correct payment is made to the correct individual. As noted at the meetings, the private sector is actively working on providing this capability and assuring effective protection. The underlying technology for such protection is digital signature.

A digital signature is created by applying an encryption algorithm to the information, resulting in a unique "signature" associated with the information. This signature is encrypted and sent with the information, which may or may not itself be encrypted. By verifying the signature and comparing it with the information, the receiver can verify that the contents of the message were not altered in transit. Of course, such a technique does not prevent or correct alterations, it only detects them.

While there are a number of different technical approaches to digital signatures, two are prevalent in the current environment. One, based on the RSA encryption algorithm, is coming into wide use in the private sector. A second, based on the El Gamal algorithm, has been adopted as the Federal standard for signature and is coming into use in the Federal government. Both require a public key infrastructure to provide a trusted third party, which will allow verification that the signer of a given document is indeed who he or she claims to be.

3. Public Key Infrastructure

In tomorrow's open networks, cryptography will help to verify the identity of a message sender, assure the integrity of a message, and protect information from unauthorized readers. Without some means of verifying where and to whom their information is going, people may hesitate to do business electronically. A Public Key Infrastructure (PKI) uses two keys, one public, like a phone number, and the other private, like a personal identification number (PIN) or password. The public key is listed in a public electronic directory, while the private key is kept secret by the individual.

The primary application of a PKI is to verify the identity of a message sender through creation of a digital signature. To create a digital signature, a sender of information uses her private key to sign the message. The receiver uses the sender's public key to verify the signature.

A PKI can also support confidentiality of messages. A sender of information obtains the receiver's public key and encrypts the data. The receiver uses his private key to decrypt

the information.

A public key infrastructure has great potential to encourage new activity on the NII because it provides a means to do business among parties without prior arrangements. For example, a mail order company posts its public key in an on-line catalogue. Customers send in their order with their credit card number in encrypted format. The company uses its private key to decrypt the information.

b. Protecting Against Copying

A more difficult technical problem that is being addressed by the private sector is protecting information against unauthorized copying. Technology using encryption to prevent data from being read by individuals who are not authorized to read it is readily available. However, preventing individuals from making unauthorized use of data they have been authorized to read is a more difficult technical problem to solve.

Once someone possesses a document in electronic form, it is easy to copy and redistribute it. If the information is copyrighted or protected by non-disclosure agreements, there is little more that the owner of the information can effectively do. Intellectual property owners are concerned that if they disseminate information with commercial value such as software, music, books, or video images, it will be widely pirated. Many of these property holders have traditionally disseminated in other media, such as paper or film.

Efforts to protect copyrighted software from unauthorized reproduction provide an interesting case study of the various approaches -- both legal and technical -- used to protect intellectual property rights. Some software developers have used cryptography to prevent illegal reproduction of their software. Alternatively, the Software Publishers Association (SPA) has a two-fold approach to this issue: it sues corporations that make illegal copies of copyrighted software, and it is also conducting a campaign to educate the public on software copyright issues. However, the international component of this problem makes legal and educational remedies difficult.

IV. GOVERNMENT ROLE AND RESPONSIBILITIES

The NII will be designed, built, owned, and operated by private citizens and private organizations. It will primarily be used by individuals and organizations, but it will also be used by Federal, State, local, and Tribal governments in support of their missions. The Federal government has an important role in the continued development and growth of the NII as a leader, facilitator, a promoter of the general welfare, a catalyst, and a

model user.

Based on information generated from the public meetings, the private sector is addressing many of the security needs of the NII. NII security, like other aspects of the NII, will be developed, built, and used by the private sector. Products and services that can be used to secure information on the NII will be designed and provided by the private sector in response to market demands. This section of the security report proposes the role of the Federal government in supporting a secure NII.

The Federal government will undertake four main activities for improving NII Security. The first three involve the government's responsibilities to ensure the sound development and use of the NII. The fourth is the government's responsibility as a user of the NII.

First, the Federal government will serve as a facilitator and a catalyst for promoting private sector activity.

Second, in its role as guardian of the public interest and general welfare, the Federal government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules for security in the NII.

Third, the Federal government can support the private sector's development of needed technology by funding research and development in critical areas.

Fourth, as a model user of the NII, the Federal government has a responsibility to ensure that its own automated information is secure.

- A. As facilitator and catalyst for private sector activity, the Federal government will (1) adopt the NII Security Tenets and the OECD Security Principles for use on the NII; (2) stimulate dialogue and awareness about security risks, needs, and solutions; (3) make Federal security products and techniques available for use in the NII; and (4) promote private sector development of high quality security products and services.**

- 1. Adopt the NII Security Tenets and the OECD Security Principles for use on the NII.**

Sound security must be based on a common understanding of what is entailed. The NII Security Tenets previously proposed and the internationally-recognized OECD Security Principles [Appendix A] form a solid foundation for developing security products, services, and practices on the NII and internationally.

Furthermore, security is needed to protect privacy and intellectual property rights. Principles on privacy and on intellectual property rights have been released by both the U.S. Advisory Council on the NII and by the Information Infrastructure Task Force.

Proposed Action 1: Promulgate the Tenets and Principles in the final version of this report by September, 1995.

2. Stimulate dialogue and awareness of security risks, needs, and solutions.

The series of public meetings co-sponsored by the Security Issues Forum and members of the NII Advisory Council is the beginning of an on-going dialogue concerning NII security. This report is designed to further that dialogue.

As the NII interconnects U.S. participants into a global information infrastructure, it introduces new threats to U.S. systems and information. Some of these threats (e.g., sophisticated "crackers" in a foreign country) may be difficult for individual participants to fully perceive. In the course of its international relations, the Federal government may learn about the prevalence and magnitude of this type of threat. This information should be shared with participants in the NII.

During the public meetings, there was considerable discussion about assuring appropriate behavior on the part of participants in the NII. One part of that discussion pointed out that many of those who break into others' systems believe such behavior is acceptable. To begin countering this incorrect perception, it was suggested that the Federal government should promote inclusion of ethical computing in educational courses.

Proposed Action 1: Develop data on threat and risk assessment for the NII and appropriately make it available to the public. Promote awareness of the existence of different threats to the NII with an understanding that there is no "one size fits all" solution, and that different threats must be treated differently. Ongoing.

Proposed Action 2: Stimulate dialogue and broad awareness of the national and economic security concerns related to the NII through public meetings and other outreach methods. Ongoing.

Proposed Action 3: Promote educational programs (along with the private sector and state, local, and tribal governments) to teach ethical behavior and awareness of security issues and risks on the NII. March 1996.

Proposed Action 4: Address the issue of minors gaining access to

adult materials on NII. September, 1995.

3. Make Federal security products and techniques available for use in the NII.

This report recognizes that strong, effective security is important to users of the NII in protecting their information. In the past, when private sector products were not available, the Federal government has developed security products for its own use that other NII users have found useful. The Data Encryption Standard (DES) (Federal Information Processing Standard Publication 46), originally developed for government use, has become a worldwide standard for protecting financial information on the world's banking system. Similarly, the Digital Signature Standard (Federal Information Processing Standard Publication 186), provides a strong, efficient, and economical means of assuring the integrity of electronic documents and the authenticity of the sender. The extent to which government-developed technologies will be adopted by the private sector is dependent on a variety of factors. The government does not intend to mandate security products for private sector use, but instead to depend on the marketplace to select those products that best meet the needs of the various NII participants.

Proposed Action 1: *Compile a list of security technologies developed for or used by the Federal government, evaluate them for appropriate and applicable use in the private sector, and make them generally available to the public. Ongoing.*

4. Promote private sector development of high quality security products and services.

NII users are demanding high quality security products and services. Flexible and responsive standards and accreditation processes can assist in the development of those products.

Some security products may provide confidentiality of information that is so strong that it can frustrate law enforcement's authorized ability to listen to communications where criminal activity is suspected. As Vice President Gore has written:

"The Administration has committed itself to cooperating with industry representatives and privacy advocates towards the goal of developing a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address national security needs as well. Such a system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be

exportable. . . .

We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrow services for their own products. Having a number of escrow agents would give individuals and businesses more choices and flexibility in meeting their needs for secure communications." (Letter to Representative Maria Cantwell and others, July 20, 1994)

In addition, the Federal government has for years regulated the export of products based on critical technologies for national security reasons. Although the U.S. has relaxed many of its export controls for advanced computing and communications technologies, certain encryption technologies remain restricted. Nevertheless, the U.S. has committed to allowing the overseas use of encryption for personal use by Americans.

Proposed Action 1: Promote the development of private certification processes through private, nationally and internationally recognized entities such as the American National Standards Institute, the International Standards Organization, nationally recognized testing laboratories, Underwriter's Laboratories, and other private sector communities of interest, such as the health, entertainment, and financial sectors. June, 1996.

Proposed Action 2: Continue to work with industry to develop alternative key escrow technologies, to make available standards and technology for public use, to develop methods for providing compatibility among different key escrow technologies, and to consider ways to promote use of such technologies overseas. December, 1995.

Proposed Action 3: Work with industry and the private sector to foster development of a public key infrastructure. December, 1995.

Proposed Action 4: Encourage the private sector to develop technology vulnerability and risk management guidance in accordance with the requirements for their communities. December, 1995.

Proposed Action 5: Review technology policy for the NII to ensure support for cooperative Federal-industry approaches in the development of security technology. January, 1996.

Proposed Action 6: Issue a proposed rule to establish a personal use exemption for overseas use of encryption. July, 1995.

- B. In its role as protector of the public interest, the government will: (1) assure adequate emergency response capability on the NII; (2) adapt current oversight processes to meet the challenges of the NII; (3) review criminal law; and (4) promote international cooperation.

1. **Assure adequate emergency response capability on the NII.**

Today the Federal government sets priorities and procedures for service on the public switched network in the event of an emergency in order to meet critical communication needs and to assist in an orderly recovery. This role should be extended to establishment of priorities and procedures to support a robust emergency response capability comparable to that provided by CERT, the Computer Emergency Response Team. An extension of this role to assure that priority communications in the NII when emergencies occur will be necessary.

Proposed Action 1: Review emergency communications and network services requirements and priorities, to include the Telecommunications Service Priority program, to assure that appropriate priorities for the NII are established in times of emergency. September, 1995.

Proposed Action 2: Cooperate with private sector and State, local, and Tribal governments to ensure that vital government and civil infrastructure security needs are being addressed. January, 1995.

2. **Adapt current oversight processes to meet the challenges of the NII.**

The government does not regulate the NII as a whole, although it does regulate different pieces, including providers such as common carriers and users such as financial institutions. As discussed above, virtually every sector of the economy, from health care to aviation, is growing to depend on the NII. Security failures in the supporting information infrastructure could jeopardize the U.S. economic well-being, national security, and public safety. Thus the current oversight processes must be adapted to meet the challenges of the NII.

Proposed Action 1: Examine whether current banking regulations are adequate in the areas of electronic banking, electronic payment systems, and "digital cash," in order, for example, to protect consumers from counterfeiting and fraud. November, 1995.

Proposed Action 2: Ensure that all Federal agencies evaluate their current oversight mechanisms and practices in light of the growing need to address the growing dependence on the NII.

December, 1995.

3. Review Criminal Law.

A review of current law is timely, particularly in the areas of intellectual property rights and computer crime. The Federal government has such reviews underway and will propose its views for public discussion in mid-1995. For example, the Intellectual Property Rights Working Group has proposed that selling software designed to defeat copy protection of copyrighted materials be deemed contributory infringement under the Copyright Act. The Federal government will continue to work with private sector and State, local, and Tribal governments to ensure that proposed changes in criminal law are appropriate.

Proposed Action 1: *Propose legislation to enable prosecution of computer-related crime. June, 1995.*

4. Promote International Cooperation.

In recognition of the increasingly global nature of the information infrastructure, the U.S. has been active in putting computer and communications security issues on the table in international fora. At the G-7 Ministerial Conference on the Information Society in Brussels in February 1995, the U.S. proposed, and the G-7 partners agreed, to increase efforts to find creative, technological and policy solutions to increase "the reliability and security of national and international networks by developing security principles that are commensurate with the risk and magnitude of harm." The OECD has been a leading international organization in the area of information and communications security.

Proposed Action 1: *Stimulate consideration of security issues at the OECD and other international fora. Ongoing.*

C. The government will promote research and development in critical and high-risk areas.

Although the private sector will continue to respond to market pressures and opportunities to create technical security products, services, and techniques, there may be a need for government to encourage private sector research and development in high risk or critical technologies. Some technologies developed by the government which are suitable for adaption for industry applications sector may become available through technology transfer programs. In other situations, government supports the private sector through funding pre-commercial, pre-competitive technology through various grant programs,

cooperative research and development agreements (CRADAs), and other technology development programs. For example, the Advanced Research Projects Agency (ARPA) and the NIST Advanced Technology Program are currently funding research into advanced technology that could be used to support an automated copy management system.

Proposed Action 1: Promote research and development through the High Performance Computing and Communications Program, ARPA, NIST, and others, of security technology that supports agencies' missions. Ongoing.

D. As a user, the government has a responsibility to protect the information in its possession and to act as a model user. Thus, it has the obligation to support all elements of a secure NII as it procures and manages its own portion of the NII. The Federal government will: (1) protect its own security requirements through good management processes; (2) improve its national security/emergency preparedness capabilities; (3) ensure that the products and services it uses meet its needs; and (4) develop a security infrastructure for its own use.

1. Protect its own information through good management practices.

The Computer Security Act of 1987 provides the framework within which Federal agencies will manage the security of the vast majority of their use of the NII. Through that mechanism, they will work to assure the confidentiality, integrity, and availability of their information as they use the NII. In March, the Office of Management and Budget (OMB) issued a draft revision to OMB Circular A-130, Appendix III, "Security of Federal Automated Information" to re-orient Federal implementation of the Act. The proposal will guide agencies in securing information as they increasingly rely on the open and interconnected NII. It stresses management controls such as individual accountability and awareness and training, rather than technical controls.

Similarly, the military will use and be dependent on the security and reliability of the NII. This may require using technologies especially designed for government use, such as advanced firewalls and encryption devices.

Proposed Action 1: Release final guidance to agencies to assure adequate security of Federal automated information through education, training, and awareness programs across agencies. September, 1995.

Proposed Action 2: Continue development of security technologies

to support unique government requirements. Ongoing.

Proposed Action 3: Develop and implement a program to ensure the security of Federal automated information consistent with guidance. January, 1996.

2. Improve its national security/emergency preparedness capabilities.

The National Communications System is a government entity that seeks to effect coordination among Federal government agencies and between the government and the telecommunications industry in order to support the government's emergency response mission. Through its efforts to promote the sharing of information between the private sector and government, the NCS promotes greater cooperation in securing networks for both the civil and private sectors.

Proposed Action 1: Review and validate national security and emergency preparedness (NS/EP) requirements for the nation's information infrastructure. December, 1995.

3. Ensure that the products and services it uses meet its needs.

The Federal government will adopt voluntary, consensus based standards wherever practicable. Where an appropriate standard developed in the private sector is not available, government will develop a standard for its own use. These standards will be available for other parties to use on voluntary basis. These standards are developed and promulgated by the National Institute of Standards and Technology (NIST) of the Department of Commerce.

The Federal government has traditionally accredited many of its standards through government laboratories. Increasingly, however, private sector evaluations are encouraged, as in "Security Requirements for Cryptographic Modules" (Federal Information Processing Standards Publication 140-1). The government also publicly issues lists of commercial products that it has accredited for its use.

Proposed Action 1: Rely, where possible, on security products which are based on industry standards. However, where commercial security services and standards are insufficient for government's needs in the NII, the government should develop security standards and use products built to those standards. Ongoing.

4. Develop a security infrastructure for its own use.

Under the auspices of the NII Security Issues Forum, the General Services Administration has established a Security Infrastructure Program Management Office. This office is coordinating the development of a public key infrastructure to meet the Federal government's needs for digital signature and confidentiality purposes. The U.S. Postal Service is pursuing complementary efforts.

Proposed Action 1: *Develop a public key infrastructure for government use. Demonstrate interoperability with multiple agencies and with industry. June, 1996.*

V. CONCLUSION

Users of the NII require reasonable confidence about the confidentiality, integrity, reliability, and availability of their communications. While the Federal government has a role in supporting a secure NII by facilitating private sector activity, ensuring public safety by protecting against abuses that result in harm to others, and supporting research and development in critical areas, much of the responsibility lies with the private sector. It is neither appropriate nor realistic to expect the Federal government to provide the security solution for the NII. Not only is the NII too complex for a one-size-fits-all solution, but without demand from users, the market in appropriate security tools and services will not succeed.

Ultimately, users must realize that no system is completely free of risk. Users of the NII must make informed choices about an acceptable level of risk for a particular transaction. While laws, policies, and technology can contribute to a secure NII, awareness of risk is the foundation upon which a secure NII will stand.

LRM ID: JAW187

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
Washington, D.C. 20503-0001

6968

Thursday, October 9, 1997

LEGISLATIVE REFERRAL MEMORANDUM

TO: Legislative Liaison Officer - See Distribution below

FROM: James J. Jukes (for) Assistant Director for Legislative Reference
OMB CONTACT: Glenn R. Schlarman
PHONE: (202)395-3514 FAX: (202)395-5167

SUBJECT: National Information Infrastructure Security Issues Forum Report on
National Information Infrastructure Security

DEADLINE: Noon Friday, October 17, 1997

In accordance with OMB Circular A-19, OMB requests the views of your agency on the above subject before advising on its relationship to the program of the President. **Please advise us if this item will affect direct spending or receipts for purposes of the "Pay-As-You-Go" provisions of Title XIII of the Omnibus Budget Reconciliation Act of 1990.**

COMMENTS: This is the proposed final version of the report, which was prepared by an interagency group. A list of agency representatives is enclosed. This version of the report reflects responses to comments on the draft published in the Federal Register in June 1996. The substantive changes from that version are on pages 4 - 7, 13, and Appendix A.

DISTRIBUTION LIST

AGENCIES:

25-COMMERCE - Michael A. Levitt - (202) 482-3151
29-DEFENSE - Samuel T. Brick Jr. - (703) 697-1305
32-ENERGY - Bob Rabben - (202) 586-6718
51-General Services Administration - William R. Ratchford - (202) 501-0563
61-JUSTICE - Andrew Fois - (202) 514-2141
69-National Aeronautics & Space Administration - Jeff Lawrence - (202) 358-1948
76-National Economic Council - Sonyia Matthews - (202) 456-6630
83-National Security Council - Glyn T. Davies - (202) 456-9221
95-Office of Science and Technology Policy - Jeff Smith - (202) 456-6047
114-STATE - Paul Rademacher - (202) 647-4463
117 and 340-TRANSPORTATION - Tom Herlihy - (202) 366-4687
118-TREASURY - Richard S. Carro - (202) 622-0650
36-Federal Communications Commission - Steve Klitzman - (202) 418-1900

EOP:

Donald H. Gips
Ira C. Magaziner
Margaret E. Evans

OCT 13 9:31

David Tornquist
Louisa Koch
David J. Haun
Harry G. Meyers
Tom Kalil
Jim Murr

LRM ID: JAW187 SUBJECT: National Information Infrastructure Security Issues Forum Report
on National Information Infrastructure Security

RESPONSE TO
LEGISLATIVE REFERRAL
MEMORANDUM

If your response to this request for views is short (e.g., concur/no comment), we prefer that you respond by e-mail or by faxing us this response sheet. If the response is short and you prefer to call, please call the branch-wide line shown below (NOT the analyst's line) to leave a message with a legislative assistant.

You may also respond by:

(1) calling the analyst/attorney's direct line (you will be connected to voice mail if the analyst does not answer); or

(2) sending us a memo or letter

Please include the LRM number shown above, and the subject shown below.

TO: Glenn R. Schlarman Phone: 395-3514 Fax: 395-5167
 Office of Management and Budget
 Branch-Wide Line (to reach legislative assistant): 395-7231

FROM: _____ (Date)
 _____ (Name)
 _____ (Agency)
 _____ (Telephone)

The following is the response of our agency to your request for views on the above-captioned subject:

_____ Concur

_____ No Objection

_____ No Comment

_____ See proposed edits on pages _____

_____ Other: _____

_____ FAX RETURN of _____ pages, attached to this response sheet

Agency Representatives to National Information Infrastructure Security Issues Forum

NSC

OSTP

Ira Magaziner,

OVP -- Don Gips

NEC -- Tom Kalil

Defense -- Roger Callahan OSD C3I (DARPA --Teresa Lunt)

Justice -- Scott Charney, paul Friedman

Energy -- John Przysucha, Phil Sibert

Transportation -- unknown

Commerce -- Mark Bohanon (NIST -- Barbara Guttman, Dennis Steinauer)

Treasury -- Martin Ferris

State -- Liza McClenaghan

GSA -- Tom Burke

NASA -- Richard Carr

FCC -- Mike Nelson

DRAFT

**Report by the National Information Infrastructure
Security Issues Forum**

NII Security: A Private and Public Responsibility

October 1997

NII Security: A Private and Public Responsibility

October 1997

1. Definition of Problem	1
What is Included and Excluded	1
General Outline	2
2. Story of the Process	2
Security Tenets	2
OECD Principles	3
Hearings	3
Draft Report and Public Comments	4
Recent Progress	6
3. The NII and Security	7
What is the NII?	7
What is NII Security?	8
Providing Security on the NII	8
4. Broad Tenets for Federal Policy-Making	10
Make it in the Open	10
Stay Flexible	10
Anticipate Diverse Interests, Abundance, and Diminished Influence	10
Today's Mores Can Fit Tomorrow's Technologies	11
5. The Federal Role is an Extension of Well-Understood Duties	11
The NII is Largely Private and so is the Duty to Protect It	11
National Security	11
An Update on Encryption Policy	13
The Scope of Federal Concern -- The Threshold for Government Action	13
6. Conclusion	14
Appendix A	
Where We Are Today on Specific Federal Actions	16
Appendix B	
OECD Principles	33
Appendix C	
The Role of Technology in Security of the NII	35
Appendix D	
Oversight and Enforcement	40

Appendix E	
The First Public Meetings: Provider and User Security Concerns	43
Appendix F	
Roles and Responsibilities: NII Security Issues Forum	48

NII Security: A Private and Public Responsibility

October 1997

1. Definition of Problem

Security is the sine qua non of the National Information Infrastructure (NII). The NII will not be used if people cannot rely on the NII to be there and work right when they need it; if they cannot trust it with valuable information; or if they cannot be sure that what they see has not been altered illicitly or inadvertently.

Security -- protecting citizens from enemies both foreign and domestic -- has long been the province of government. Yet, determining the appropriate Federal role in NII security is not always obvious nor straightforward. Most of the NII is privately owned and operated. Yet, as the economy and society depend increasingly on the secure performance of the NII, the responsibility of the Federal government to assure that security is addressed increases. The challenge is to find the right balance of public and private responsibility.

To develop a workable set of tenets that can help define the Federal role in NII security, the NII Security Issues Forum (Forum) was established by the Information Infrastructure Task Force (IITF) formed by Vice President Gore. The Forum is chaired by Sally Katzen, the Administrator of the Office of Information and Regulatory Affairs in the Office and Management and Budget. Membership includes representatives from each of the IITF's committees as well as every Executive Branch organization with significant information security responsibilities. The Forum's charter is located at Appendix F.

a. What is Included and Excluded

Security, for purposes of this report, is defined as:

- integrity -- assuring that information will not be accidentally or maliciously altered or destroyed;
- reliability -- assuring that systems will perform consistently and at an acceptable level of quality;
- availability -- assuring that information and communications services will be ready for use when expected; and
- confidentiality -- assuring that information will be kept secret, with access limited to appropriate persons.

Security is an essential tool to control access to information, including personal information and intellectual property. This report recognizes that other fora, both within and outside the IITF, are debating the policy framework that will set the access rules for content.

b. General Outline

What follows in this report is: (1) a review of the process by which the Forum developed its recommendations, (2) a discussion of the nature of security and the NII, (3) a framework for Federal policy-making in the area of NII security, and (4) a discussion of the appropriate Federal role including, in Appendix A, specific actions the government has taken to date and, where appropriate, identification of lead agencies for further implementation.

2. Story of the Process

Beginning in 1994, the Forum began a public dialogue which included discussing five broad security tenets, the security principles developed by the Organization for Economic Cooperation and Development, and soliciting provider and user security concerns via public hearings. The Forum then drafted a report, invited written comments on it and conducted a public hearing on those comments. This final report is the result of those efforts.

a. Security Tenets

On February 10, 1995 (60 Federal Register 8100), the IITF proposed five security tenets for public comment, based on input from public meetings discussed below. These tenets indicate that NII users expect:

- 1) The ability to control who sees (or cannot see) their information and under what terms.
- 2) The ability to know who they are communicating with.
- 3) The ability to know that information stored or transmitted is unaltered.
- 4) The ability to know when information and communication services will (or will not be) available.
- 5) The ability to block unwanted information or intrusions.

Two conditions attach to these security tenets:

None of these tenets is absolute. For each tenet there may be valid societal reasons -- such as an emergency or a need to protect another's rights -- that cause the tenet to be conditioned in some manner. And they must be balanced with each other (e.g., caller ID supports the second tenet but may violate the first), as well as with broader societal goals (e.g., emergencies may override the fifth tenet).

Each tenet requires NII participants to take responsibility for establishing the terms and conditions under which they will exchange information. The distributed and empowering nature of this technology demands a greater level of personal responsibility from participants than when communications systems were more limited in scope and scale. Education of NII participants is thus a critical task.

b. OECD Principles

The United States is not alone in addressing security concerns in the evolving global information infrastructure as exhibited by the security principles developed by the Organization for Economic Cooperation and Development (OECD) and endorsed by its members (the United States and 23 other nations). These guidelines articulate needs for explicit accountability for security, greater awareness of security practices and procedures, and respect for the rights and legitimate interests of other users. See Appendix B for the text of the OECD principles. They have been incorporated into two National Institute of Standards and Technology (NIST) publications: "An Introduction to Computer Security: The NIST Handbook," which sketches them out, and "Federal Computer Security Principles and Practices" which explains them in detail.¹

c. Hearings

To promote public dialogue, the Forum held seven public meetings in cooperation with Mega-Project III of the U.S. Advisory Council on the NII. The first was a general meeting while five subsequent meetings explored the needs of various sectors: information content industries (software and entertainment), finance, health and education, government services, and intelligent transportation. The last meeting addressed the availability and reliability of the NII.

The public meetings covered security as defined earlier in this report. The most salient concerns expressed by participants were those related to privacy (e.g., the inability to control secondary uses of information, the placement of liability for lost or misused information, how much government itself can be trusted with information, and protecting one's system from excessive or unwanted incoming communications) and those pertaining to protection against disabling attacks (e.g., protecting one's system from hackers and ensuring that systems will be there when needed).

Respondents differed over whether government intervention would improve security and privacy in the NII. Some wanted government to combat defamation and pornography on the NII or felt that it should spend more on national security and emergency preparedness. Others felt that government involvement could create inefficiencies, reduce privacy, increase fraud, and depersonalize society. Many argued that export controls over of cryptographic hardware and software would inhibit the development of security products for the NII.

The public hearings elicited useful information. For instance, there is considerable technology being developed to protect intellectual property (e.g., software that can disable itself

¹ See the NIST Website at <http://csrc.ncsl.nist.gov/nistpubs/>. The handbook is also available from the Government Printing Office ((202) 512-1800), for \$18.00, cite stock number SN003-003-03374-0.

if not paid for and keys that can decrypt movies for one-time viewing). Participants in the meeting on health care wanted to consider the use of technologies traditionally associated with national security information (e.g., need-to-know controls, compartmentalization, and automatic record destruction). Those focussed on financial services were concerned about authentication, techniques to foil electronic counterfeiting, and how individuals could control access to personal data kept in institutional databases. Transportation experts were concerned both about privacy (e.g., the automatic collection of license plate numbers as they zip past electronic toll booths) and preventing collisions (e.g., if automatic traffic systems collapse without warning). The issue of smart cards to deliver government benefits (e.g., food stamps) was raised with fears that, absent security, such cards could be converted to cash, counterfeited, or altered to increase their value. Discussions on the overall infrastructure concentrated on emergency preparedness and the need to protect vulnerable communications systems from unauthorized intervention by authorized insiders as well as from hostile outsiders. See Appendix E for a more detailed discussion of the individual meetings.

d. Draft Report and Public Comments

A report was drafted based on these inputs which covered the government's coordinating functions (e.g., education and emergency preparedness), its oversight and enforcement roles, technology issues, and concluded with a set of recommendations and proposed actions. The recommendations and proposed actions were presented within the framework of four main activities for government. First, when needed and requested to do so, it will serve as a facilitator and a catalyst for promoting private sector activity. Second, as guardian of the public interest and general welfare, the Federal government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules. Third, as necessary it will support the private sector's development of needed technology by funding research and development in critical areas. And fourth, as a model user of the NII, the Federal government will ensure that its own automated information is secure.

In June 1995, the draft report entitled "NII Security: The Federal Role" was released for public comment. While some comments were received from individuals, most were from commercial organizations and understandably focused on issues affecting electronic commerce. The tenor of their comments was positive and in general agreement with the four main activities specified above. There were, however, a number of recurring concerns and they are discussed below.

A broad principle expressed by many commenters was that the NII will only succeed if it is a market-driven system fueled by private sector activity with the government role kept at a minimum. One commenter said it best: "In every discussion . . . the government should ask 'why it should be considered for the task'." The Forum agrees with this overarching principle and finds it to be entirely consistent with the private-sector orientation of the NII itself.

Most of the commenters also pointed out that security is a global, not just domestic issue

and involvement by the United States Federal government must not place U.S. companies at a disadvantage in the global marketplace. These commenters prefaced their remarks with expressions of support for law enforcement's public safety responsibilities and the government's national security obligations -- so long as they did not interfere with the development of global networks or frustrate business opportunities. One commenter stated that "[t]he Federal government should not interfere with the development, use, or export of encryption software and hardware." Another stated that the private sector and the government should work closely together to develop means by which sound procedures for protection of basic rights can be addressed globally. The Forum agrees with the latter view, and later in this report describes how this cooperation is now being accomplished.

Many commenters were also concerned that the government might attempt to set standards for quality assurance or even formally certify security tools, thereby undercutting the market's role in providing (and sifting through) such products. A related concern was that the government might be too quick to declare existing standards inadequate for its own needs. Indeed, most respondents felt the market was doing a good job in providing security tools as well as standards. "If standards must be developed," said one commenter, "they should be industry-led, voluntary, and market driven." The Forum agrees, and, as a point of clarification, it did not intend to suggest a mandatory product certification process or even a specific model for a voluntary one. At the same time, the Forum encourages the private sector to develop "centers of excellence" or other processes whereby best products and best practices can be easily identified and selected by the less experienced users of the NII. In sum, the Forum's position is that the private sector should develop and implement its own security solutions and, whenever possible, the government should look to the private sector for its solutions as well.

Protecting children from inappropriate material and protecting intellectual property from misuse and copying also received a fair number of comments. Most felt that the protection of children was the role of the private sector, not an expanded one for government. This issue is receiving attention far and wide; as public and legal reaction to the Communications Decency Act of 1996 proved, consensus resolution may be a long way off. On the issue of intellectual property, one commenter felt that the report's discussion did not adequately reflect the seriousness of the issue and asked for a commitment to greater discussion and recognition of that fact. The Forum agrees that such discussion is essential, although not in the context of this report. As this final report is written, a number of expert organizations, private and public, domestic and international, are engaged in that discussion.

With regard to emergency response capability, one commenter expressed uncertainty as to how the government will assure emergency response since it neither owns nor controls the NII. The Forum finds that the need for public-private cooperation is again underscored here.

Several commenters also thought the report would benefit from a broader discussion of the threats faced by NII users. As is discussed later in this report, the Forum firmly supports the progressive exchange of comprehensive threat and vulnerability data. This report, however, is

not the appropriate venue for that exchange. Threats and vulnerabilities are ever-changing, are often situation-dependent, and in some cases are not appropriate for public discussion.

Finally, some commenters noted that technology, rather than impelling further government involvement with the NII, might have the opposite effect in allowing market forces to take over functions (e.g., efficient and reasonably priced access) once performed by regulation. Finally, one commenter suggested that “the title of the report might be adjusted to lessen the implication that the Federal role in NII security is the only or primary one.” We have revised the title accordingly.

After reviewing the public comments, the Forum held one final public meeting of the reply-comment variety often used in rule making. Invited witnesses addressed the comments received on the draft report focusing on the three specific areas: product certification, reliability of the information infrastructure, and encryption policy.

In urging us to exercise caution and flexibility in policy development, one witness from finance and banking pointed out, as an example, that today we do not know what kind of electronic money or associated delivery systems will “win out” in the market place and until we do, the necessary security system is also unknown. That witness also spoke of a number of industry technology task forces that are looking at developing standards for security and privacy, reminding us that the private sector, not just government, has the public interest at heart.

A witness from the information technology industry spoke of product certification in terms of fundamental customer satisfaction saying simply that if certification is “useful to your customer then it is useful to the supplier because it makes for a satisfied customer” and “suppliers want repeat business.” Another said that the government should not compete with the private sector in terms of research, product development or the provisions of service. The Forum agrees with both comments.

On infrastructure reliability, the witnesses generally held that with the NII’s opportunities come risks, but manageable ones. They also pointed out that to manage them, the risks must be understood and therefore education is very important. In that regard, the government having a wealth of information on risks and vulnerabilities, was urged to make much of it available so people will understand what risks they are accepting. The Forum embraces that view as well.

On encryption policy, witnesses remarked that they would rather see private sector led, industry driven solutions that meet consumers needs and for the government to update its export policies. The recent encryption policy changes, described later in this report, are consistent with these comments.

f. Recent Progress

Since the draft report was released and comments were received, the issue of NII security

and the proper government role has continued to evolve. Earlier concerns are still pressing, but a greater awareness is also developing regarding the security of the overall NII against a systematic attack. Most noteworthy is that on July 15, 1996, the President signed Executive Order 13010 establishing the Commission on Critical Infrastructure Protection which is to partner with the private sector and over the next year study the risk to the nation's critical infrastructure elements, including the NII. The Forum looks forward to seeing the Commission's findings and recommendations as they become available and encourages the reader to follow its activities as well.² In addition, the national security and law enforcement agencies are dedicating added resources to such infrastructure protection issues (e.g., the National Communications System has established an Infrastructure Assurance Branch to plan for the future and the Federal Bureau of Investigation's Computer Crime Squad is now investigating intrusions into major computer networks). The private sector is also giving added attention to this issue (e.g., the Information Technology Industry Council is guiding an all industry group to explore the viability of an industry-based security center of excellence and the 3,000 member National Computer Security Association is delivering services and raising awareness through a variety of conferences, industry consortia, procedural guidance, and security alerts).³

3. The NII and Security

Popular imagination often associates NII security with defenses against attacks by youthful hackers invading the Internet and planting Trojan horses, logic bombs, and viruses in their wake. Notwithstanding the occasional reality of such incidents, both the NII and security are broader phenomena.

a. What is the NII?

The broadest definition of the NII includes all networks that permit public access (at some level) coupled with telephones and computers accessible from them (e.g., in 1988, the infamous Morris Worm attacked not the Internet, but certain types of computers attached to it). Clearly the NII includes the telephone system (both wireline and wireless/pager networks) and the Internet. To that one may add cable (even though it is currently receiver-only), membership-based networks that ride on top of the phone system (e.g., airlines reservations, inter-library services, private networks such as Lexis/Nexis), private corporate networks that permit dial-up access and publicly owned networks that are (normally) inaccessible such as today's FAA or tomorrow's intelligent vehicle/highway systems. Defense communications also fit in, along with the power lines that today carry virtually no message traffic -- but one day might. All of these elements and more belong to the NII and for the most part they are being designed, built, owned, and operated by private citizens and private organizations. The difficulty

² See the Commission's Website at <http://www.pccip.gov/pccip/>

³ See the ITIC and NCSA Websites at <http://www.itic.org.isec.htm> and <http://www.ncsa.com>, respectively

of defining the NII explicitly, combined with the vast heterogeneity of networks and equipments that may be said to be part of it, should be an immediate caution to policy-makers: one size most definitely does not fit all.

b. What is NII Security?

As discussed earlier, NII security comprises four elements -- integrity, reliability, availability, and confidentiality -- and potential failures of security vary as much as the NII's constituent parts do. Security can be considered as being inadequate when users access spectrum they are not entitled to (e.g., to jam or override legitimate signals), when authorized users abuse unconstrained access into a system (e.g., E-mail flooding), when authorized users access a system for unauthorized purposes, when unauthorized users access a system for any reason, and when individuals and institutions access and distribute information they possess in violation of law or contract (e.g., defeating copyright protection). Security can also be compromised inadvertently (e.g., the accidental release of private or proprietary information).

The consequences of such breaches include the theft of service (e.g., cellular phone call fraud), theft of information (e.g., proprietary industrial processes), theft of assets (e.g., illicit funds transfers), violating privacy (e.g., viewing a person's medical history) corrupting data in storage or motion (e.g., overriding machinery control instructions to create accidents), and disrupting information services (e.g., telephony) or attached services (e.g., electric power distribution).

c. Providing Security on the NII

Societies are not helpless against attacks on their information infrastructures. Information systems can be defended (or the results of security failures mitigated) in various ways ranging from taking them off-line and manual overrides, to semantic filters, firewalls, encryption, digital signatures for access control, intrusion detection and anti-virus programs, event logging, archiving critical information and programs to unerasable media, and increased security awareness among users and administrators. Many attacks on information systems are criminal acts and thus a robust ability to prosecute perpetrators can deter attacks. Finally, nations have other ways of dealing with exceptional attacks on their information infrastructures that carry national security implications.

In the physical world, ensuring the security of a nation against external invasion is almost entirely a matter of public (government) effort -- the provision of national defense. Ensuring a community's security against crime mixes private effort (e.g., locking doors, watching over one's neighborhood and reporting suspicious behavior) and public effort (e.g., law enforcement).

Ensuring the protection of the NII must also combine private and public effort because it combines the protection of systems -- almost all of which are private -- and the prosecution of violators. If public efforts could be guaranteed (e.g., today's attackers were caught and tomorrow's were deterred, all effects could be reversed, etc.), the need for private vigilance

would be far less. Unfortunately, the opposite is more likely: not all attacks can be identified as such (and some security breaches may not be per se illegal), attackers are very hard to identify (or extradite if operating from certain countries), and their effects are often difficult to reverse. Indeed, it remains to be seen how effective law enforcement can be in providing NII security. What is not in doubt, however, is that virtually everything required to defend an information system is within the control of the system's owner: from the choice of operating system and security software, to system design for redundancy and fault-tolerance, controls over access privileges and the choice of who to trust with what. Thus, the matter of NII security is ineluctably a matter for system owners -- which is to say the Federal government cannot protect the NII if its owners do not protect their part of it. Like other aspects of the NII, security will be developed, built, and used by the private sector.

What is needed most for a secure NII? One view expressed in the National Research Council's report, "Realizing the Information Future," is that while security needs can be addressed to some extent by technological methods and a legal framework, structures must be in place to make them work. If the NII is to succeed, a structure or a collection of structures -- a security architecture -- must exist to ensure security. The report states: "This security architecture must include technical facilities, recommended operational procedures, and means for recourse within the legal system. This architecture will be based on a variety of public and private institutions and policies. Although an architecture will define how institutions, policies, and technologies interconnect, a sound security architecture will consist not of rigidly prescribed technologies or solutions, but must be able to flexibly adapt to change." The report also notes that such an architecture will require research and development over time.

Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources," describes a security architecture in the context of a system security plan. The major ingredients of such an architecture are the rules of the system including expected behavior of the users, training to ensure that users are aware of their responsibilities, personnel security including individual access privileges, incident response capabilities, continuity of support and contingency planning, technical security, system interconnections and information sharing, and public access controls. Add to the foregoing physical and other security procedures, and one sees clearly that a security architecture is one of multiple layers, each as important as the next to achieve an overall acceptable level of risk.

The need for such an architecture is apparent for almost every user of the NII, government and the private sector alike. But it may not be appropriate or advisable for one user (or group of users) to dictate to another the specifications for that architecture. Just as each user's needs are different, so too are the applications that satisfy those needs and thus the architecture (including security) required to support those applications. In contemplating policy-making and the government's role in security of the NII, it is prudent to be mindful of the variety which is the NII.

4. Broad Tenets for Federal Policy-Making

NII security policy must be made with care. Information technology, despite its manifold promise, is new, poorly understood, and likely to have ramifications that cannot be predicted. For these reasons, this report notes several broad considerations that ought to go into the making of all NII security policy.

a. Make it in the Open

NII security policy must be made in the open by accountable officials. That is: the policy-making process (who, what, and when) should be transparent, rationales for policy should be clearly and honestly stated, as much backup evidence as possible (consistent with sensitive law enforcement techniques and national security) should be in the public domain, and meaningful opportunities for public participation should be provided.

Although all Federal policy-making should strive toward openness, there are special reasons why this holds for NII security policy. First, NII security is in part about who can keep secrets from whom; too many citizens are prepared to believe that NII security policies are designed to permit the government to maintain a monopoly on secrecy. NII security depends on private action. Convincing systems owners and other participants to protect themselves against a security threat means asking them to make investments, change their habits, and at times reduce the openness and flexibility of public networks. Sharing information about incidents will encourage them to take security seriously. The fact that our the nation's economic well being is becoming increasingly dependent on the NII should drive us to more open communication, public education, and awareness.

b. Stay Flexible

The policy-making process should allow itself time to understand the specific technology at issue as well as how its implications and uses play out. Few technologies change as rapidly as that associated with the NII. Five years ago, few had heard of the World-Wide Web. Policy discussions of public access to the NII revolved around high-definition televisions and set-top boxes -- each with its own regulatory issues. Today, the Web is everywhere, electronics firms are introducing Web TVs, and public policy has to start over virtually from scratch. Thus, for example, security policy for electronic commerce must be flexible enough to adapt to whatever standard method of electronic payment is adopted by the marketplace.

c. Anticipate Diverse Interests, Abundance, and Diminished Influence

NII security policy must also fit a rapidly changing institutional environment. First, all policy must balance interests (e.g., secure international electronic exchange versus the need to decipher hostile communications), and as the importance of one interest grows, the proper balancing point shifts. Second, much existing policy effecting the NII has been predicated on scarcity (e.g., rigid telecommunications service due to provider monopolies and limited available

bandwidth resulted in tightly regulated over-the-air broadcasters). Today's trends are characterized by a multiplicity of providers and growing abundance. Third, when the United States government accounted for a large percentage of the world's information technology products, its influence was large and its policies could reflect this fact. The United States government's share is dropping rapidly; it has a limited ability to influence technology in a particular direction.

d. Today's Mores Can Fit Tomorrow's Technologies

Finally, although it ought to go without saying, the Forum has seen no evidence that suggests that the NII cannot be adequately protected within the overall context of today's institutions and legal structures founded on English common law and the U. S. Constitution's protections for speech, search and seizure, due process, and rules of evidence. Appendix D is the draft report's comprehensive discussion of the oversight and enforcement issues that are germane to NII security.

5. The Federal Role is an Extension of Well-Understood Duties

What then ought the Federal government do to promote and enhance NII security? This report argues that the proper role can be elucidated by appreciating the private nature of the NII, assessing the national defense and public safety threat correctly, and deriving its duties from the Federal government's on-going functions and international responsibilities -- not creating new ones.

a. The NII is Largely Private and so is the Duty to Protect It

The Federal government should not need to encourage the private sector to defend the overwhelming bulk of NII which it owns and operates. But, if necessary, it can foster the development and dissemination of means and motivations for doing so. And in conjunction with other branches and levels of government, it can enforce laws that make most systems intrusions illegal. But the Forum believes that the best incentive of all is for the private sector systems owners and operators to appreciate that when they are perceived as not "doing enough," pressure will build for the government to "do something." At the same time, and regardless of such pressure, the Federal government cannot realistically or practically be expected to protect the NII in the same sense that it is expected to protect the nation from a foreign aggressor. In no sense can it throw a firewall around the NII and protect it from the global information infrastructure. In the end, the Federal government is an understudy, but (except where its own systems are involved) cannot take the stage.

b. National Security

As the United States as a whole becomes increasingly reliant on the NII for communications and information, other key components of the U.S. infrastructure will become dependent on it -- they already are. For example, the power grid, transportation systems,

financial institutions, and economic transaction data are all be dependent on the NII. Security weaknesses in the NII can place those other infrastructure elements at risk. Hence, a significant attack on the NII would be a threat to our national security in addition to the significant personal and economic harm it would cause. A challenge we face is identifying the point at which a private system's vulnerability to debilitating electronic attack becomes an unacceptable risk to the nation's economic well being or general welfare of its citizens -- the threshold separating criminal mischief (however severe) and national security.

Earlier we mentioned that the creation of the President's Commission on Critical Infrastructure Protection illustrates the rising concern over the national security implications and our vulnerability to a significant attack. Yet, a vulnerability does not necessarily constitute a threat or an unacceptable risk. If the government is to base NII security policy on the potential threat, or attempt to influence the private sector's actions as to their responsibilities, it must go further in elucidating the nature, motive, and consequences of the threat (finding hackers overseas does not say much; any decent university computer science department has its share). We must also attempt to discern what motivation a rational state actor might have in attacking our NII, how such an attack would be characterized (e.g., an act of war, terrorism, espionage or sabotage), and how we would respond if we were attacked (e.g., in the physical world, even acts of foreign sponsored espionage resulting in the loss of life have not been regarded as acts of war). Where possible, we need to share publicly our findings, for to make a case for extraordinary exertions requires a convincing public rationale.

If a widespread attack on the NII created what was, in effect, a disaster, what should the government's role be with respect to recovery? Unquestionably, the government's response in the event of such an attack would be no less than its response to any major natural (or man made) disaster -- one of ensuring public safety and coordinating and supplying emergency services. But, after such an attack, individual information systems must be recovered, and virtually all such systems are private. Even in the wake of a widespread attack, the government's role remains limited.

With growing sector interdependence and national security implications of an attack on the NII, emergency preparedness is becoming increasingly important. Three types of preparedness and response needs were discussed in the draft report. The first is an entity analogous to the Carnegie-Mellon's Computer Emergency Response Team (CERT), which currently acts as an Internet "911." The second is a system for planning and recovery during and after an emergency which sets, among other things, a priority of restoration -- opening up at least an emergency lane for essential traffic. One model is the National Communications System (NCS)/Federal Communications Commission's Telecommunications Service Priority System managed by the NCS which establishes the regulatory, administrative, and operational framework for priority restoration of communications services in support of emergency planning and response. The third emergency preparedness need involves the exchange of objective information concerning threats, vulnerabilities, and risks. Among the possible models for such exchange are CERT bulletins, industry newsletters, mutual assistance agreements, and on-line news groups.

c. An Update on Encryption Policy

The draft report's entire discussion of technology issues has been moved to Appendix C of this final report. Included in that discussion is a look at the use of encryption, entitled "Protecting Information." What follows here is an overview of what has occurred recently with respect to the world of policy. Much has taken place. That's not to say that all the problems have been solved, but, in the eyes of many -- progress has been made. In July 1996 the Administration proposed a new encryption policy framework designed to allow, and indeed encourage, the use of strong encryption internationally for both commerce and private communications while protecting public safety and national security.

The framework is based upon a global key management infrastructure that will have trusted private sector parties holding spare keys to confidential data that can be recovered only by the key owner or by law enforcement acting under proper authority.

The goal is to encourage commerce, both here and abroad, and is similar to the approach other countries are taking. It will permit nations to establish an interoperable key management infrastructure that can address each country's needs consistent with multi-lateral law enforcement agreements. For this to work, U.S. industry must take the lead and promote this framework internationally, but this will take time. So, for two years only, the government will allow liberalized export of unescrowed strong encryption products (up to 56 bit key length) provided the export applicant demonstrates the intent and ability to develop a key recovery system for its product.

Also part of this policy is the transfer of export control jurisdiction from the Department of State to the Department of Commerce and the launching of several key recovery pilot projects. The domestic use of encryption remains uncontrolled.

U.S. industry leaders are developing architectures and products that capitalize on the policy liberalization and will enable the United States to maintain its advantage in the international marketplace. This policy evolution involved an impressive degree of public-private cooperation and compromise on an issue that for years was the sole domain of the national security and Federal law enforcement communities.

Congress too is engaged in this effort and is considering various legislative proposals. The Forum regards continued public dialogue on all fronts as essential to the satisfactory resolution of this issue.

d. The Scope of Federal Concern -- The Threshold for Government Action

While the Forum has found ample evidence that many of the roles for NII security are not in doubt and the government serves primarily as an understudy, there remain unanswered questions as to when the understudy should step forward to assume the lead role -- the threshold for government action. In the physical world, while most thresholds are decided, even now,

some degree of uncertainty exists and debates occur from time-to-time. We should not expect it to be any different in Cyberspace, especially early on. These questions provide an opportunity for additional study and the Forum encourages such research.

In Appendix A, each of the four areas of government activities mentioned earlier (i.e., facilitator and a catalyst, guardian of the public interest, funding research and development, and model user) are restated together with corresponding action items. Found along with each item is action taken to date and, as appropriate, the lead agency for further implementation. The reader should note while reviewing these action items that the Forum's findings are conditioned by the following assumptions: 1) Where the security of private sector information systems affects responsibilities already under government aegis, the government has a reasonable right to demand assurance on these matters; 2) Only the government can enforce the law; 3) Only the government can provide for the national defense; 4) Where needed, the government will continue to support the development of better security products through its funding of research; 5) The government ought to promote education on an individual's duty to protect information and information systems that are entrusted to them, to respect the information and information systems of others, and to accord intellectual property rights their due respect; and, 6) The United States government should work toward an international consensus on how nations should cooperate to bolster the security of the Global Information Infrastructure.

6. Conclusion

The charter for the Security Issues Forum is located at Appendix F to this report. It calls on the Forum to "ascertain the security needs of the various NII user communities and the Federal role in assuring such security." While the process leading to this report determined much in the way of security needs and to a large degree identified the appropriate Federal role in assuring those needs, the Forum suggests that this report is but a snapshot at a point-in-time. The process of defining security needs and roles for the NII is dynamic, will continue to evolve, and will require additional snapshots to ensure we continue in the right direction and at the proper pace. Again, one tenet of security policy-making for the NII is to stay flexible.

The new title of this report demonstrates the Forum's long-held belief that the responsibility for security of the NII is shared between the public and private sectors. And beyond the title, this report is clear in its finding that the private sector holds the primary security role. The Forum validated this position through considerable dialogue with the public -- from the public meetings of 1994, to the public comments on the draft report, to member agencies' routine contacts with members of the public. Our recommendations go directly to the point of private sector responsibility (e.g., develop best products and best practices for all to use) with the Federal government serving in a support role (e.g., making available threat and vulnerability data necessary for private sector risk assessments).

The Forum concludes that the vitality of NII security hinges upon the government sharing with the system owners and operators threat and vulnerability data which is timely and specific enough to allow the private sector to make informed risk management decisions. The Forum

also calls on industry to reciprocate by sharing with their regulators pertinent data regarding losses suffered due to electronic intrusions which, in turn, obligates regulators to be sufficiently knowledgeable of NII security issues to react appropriately to such reports. To both, the Forum encourages the reporting of illegal acts to the appropriate law enforcement authorities. By working together, government and industry can leverage scarce resources and develop and share appropriate risk mitigation techniques.

It bears repeating that the NII is being designed, built, owned, and operated by private citizens and private organizations. And security, like other aspects of the NII, will be developed, built, and used by the private sector. Based on the Forum's study, it is apparent that the private sector is already addressing many of the security needs in response to market demands from the users, most of whom are private sector individuals and organizations. As for its role, the Security Issues Forum has not yet assessed its future direction, whether for instance it will take another snapshot of NII security needs. But, before the Forum moves on to new endeavors, much is needed from the member agencies in the way of follow-through on the action items first identified in the draft report and restated in this final. At this point, follow-through is the number one task.

Appendix A

Where We Are Today on Specific Federal Actions

The draft report presented 25 specific actions for the federal government in supporting a secure NII. While this appendix restates the original text of each of those action items, the progress reported here includes examples of complimentary private sector initiatives that make the call for exclusive government action less compelling. Each of these actions are within the framework of the four main activities mentioned in the body of the report. The first three of those activities involve the government's responsibilities to ensure the sound development and use of the NII and the fourth is the government's responsibility as a user of the NII.

First, the Federal government will serve as a facilitator and a catalyst for promoting private sector activity. Second, in its role as guardian of the public interest and general welfare, the Federal government will cooperate with other governments, the private sector, and the public-at-large in setting legal and policy ground rules for security in the NII. Third, the Federal government can support the private sector's development of needed technology by funding research and development in critical areas. Fourth, as a model user of the NII, the Federal government has a responsibility to ensure that its own automated information is secure.

Facilitator and Catalyst

As facilitator and catalyst for private sector activity, the Federal government will:

1. adopt the NII Security Tenets and the OECD Security Principles for use on the NII;
2. stimulate dialogue and awareness about security risks, needs, and solutions;
3. make Federal security products and techniques available for use in the NII; and
4. promote private sector development of high quality security products and services.

1. Adopt the NII Security Tenets and the OECD Security Principles for use on the NII.

Sound security must be based on a common understanding of what is entailed. The NII Security Tenets previously proposed and the internationally-recognized OECD Security Principles [Appendix B] form a solid foundation for developing security products, services, and practices on the NII and internationally. Furthermore, security is needed to protect privacy and intellectual property rights. Principles on privacy and on intellectual property rights have been released by both the U.S. Advisory Council on the NII and by the Information Infrastructure Task Force.

Action 1: Promulgate the Tenets and Principles in the final version of this report.

Where we are today: The tenets and principles are hereby adopted.

2. Stimulate dialogue and awareness about security risks, needs, and solutions. As a facilitator and catalyst, the government will stimulate dialogue and awareness of security risks, needs, and solutions. The series of public meetings co-sponsored by the Security Issues Forum

Appendix A

and members of the NII Advisory Council was the beginning of an on-going dialogue concerning NII security. This report is designed to continue that dialogue.

As the NII interconnects U.S. participants into a global information infrastructure, it introduces new threats to U.S. systems and information. Some of these threats (e.g., sophisticated "crackers" in a foreign country) may be difficult for individual participants to fully perceive. In the course of its international relations, the Federal government may learn about the prevalence and magnitude of this type of threat. This information should be shared with participants in the NII.

During the public meetings, an area of considerable discussion concerned assuring appropriate behavior on the part of participants in the NII. One part of that discussion focused on the point that many of those who break into others' systems believe such behavior is acceptable. To begin countering this incorrect perception, it has been suggested that the Federal government should promote the notion of ethical computing in educational courses.

Action 2: Develop data on threat and risk assessment for the NII and appropriately make it available to the public. Promote awareness of the existence of different threats to the NII with an understanding that there is no "one size fits all" solution, and that different threats must be treated differently within the overall context of managed risk..

Where we are today: These are continuing efforts within government and the private sector, specific examples include:

- A report by the Office of Science and Technology Policy, "Cybernation: The American Infrastructure in the Information Age," is a primer on risks and reliability and provides a framework for a common understanding of the technical and policy challenges inherent in today's network reliability issues. Contact the Office of Science and Technology Policy at (202) 395-7347 for more information.
- Three reports from the Reliability and Vulnerability Working Group of the Telecommunications Policy Committee: "National Information Infrastructure Risk Assessment, A Nation's Information at Risk;" the "NII Blueprint for Action;" and the "NII Capability Assessment" are especially noteworthy. These reports are available at the National Communications System Website (http://www.ncs.gov/n5_hp/html/rvwgdocs.htm).
- The National Institute of Standards and Technology's Computer Security Resource Clearinghouse Website (<http://csrc.ncsl.nist.gov/>) provides up-to-date information on common criteria for information technology security and reports alerts and notifications from the Federal Computer Incident Response Capability (FedCIRC) and Forum of Incident Response and Security Teams (FIRST). Also available at their Website is NIST Special Publication 800-14, "Generally Acceptable Principles for Securing Information Technology Systems."

Appendix A

- The President's Commission on Critical Infrastructure Protection is looking at threats to and vulnerabilities of the Nation's information and other critical infrastructures and will report its findings and recommendations to the President in the fall of 1997. The Commission may be contacted by mail at P.O. Box 46258, Washington, D.C. 20050 or e-mail at "comments@pccip.gov" or visit the Commission's Website (<http://www.pccip.gov/pccip/>) for more information.
- While Carnegie-Mellon's Software Engineering Institute's Center for Emergency Response Team (CERT) (<http://www.cert.org>) is the most well know example of Academia's involvement in this area, it limits its focus to Internet issues. There are an increasing number of educational institutions that are addressing information systems security issues in a broader sense. Two such examples are George Mason University's Center for Secure Information Systems, Laboratory for Information Security (<http://www.isse.gmu.edu/~csis/>) and Purdue University's Computer Operations, Audit and Security Technology program (<http://www.cs.purdue.edu/coast/coast.html>).

Action 3: Stimulate dialogue and broad awareness of the national and economic security concerns related to the NII through public meetings and other outreach methods.

Where we are today: There are many ongoing efforts by the private sector, individual government agencies within their normal areas of responsibility, and by multi-agency or specialized groups. Two of note are:

- The Information Security Exploratory Committee hosted by the Information Technology Industry Council is looking at the viability of a private sector organization that could serve as a mechanism for the exchange threat and vulnerability data and thus facilitate development of risk management techniques. For more information, contact the Information Technology Industry Council at 202-626-5735 or isec@itic.nw.dc.us.
- On broad scale are the public outreach efforts and public hearings by the President's Commission on Critical Infrastructure Protection. The Commission may be contacted by mail at P.O. Box 46258, Washington, D.C. 20050 or e-mail at "comments@pccip.gov" or visit the Commission's Website (<http://www.pccip.gov/pccip/>) for more information.

Action 4: Promote educational programs (along with the private sector and state, local, and tribal governments) to teach ethical behavior and awareness of security issues and risks on the NII.

Where we are today:

- Within the Federal government there are many developing activities such as the National Institute of Standards and Technology's Computer Security Resource Clearinghouse Website (<http://csrc.ncsl.nist.gov/>); a fledgling Federal employee security education

Appendix A

Website that will be managed by the Department of Education known as the Interagency Information Technology Security Institute; and, although chartered to address classified national security information systems, the National Security Telecommunications and Information Systems Security Committee is developing an education, training and awareness Website for both national security and unclassified systems security.

- Within Academia, there are a number of examples of this developing educational discipline. Two examples are George Mason University's Center for Secure Information Systems, Laboratory for Information Security (<http://www.isse.gmu.edu/~csis/>) and Purdue University's Computer Operations, Audit and Security Technology program (<http://www.cs.purdue.edu/coast/coast.html>).

Action 5: Address the issue of minors gaining access to adult materials on the NII.

Where we are today:

- This is an especially volatile issue that mixes free speech and privacy issues with child protection efforts. The Communication Decency Act was enacted by Congress, signed into law by the President, held to be unconstitutional by the U.S. Supreme Court. In the meantime, the marketplace is developing and selling various software products that screen or block incoming material as deemed inappropriate by the individual consumer. On July 16, 1997, President Clinton and Vice President Gore announced a strategy designed to give parents and teachers the tools they need to prevent children from getting access to inappropriate material on the Internet, and to guide them towards high-quality educational resources. For more information on this cooperative strategy, visit the Internet Parents Organization Website (<http://www.netparents.org/>).

3. Make Federal security products and techniques available for use in the NII. To the extent it is necessary, as facilitator and catalyst, government will make Federal security products and techniques available to users of the NII. This report recognizes that strong, effective security is important to users of the NII in protecting their information. In the past, when private sector products were not available, the Federal government has developed security products for its own use that other NII users have found useful (e.g., the Data Encryption Standard (Federal Information Processing Standard Publication 46), became a worldwide standard for protecting financial information on the world's banking system and the Digital Signature Standard (Federal Information Processing Standard Publication 186), provides a means of assuring the integrity of electronic documents and the authenticity of the sender). For the future, the extent to which the government will find it necessary to develop technologies for its own use will depend on a variety of factors such as the availability of commercial products to meet government's own needs. Similarly, it remains to be seen whether the private sector will use government products for commercial use. At least one thing is clear, the government does not intend to mandate security products for private sector use, but instead to depend on the marketplace to select those

Appendix A

products that best meet the needs of the various NII participants.

Action 6: Compile a list of security technologies developed for or used by the Federal government, evaluate them for appropriate and applicable use in the private sector, and make them generally available to the public.

Where we are today:

- The National Institute of Standards and Technology's Computer Security Resource Clearinghouse Website includes up-to-date information on tools and technologies (<http://csrc.ncsl.nist.gov/>). Although in its infancy, this effort is entirely consistent with a recommendation in a report from the Information Infrastructure Task Force's Technology Policy Working Group to create such a government clearinghouse. See the working group's report at the IITF Website (http://nii.nist.gov/pubs/sec_task_rpt.html) for more information. The working group based their recommendation on a report prepared by the Cross Industry Working Team, "A Process for Information Technology Policy: An XIWT Report on Industry-Government Cooperation for Effective Public Policy," which is available at their Website (<http://WWW.CNRI.Reston.VA.US:3000/XIWT/>).
- 4. Promote private sector development of high quality security products and services. NII users are demanding high quality security products and services. Flexible and responsive standards and accreditation processes can assist in the development of those products and as facilitator and catalyst, the government should promote private sector development of high quality security products and services.

However, some security products may provide confidentiality of information that is so strong that it can frustrate law enforcement's authorized ability to listen to communications where criminal activity is suspected. As Vice President Gore has written:

"The Administration has committed itself to cooperating with industry representatives and privacy advocates towards the goal of developing a key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address national security needs as well. Such a system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be exportable. . . .

We also recognize that a new key escrow encryption system must permit the use of private-sector key escrow agents as one option. It is also possible that as key escrow encryption technology spreads, companies may establish layered escrow services for their own products. Having a number of escrow agents would give individuals and businesses more choices and flexibility in meeting their needs for secure communications." (Letter to Representative Maria Cantwell and others, July 20, 1994)

Appendix A

In addition, the Federal government has for years regulated the export of products based on critical technologies for national security reasons. Although the U.S. has relaxed many of its export controls for advanced computing and communications technologies, certain encryption technologies remain restricted. Nevertheless, the U.S. has committed to allowing the overseas use of encryption for personal use by Americans.

Action 7: Promote the development of private certification processes through private, nationally and internationally recognized entities such as the American National Standards Institute, the International Standards Organization, nationally recognized testing laboratories, Underwriter's Laboratories, and other private sector communities of interest, such as the health, entertainment, and financial sectors.

Where we are today:

- As expected, the marketplace is performing this function and some are considering whether an organized private sector effort for voluntary accreditation of products, services and organizations or bodies is desirable. One notable effort -- the Information Security Exploratory Committee -- is being hosted by the Information Technology Industry Council and is looking at the viability of a private sector organization that could exchange threat and vulnerability data as well as evaluate and perhaps certify private sector products and processes. The Committee is basing its analysis on a conceptual model developed by the President's National Security Telecommunications Advisory Committee. More information about this effort may be found on the Information Technology Industry Council's Website (<http://www.itic.org/isec.htm>) or by calling them at 202-626-5735. Without endorsing particular products or organizations, the Forum certainly encourages this process to continue.
- The National Computer Security Association is undertaking a number of certification and coordinating functions for its 3,000 members. See the NCSA Website at <http://www.ncsa.com> for more information.

Action 8: Continue to work with industry to develop alternative key escrow technologies, to make available standards and technology for public use, to develop methods for providing compatibility among different key escrow technologies, and to consider ways to promote use of such technologies overseas.

Where we are today:

- In May 1997 the National Institute of Standards and Technology issued a broad agency announcement soliciting proposals for products and services that will demonstrate the viability of an infrastructure for key recovery, which can be used to support data encryption in federal government applications as part of the Key Recovery Demonstration Project. The project involves several government agencies and is an effort to implement, test and evaluate

Appendix A

different key recovery technologies that could be used by both federal agencies and the private sector. More information about the demonstration project and the broad agency announcement is available at the Government Information Technology Services Board Website (<http://gits-sec.dyniet.com>).

- Under the auspices of the Government Information Technology Services Board, there are some 40 pilot projects ongoing as of the writing of this report. For more information contact the Board's Champion for Security and Privacy at the U.S. Department of Treasury, C-126, 1425 New York Avenue, NW, Washington, DC 20220 or call (202) 622-1522 or visit the Board's Website (<http://gits-sec.dyniet.com>).
- Private sector efforts include the Internet Engineering Task Force (IETF) PKIX Working Group (<http://www.ietf.cnri.reston.va.us/>) and the American National Standards Institute (ANSI) X9F Working Group (<http://www.x9.org/>) are developing standards based on the use of X.509 v3 certificates. In addition, the Open Group's Security Program Group is developing an architecture for PKI (<http://www.rdg.opengroup.org/public/tech/security/pki>).

Action 9: Work with industry and the private sector to foster development of a public key infrastructure.

Where we are today:

- In May 1997 the National Institute of Standards and Technology issued a broad agency announcement soliciting proposals for products and services that will demonstrate the viability of an infrastructure for key recovery, which can be used to support data encryption in federal government applications as part of the Key Recovery Demonstration Project. The project involves several government agencies and is an effort to implement, test and evaluate different key recovery technologies that could be used by both federal agencies and the private sector. More information about the demonstration project and the broad agency announcement is available at the Government Information Technology Services Board Website (<http://gits-sec.dyniet.com>).
- Under the auspices of the Government Information Technology Services Board, there are some 40 pilot projects ongoing as of the writing of this report. For more information contact the Board's Champion for Security and Privacy at the U.S. Department of Treasury, C-126, 1425 New York Avenue, NW, Washington, DC 20220 or call (202) 622-1522 or visit the Board's Website (<http://gits-sec.dyniet.com>).
- Private sector efforts include the Internet Engineering Task Force (IETF) PKIX Working Group (<http://www.ietf.cnri.reston.va.us/>) and the American National Standards Institute (ANSI) X9F Working Group (<http://www.x9.org/>) are developing standards based on the use of X.509 v3 certificates. In addition, the Open Group's Security Program Group is developing an architecture for PKI (<http://www.rdg.opengroup.org/public/tech/security/pki>).

Appendix A

Action 10: Encourage the private sector to develop technology vulnerability and risk management guidance in accordance with the requirements for their communities.

Where we are today: It is quite apparent that little is needed in the way of government encouragement to get the private sector to undertake these efforts. A few examples of ongoing activities are:

- The Information Security Exploratory Committee hosted by the Information Technology Industry Council is looking at the viability of a private sector organization that could serve as a mechanism for the exchange threat and vulnerability data and thus facilitate development of risk management techniques. For more information, contact the Information Technology Industry Council at 202-626-5735 or isec@itic.nw.dc.us.
- The National Security Telecommunications Advisory Committee established an Infrastructure Assurance Task Force to conduct risk assessments of the telecommunications infrastructure and the companies that comprise it. The electric power, financial services and transportation sectors are also cooperating with NSTAC to conduct similar risk assessments of those sectors. For further information on NSTAC activities contact the National Communications System at (703) 607-6220 or visit their Website at <http://www.ncs.gov>.
- For more information on private sector activities the Forum recommends visiting the Websites of both the Computer Security Institute (<http://www.gocsi.com/>) and the National Computer Security Association (<http://www.ncsa.com>).

Action 11: Review technology policy for the NII to ensure support for cooperative Federal-industry approaches in the development of security technology.

Where we are today: There are many ongoing activities with some examples being:

- Agencies who fund information systems security research have formed the Infosec Research Council to coordinate the research efforts of the members agencies. One of the actions of the group is to provide a continuing and independent assessment of the state of advanced technical areas in need of intensified effort. More information about the Council's activities may be found at their Website (<http://does-is.llnl.gov/irc/>).
- The Network Security Group of the National Security Telecommunications Advisory Committee holds regular research and development exchanges with the private sector to foster the exchange of information on network security, avoid duplication of effort, identify needs and areas for further study. This group is also considering the notion of a joint industry-government information security R&D consortium with the goal of avoiding duplication and helping to develop industry-wide standards on portable access control, secure networking architecture, and reliable recovery methods. For further

Appendix A

information on NSTAC activities contact the National Communications System at (703) 607-6220 or visit their Website at <http://www.ncs.gov>.

- The Financial Services Technology Consortium is conducting a number of government-industry pilots. One pilot on electronic check processing involves the Financial Management Service of the Department of the Treasury, Defense Finance and Accounting Service, the Federal Reserve Boston and three commercial banks. Contact Treasury's Financial Management Service at Liberty Center 401, 14th Street, SW, Washington, DC 20227 for more information.
- One area where government is actively supporting research is in automated intrusion detection. Of note are the numerous projects being supported by the Defense Advanced Research Projects Agency. The Forum finds it significant that this research is being conducted in an open, unclassified environment which will permit sharing the product of the research with those that need it most -- the public. More information on these efforts which involve a host of universities and private business concerns can be found at two DARPA Websites (<http://www.ito.darpa.mil/ResearchAreas96/InfoSurvivability.html>) and (<http://yorktown.dc.isx.com/iso/planning/information.html>). Also watch for an upcoming report from the National Security Telecommunications Advisory Committee's Intrusion Detection Study Group on the state of play in intrusion detection R&D efforts. For further information on NSTAC activities contact the National Communications System at (703) 607-6220 or visit their Website at <http://www.ncs.gov>.
- The Information Infrastructure Task Force's Technology Policy Working Group recommended that the government create a clearinghouse with which the private sector could interact directly on matters involving security technology policy and assist cooperation on development of policy and technology. See the report at the IITF Website (http://nii.nist.gov/pubs/sec_task_rpt.html). The working group based their recommendation on a report prepared by the Cross Industry Working Team, entitled "A Process for Information Technology Policy: An XIWT Report on Industry-Government Cooperation for Effective Public Policy." See the report at the Cross Industry Team's Website (<http://WWW.CNRI.Reston.VA.US:3000/XIWT>).

Action 12: Issue a proposed rule to establish a personal use exemption for overseas use of encryption.

Where we are today:

- This action was completed in February 1996 with the Department of State's Amendment of the International Traffic in Arms Regulations (22 CFR Parts 123 and 126) to exempt the temporary export of cryptographic products for personal use.

Appendix A

Protector of the Public Interest

In its role as protector of the public interest, the government will:

1. assure adequate emergency response capability on the NII;
2. adapt current oversight processes to meet the challenges of the NII;
3. review criminal law; and
4. promote international cooperation.

1. Assure adequate emergency response capability on the NII. Today the Federal government sets priorities and procedures for service on the public switched network in the event of an emergency in order to meet critical communication needs and to assist in an orderly recovery. This role should be extended to establishment of priorities and procedures to support a robust emergency response capability comparable to that provided by CERT, the Computer Emergency Response Team. An extension of this role to assure that priority communications in the NII when emergencies occur will be necessary.

Action 13: Review emergency communications and network services requirements and priorities, to include the Telecommunications Service Priority program, to assure that appropriate priorities for the NII are established in times of emergency.

Where we are today:

- The Telecommunications Service Priority program is a program managed by the National Communications System and assisted by the National Security Telecommunications Advisory Committee. In direct response to proposed action 13, the Telecommunications Service Priority Program System Oversight Committee found the system to be effective to meet today's national security and emergency preparedness telecommunications needs. Regular monitoring ensures that as new technologies are employed, effectiveness will continue. For information on these activities contact the National Communications System at (703) 607-6220 or visit their Website (<http://www.ncs.gov>).
- In July 1997, responding to a Federal Communications Commission tasking, the Network Reliability and Interoperability Council issued a comprehensive report which discusses how to assure the ability of users and information providers to "seamlessly and transparently transmit and receive information between and across telecommunications networks." The key findings and recommendations of the report include detailed discussions regarding security as used in the context of this report. The Council, comprising over 200 technical experts from all parts of the telecommunications industry, stated its belief that competitive market forces, voluntary standards processes and agreements among service providers, equipment suppliers and other participants, should be relied on as the primary vehicles by which to achieve desired results. Visit the FCC Website for the report and more information on the activities of the Council (<http://www.fcc.gov/oet/nric/>).

Appendix A

Action 14: Cooperate with private sector and State, local, and Tribal governments to ensure that vital government and civil infrastructure security needs are being addressed.

Where we are today:

- The President's Commission on Critical Infrastructure Protection is looking at threats to and vulnerabilities of the Nation's information and other critical infrastructures (including essential government services) and will report its findings and recommendations to the President in the fall of 1997. The Commission may be contacted by mail at P.O. Box 46258, Washington, D.C. 20050. For more information see the Commission's Website (<http://www.pccip.gov/pccip/>).
- 2. Adapt current oversight processes to meet the challenges of the NII. The government does not regulate the NII as a whole, although it does regulate different pieces, including providers such as common carriers and users such as financial institutions. As discussed above, virtually every sector of the economy, from health care to aviation, is growing to depend on the NII. Security failures in the supporting information infrastructure could jeopardize the U.S. economic well-being, national security, and public safety. Thus the current oversight processes must be adapted to meet the challenges of the NII.

Action 15: Examine whether current banking regulations are adequate in the areas of electronic banking, electronic payment systems, and "digital cash," in order, for example, to protect consumers from counterfeiting and fraud.

Where we are today: This is a continuing process with the following being of note:

- In September 1996 the Department of Treasury held a two-day conference, "Toward Electronic Money and Banking: The Role of Government." In addition to issues regarding e-money payment systems and the perspectives of issuers, the conference covered privacy, security, authentication, and other consumer issues. A conference paper "An Introduction to Electronic Money Issues" and conference proceedings are available at the Office of the Comptroller of the Currency Website (<http://www.occ.treas.gov/>).
- At the Office of the Comptroller of the Currency Website (<http://www.occ.treas.gov/>) is a description of the activities of the Consumer Electronic Payments Task Force, an intra-Treasury effort to look at issues affecting consumers as a result of emerging electronic money and the extent to which they are addressed by existing state and federal laws, regulations, and voluntary industry guidelines.
- The Financial Crimes Enforcement Network (FinCEN) is coordinating the Department of Treasury's law enforcement efforts regarding electronic banking and payment systems and e-money. They have formed a Treasury E-money Council and an International Financial Activities Task Force to look at global money laundering. For more

Appendix A

information see the FinCEN Website (<http://www.ustreas.gov/treasury/bureaus/fincen/>).

- The Federal Reserve Board and the Reserve Banks continue to be active in this area. For example, in March the Board submitted a report to Congress concerning the availability of consumer information and its relationship to financial fraud and in September, the Federal Reserve Bank New York released a report for commercial banks, "Sound Practices Security Guidance on Information Security." These reports are available on their respective Websites (<http://www.bog.frb.fed.us/> and <http://www.ny.frb.org>).

Action 16: Ensure that all Federal agencies evaluate their current oversight mechanisms and practices in light of the growing need to address the growing dependence on the NII.

Where we are today: Continuing.

3. Review criminal law. A review of current law is timely, particularly in the areas of intellectual property rights and computer crime. The Federal government has such reviews underway and will propose its views for public discussion in mid-1995. For example, the Intellectual Property Rights Working Group has proposed that selling software designed to defeat copy protection of copyrighted materials be deemed contributory infringement under the Copyright Act. The Federal government will continue to work with private sector and State, local, and Tribal governments to ensure that proposed changes in criminal law are appropriate.

Action 17: Propose legislation to enable prosecution of computer-related crime.

Where we are today: Continuing as needed, specific actions taken include:

- The President has signed into law the National Information Infrastructure Protection Act of 1996 which closes apparent gaps in the Computer Fraud and Abuse Act of 1984. Among other things, this statute makes it a Federal crime to improperly access a Federal computer or any computer used in interstate or foreign commerce, including to damage, inflict a virus or otherwise stall operations.
- The President has signed into law the Economic Espionage Act of 1996. This statute makes it a Federal crime to steal, possess or copy a trade secret without authorization with increased penalties for violations that are intended to benefit a foreign government.

4. Promote international cooperation. In recognition of the increasingly global nature of the information infrastructure, the U.S. has been active in putting computer and communications security issues on the table in international fora. At the G-7 Ministerial Conference on the Information Society in Brussels in February 1995, the U.S. proposed, and the G-7 partners agreed, to increase efforts to find creative, technological and policy solutions to increase "the reliability and security of national and international networks . . . by developing security principles that are commensurate with the risk and magnitude of harm." The OECD has been a

Appendix A

leading international organization in the area of information and communications security.

Action 18: Stimulate consideration of security issues at the OECD and other international fora.

Where we are today: Continuing.

Promote Research and Development in Critical and High Risk Areas

Although the private sector will continue to respond to market pressures and opportunities to create technical security products, services, and techniques, there may be a need for government to encourage private sector research and development in high risk or critical technologies. Some technologies developed by the government which are suitable for adaption for industry applications sector may become available through technology transfer programs. In other situations, government supports the private sector through funding pre-commercial, pre-competitive technology through various grant programs, cooperative research and development agreements, and other technology development programs. For example, the Defense Advanced Research Projects Agency and the NIST Advanced Technology Program are currently funding research into advanced technology that could be used to support an automated copy management system.

Action 19: Promote research and development through the High Performance Computing and Communications Program, DARPA, NIST, and others, of security technology that supports agencies' missions.

Where we are today:

- In May 1997 the National Institute of Standards and Technology issued a broad agency announcement soliciting proposals for products and services that will demonstrate the viability of an infrastructure for key recovery, which can be used to support data encryption in federal government applications as part of the Key Recovery Demonstration Project. The project involves several government agencies and is an effort to implement, test and evaluate different key recovery technologies that could be used by both federal agencies and the private sector. More information about the demonstration project and the broad agency announcement is available at the Government Information Technology Services Board Website (<http://gits-sec.dyniet.com>).
- In 1996 DARPA initiated a four-year research effort in information survivability to develop technologies that could be used to protect the information infrastructure. This year, they initiated a related effort for information assurance which aims at furthering the technologies developed in the survivability area and applying them to systems that are attractive commercially while also addressing specific government and defense needs. More information on these efforts which involve a host of universities and private business concerns can be found

Appendix A

at two DARPA Websites (<http://www.ito.darpa.mil/ResearchAreas96/InfoSurvivability.html>) and (<http://yorktown.dc.isx.com/iso/planning/information.html>).

Government as a User

As a user, the government has a responsibility to protect the information in its possession and to act as a model user. Thus, it has the obligation to support all elements of a secure NII as it procures and manages its own portion of the NII.

The Federal government will:

1. protect its own security requirements through good management processes;
2. improve its national security/emergency preparedness capabilities;
3. ensure that the products and services it uses meet its needs; and
4. develop a security infrastructure for its own use.

1. Protect its own security requirements through good management processes. The Computer Security Act of 1987 provides the framework within which Federal agencies will manage the security of the vast majority of their use of the NII. Through that mechanism, they will work to assure the confidentiality, integrity, and availability of their information as they use the NII.

Similarly, the military will use and be dependent on the security and reliability of the NII. This may require using technologies especially designed for government use, such as advanced firewalls and encryption devices.

Action 20: Release final guidance to agencies to assure adequate security of Federal automated information through education, training, and awareness programs across agencies.

Where we are today:

- This action was accomplished in February 1996 with the issuance of the revised OMB Circular A-130, Appendix III. The new Appendix III, "Security of Federal Automated Information Resources," recognizes that security is inherently a management issue with a focus on personnel management to be included as part of an security architecture or system security plan comprising multiple layers. The major ingredients of such an architecture are the rules of the system including expected behavior of the users, training to ensure that users are aware of their responsibilities, personnel security including individual access privileges, incident response capabilities, continuity of support and contingency planning, technical security, system interconnections and information sharing, and public access controls, physical security procedures, etc. OMB Circular A-

Appendix A

130 may be found on the OMB Website (<http://www.whitehouse.gov/WH/EOP/OMB/>).

- As this report is being finalized Congress is considering modifications to the Computer Security Act of 1987. Appropriate agencies are closely following these developments.

Action 21: Continue development of security technologies to support unique government requirements.

Where we are today: Continuing as needed. But, as a general policy matter, agencies should look first to the market place for information technology products and processes of all kinds, including those pertaining to security.

- One example of cross-cutting activities began in 1996 when DARPA initiated a four-year research effort in information survivability to develop technologies that could be used to protect the information infrastructure. This year, they initiated a related effort for information assurance which aims at furthering the technologies developed in the survivability area and applying them to systems that are attractive commercially while also addressing specific government and defense needs. More information on these efforts which involve a host of universities and private business concerns can be found at two DARPA Websites (<http://www.ito.darpa.mil/ResearchAreas96/InfoSurvivability.html>) and (<http://yorktown.dc.isx.com/iso/planning/information.html>).

Action 22: Develop and implement a program to ensure the security of Federal automated information consistent with guidance.

Where we are today: Continuing.

2. Improve its national security/emergency preparedness capabilities. The National Communications System is a government entity that seeks to effect coordination among Federal government agencies and between the government and the telecommunications industry in order to support the government's emergency response mission. Through its efforts to promote the sharing of information between the private sector and government, the NCS promotes greater cooperation in securing networks for both the civil and private sectors.

Action 23: Review and validate national security and emergency preparedness requirements for the nation's information infrastructure.

Where we are today:

- The National Security and Emergency Preparedness Subgroup of the National Communications Systems, in concert with the NSTAC, has reviewed the requirements for the

Appendix A

NII and has identified eight primary features or capabilities that need to be built into the evolving NII to ensure continuity of service. Needed are priority information exchanges, priority service provisioning and restoration procedures, emergency broadcast capabilities, a sustainable coordinating mechanism, assured and reliable service, interoperability, protected information support, network security. For more information on these activities contact the National Communications System at (703) 607-6220 or visit their Website (<http://www.ncs.gov>).

3. Ensure that the products and services it uses meet its needs. The Federal government will adopt voluntary, consensus based standards wherever practicable. Where an appropriate standard developed in the private sector is not available, government will develop a standard for its own use. These standards will be available for other parties to use on voluntary basis. These standards are developed and promulgated by the National Institute of Standards and Technology of the Department of Commerce.

The Federal government has traditionally accredited many of its standards through government laboratories. Increasingly, however, private sector evaluations are encouraged, as in "Security Requirements for Cryptographic Modules" (Federal Information Processing Standards Publication 140-1). The government also publicly issues lists of commercial products that it has accredited for its use.

Action 24: Rely, where possible, on security products which are based on industry standards. However, where commercial security services and standards are insufficient for government's needs in the NII, the government should develop security standards and use products built to those standards.

Where we are today: This is an continuing effort and is indeed now viewed more as a principle and a matter of policy than a specific action item.

4. Develop a security infrastructure for its own use. Under the auspices of the NII Security Issues Forum, the General Services Administration has established a Security Infrastructure Program Management Office. This office is coordinating the development of a public key infrastructure to meet the Federal government's needs for digital signature and confidentiality purposes. The U.S. Postal Service is pursuing complementary efforts.

Action 25: Develop a public key infrastructure for government use. Demonstrate interoperability with multiple agencies and with industry.

Where we are today:

- In May 1997 the National Institute of Standards and Technology issued a broad agency announcement soliciting proposals for products and services that will demonstrate the

Appendix A

viability of an infrastructure for key recovery, which can be used to support data encryption in federal government applications as part of the Key Recovery Demonstration Project. The project involves several government agencies and is an effort to implement, test and evaluate different key recovery technologies that could be used by both federal agencies and the private sector. More information about the demonstration project and the broad agency announcement is available at the Government Information Technology Services Board Website (<http://gits-sec.dyniet.com>).

- Under the auspices of the Government Information Technology Services Board, there are some 40 pilot projects ongoing as of the writing of this report. For more information contact the Board's Champion for Security and Privacy at the U.S. Department of Treasury, C-126, 1425 New York Avenue, NW, Washington, DC 20220 or call (202) 622-1522 or visit the Board's Website (<http://gits-sec.dyniet.com>).
- Private sector efforts include the Internet Engineering Task Force (IETF) PKIX Working Group (<http://www.ietf.cnri.reston.va.us/>) and the American National Standards Institute (ANSI) X9F Working Group (<http://www.x9.org/>) are developing standards based on the use of X.509 v3 certificates. In addition, the Open Group's Security Program Group is developing an architecture for PKI (<http://www.rdg.opengroup.org/public/tech/security/pki>).

Appendix B

**Excerpt from the
Guidelines for the Security of Information Systems
Organisation for Economic Cooperation and Development
26 November 1992**

V. PRINCIPLES

1. Accountability Principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness Principle

In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

3. Ethics Principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary Principle

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

5. Proportionality Principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

Appendix B

6. Integration Principle

Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

7. Timeliness Principle

Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security of information systems.

8. Reassessment Principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy Principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

See the OECD Website for more information about the OECD security guidelines and principals (<http://www.oecd.org/dsti/iccp/legal/secur-en.html#2>).

Appendix C

The Role of Technology in Security of the NII

At the heart of information security in the NII is the technical ability for individuals to protect their information and systems. At every public meeting and in comments received on the draft report, technical approaches in use or being developed to protect systems or information have been discussed. These have varied from techniques being used by firms to protect their intellectual property rights, to protection being designed into systems of electronic cash, to "firewall" techniques for protecting firms' networks when connected to the Internet. These discussions indicated that the marketplace, to the extent that users are demanding security, is responding with both specific security products as well as general NII products and services that incorporate security protection.

At the same time, the security technology challenges of the NII are formidable. Information and services will need to be protected, yet also available to communities of interest. Much of the technology that will be used to provide security in future use of the NII is yet to be developed. The discussion that follows summarizes today's technological approaches to security, identified during the Forum's activities and by its member agencies during the course of their business operations. It should not be read as a complete description of the security technology needs of the NII, nor to minimize the complexity of fulfilling those needs.

The many products and techniques that exist approach security from one of two principal strategies -- protecting a system from outside attack (e.g., firewalls), or protecting the information itself regardless of where it resides, normally through some form of cryptography. In addition, the networks themselves should be protected.

Protecting Systems

Technical security measures have traditionally focused on controlling access to the system. As today's processing environment becomes more open, however, that task becomes significantly more difficult.

Participants in the public meetings demonstrated an understanding of a wide array of technical security techniques used to protect their systems. Moreover, a consensus view emerged that incentives exist for the marketplace to provide appropriate security techniques. A number of participants expressed surprise that the government was taking an interest in this issue, other than as a user. Most felt that their technical security needs would be satisfactorily addressed by the private sector.

Appendix C

1. Access Control

Today, individual access to and accountability on systems is controlled largely by password management. That is, an individual is required to identify some unique piece of information known only to the individual and the system in order to identify himself to the system. Over the years, password schemes have become more complex to make systems more secure, and the ability of those trying to penetrate systems by obtaining passwords has become substantially better. For example, a large number of sophisticated password "sniffers" -- software programs designed to capture passwords as they are sent across hosts -- are widely available on the Internet.

Stronger schemes for protecting systems include timed password-changing mechanisms. These mechanisms change acceptable passwords at timed intervals previously agreed upon between the system and a device held by individuals desiring to remotely access the network. Other methods are being developed to substitute for password schemes. They identify individuals to a system by the rhythm of their keystrokes or by biometrics such as fingerprints or a retinal scan.

2. Secure Gateways

Secure gateways or "firewalls" help protect systems by limiting outside access to internal system capabilities. Despite recent publicity about break-ins, strong technical measures exist that afford protection. Where break-ins have occurred, they have usually exploited known weaknesses in a software version which have not been fixed, even though fixes are readily available.

A different concern is the need to block the reception of unwanted information. A large volume of unwanted messages could, for example, overwhelm a receiver's ability to handle them and effectively shut the system down.

Individuals and organizations are responsible for making reasonable efforts to secure their own systems in the same way they have a responsibility to lock their doors to deter burglars from entering. Private sector firms are responding to the need for secure gateways by developing increasingly sophisticated commercial products. However, like seat belts in cars, they only work when they are used.

3. Protecting Networks

Related to the security of systems is the security of networks. Networks, comprising a variety of technologies, are what connect systems with each other. The most common threats to networks concern breakdowns in their availability and reliability, resulting in slow or noisy

Appendix C

connections, network outages, or loss of data. These threats can be caused by natural disasters such as fires, floods, or earthquakes, but also could include a physical attack, such as a bomb, or an electronic attack, such as a virus. Procedural errors such as design errors, software bugs, and operational mistakes can also place a network at risk.

Basic physical security precautions can help, such as fire protection systems and doors with locks. Back-up equipment enables a network provider to quickly restore service, while quality assurance software can minimize design errors, and technical security measures can warn about an impending breakdown or prevent an outage or loss of data.

Protecting Information

Protecting information requires different technology than protecting a system. Once information is outside a controlled system, the owner has little control over who can gain access to it. Therefore, technology which can provide assurance that information itself cannot be read, copied, or modified is critically important in an open processing environment such as the NII.

Cryptographic mechanisms already widely used are unique in that they directly protect information from being compromised or altered without authorization. Cryptography is used by banks to assure the integrity of financial transactions, by computer operating systems to conceal passwords, by users of the Internet to protect the privacy and confidentiality of their communications, and by holders of smart cards to protect information contained on the card. There is no doubt that in the future there will be widespread use of this technology, which will be virtually transparent to end-users. Cryptography is also used in other security services, such as digital signatures and passwords.

Many hurdles remain to easy use of cryptography. For example, one problem is the awkwardness of handling encrypted information. Also, the lack of a public key infrastructure makes it difficult for individuals and organizations to manage keys efficiently. Another factor which has limited cryptography is the risk of unmanaged cryptography for business -- whether it be a disgruntled employee who encrypts corporate financial records before departing, an employee who is absent when critical files are needed, or merely someone who forgets the keys. Finally, the lack of agreement on cryptographic standards is slowing the proliferation of cryptography.

1. Confidentiality

Cryptography is essential to protecting the confidentiality of automated information. It provides the protection of information being undecipherable, even if someone gains access to it. It is this use that crystallizes a conflict between citizens' needs to protect confidential information and the societal need for justice and safety. Strong cryptography can be used to thwart law

Appendix C

enforcement's legitimate ability to understand the contents of lawful wiretaps. On the other hand, weak cryptography will not provide effective protection of confidentiality of citizens' sensitive communications and data.

A number of alternative approaches to resolve this dilemma are being proposed. Many involve an emergency key recovery approach whereby, keys to strong encryption are held by a trusted party (such as a bank or in some cases, a party internal to the user's organization). Under this approach, the keys would be provided to law enforcement authorities upon presentation of a duly-executed wiretap warrant. Some of these approaches could also assist firms in recovering lost data, where, for example, a key has been lost. Private sector approaches being developed to meet the needs of corporate key recovery may also benefit government, both as a user and in its law enforcement responsibilities. The ultimate solution will be market-driven.

As a user, government has its own needs for security. In 1993, the government introduced and fielded a technology for the protection of its own voice and low-speed telephonic data communications. The use of this technology, known as the Escrowed Encryption Standard, or "Clipper" chip was optional for U.S. government agencies and was also made available for voluntary use by the private sector, but domestically individuals could continue to choose to use any encryption technique they chose.

The private sector reacted strongly to this initiative, objecting to the key escrow feature, to the fact that the technology is hardware-based, and to its use of a classified algorithm. However, the technology gave the government no new authority or abilities. In the body of this report is a progress report on encryption policy.

2. Digital Signatures

In an open digital environment, verifying the source of a message or document and assuring that it has not been changed was mentioned as a concern in a number of different meetings. For example, in electronic payments there is concern that the correct payment is made to the correct individual. As noted at the meetings, the private sector is actively working on providing this capability and assuring effective protection. The underlying technology for such protection is digital signature.

A digital signature is created by applying an encryption algorithm to the information, resulting in a unique "signature" associated with the information. This signature is encrypted and sent with the information, which may or may not itself be encrypted. By verifying the signature and comparing it with the information, the receiver can verify that the contents of the message were not altered in transit. Of course, such a technique does not prevent or correct alterations, it only detects them.

Appendix C

While there are a number of different technical approaches to digital signatures, two are prevalent in the current environment. One, based on the RSA encryption algorithm, is coming into wide use in the private sector. A second, based on the El Gamal algorithm, has been adopted as the Federal standard for signature and is coming into use in the Federal government. Both require a public key infrastructure to provide a trusted third party, which will allow verification that the signer of a given document is indeed who he or she claims to be.

3. Public Key Infrastructure

In tomorrow's open networks, cryptography will help to verify the identity of a message sender, assure the integrity of a message, and protect information from unauthorized readers. Without some means of verifying where and to whom their information is going, people may hesitate to do business electronically. A Public Key Infrastructure (PKI) uses two keys, one public, like a phone number, and the other private, like a personal identification number (PIN) or password. The public key is listed in a public electronic directory, while the private key is kept secret by the individual.

The primary application of a PKI is to verify the identity of a message sender through creation of a digital signature. To create a digital signature, a sender of information uses her private key to sign the message. The receiver uses the sender's public key to verify the signature.

A PKI can also support confidentiality of messages. A sender of information obtains the receiver's public key and encrypts the data. The receiver uses his private key to decrypt the information.

A public key infrastructure has great potential to encourage new activity on the NII because it provides a means to do business among parties without prior arrangements. For example, a mail order company posts its public key in an on-line catalogue. Customers send in their order with their credit card number in encrypted format. The company uses its private key to decrypt the information.

Appendix D

Oversight and Enforcement

There is a need for effective law and oversight of both the NII itself and of public safety-related uses of the NII. A sound legal system that applies civil remedies and criminal penalties is essential to fulfilling this need. In the public meetings, participants focused primarily on civil remedies and litigation, rather than criminal issues. In addition, considerable activity is occurring in State, local, and Tribal governments, particularly regarding criminal computer law.

1. Law and Regulation

Various activities are overseen by government because they affect the well-being of the nation. For example, some sectors of the economy are regulated to ensure the public health or safety. As these activities become increasingly reliant upon the NII for communications and information, a security weakness in the NII can become a threat to the public health or safety. To effectively manage risk in their public safety oversight role, Federal agencies will need to ensure the secure use of the NII by their overseen sector. Thus, for example, the Transportation Department may need to adjust its regulatory oversight of aircraft to account for the risks involved in aircraft's use of the NII. Similarly, the Securities and Exchange Commission may need to adapt its oversight of securities exchanges, and the Treasury Department and the Federal Reserve Board their oversight of the nation's banking system.

2. Civil Law

Civil litigation includes specialized or statutory suits, contract actions, tort actions, and injunctive relief. Several participants in the meetings stated that issues of liability must be resolved before widespread use of the NII occurs. In reality, however, a range of accepted solutions and practices concerning information security will be decided in increments through the court system as a body of case law develops over time.

Civil law addresses the issue of liability. In every public meeting, users and providers of NII services questioned how the current system of liability for damages would affect their use. For instance, concerns were raised that unknown exposure to liability could prevent potential providers from offering services.

Specialized suits can be used to protect intellectual property rights against copyright, patent and trademark infringement, or other violations of established statutory rights. Whether a particular statute extends to activities on the NII when Congress did not specify the statute's application in a networked environment may be subject to litigation on a case-by-case basis.

Contract actions are law suits contesting provisions in express or implied contracts. Tort actions resolve disputes for money damages alleging a breach of a duty which caused harm to the

Appendix D

plaintiff. Injunctions involve obtaining a court order to prevent specific actions or require certain activities. For example, such an order might prohibit use of the Internet in a certain way or require a user to make certain disclosures before using the Internet. Other forms of civil action and novel theories of liability involving all aspects of the NII continue to evolve.

Civil liability is likely to create incentives for improving security of information systems.¹ If users, system managers, and service providers face liability in contract for failure to perform a contractual duty, or liability in tort for negligence, they will have an incentive to take reasonable steps to secure their systems, ensure accuracy of their data, and limit unauthorized access and use. A presenter at one public meeting noted that some private parties currently protect their proprietary information by simply not putting it on networks. Attaching legal consequences for the unauthorized or improper use of electronic data will increase the likelihood that the NII will be a trustworthy, reliable system.

Courts are beginning to be confronted with cases that test the effects that civil liability practices will have on the security of the NII. Until a settled body of law develops, various parties' responsibilities and potential liability for negligent security will be uncertain. Legislation that would impose criminal and/or civil penalties for security violations such as blocking, tampering, masquerading, or denying service in the network environment is, of course, possible. However, consensus about what constitute reasonable standards for information security will be difficult to achieve. Because security requirements greatly vary in different contexts, such as finance, law enforcement, medicine, national security, research, and education, there may be a need for context-specific standards that can evolve as requirements change.

3. Criminal Law

Traditionally, laws have focused explicitly on the computer, since it could be easily recognized as the venue where a crime occurred. The laws were intended to protect the information contained in computers. Technology, however, has evolved so that proscribing conduct with regard to computers does not adequately protect information. Today, information can be intercepted and modified in transit between computers, or when it is present in devices not typically thought of as computers, such as telephones, cable systems, satellite and cellular channels, etc.

Many actions that would compromise security of the NII are already criminal violations.

¹ Lost or scrambled files, system downtime, invasion of privacy, and economic or physical injury can be foreseen as a result of sloppy security of networks. For example, liability for system managers can be envisioned for failure to enforce password expiration, eliminate access by former employees, replace default configurations, or implement technical solutions to prevent or reduce breaches in security.

Appendix D

For example, it is illegal to conduct a wiretap without a court order. Fraud, whether perpetrated electronically or not, is a criminal offense. In other areas, laws may need to be amended.

Legislative efforts to protect computers and information suffer, on the one hand, from having to exhaustively yet clearly define these terms in order to make the laws meaningful. On the other hand, the laws must be sufficiently broad and adaptable that the statute will not be rendered obsolete by rapid technological change.

In order for the NII to be secure, laws must be enforceable. Hence, law enforcement officials such as police officers must maintain the ability to enforce laws effectively in it. Future crimes are likely to be planned and coordinated using the NII. The NII will also be used by criminals to smuggle stolen corporate information, engage in the transmission of child pornography, engage in industrial sabotage, or electronically stalk, terrorize, or threaten other NII users. In all of these cases, law enforcement must be able to protect citizens.

4. International Issues

International computer offenses are easier to commit than traditional international crimes, because they do not necessarily require additional manpower or physical transportation. Someone can ship information covertly via telephone and data networks. They need no passport and pass no checkpoint, but cross borders simply by typing a command.

Second, computer crime has not received the emphasis given other international crimes. Until relatively recently the United States, probably the most computerized nation, has not mobilized against computer criminals, even though it is the frequent target of such computerized attacks. Although the U.S. now recognizes the seriousness of the threat, it is not surprising that less computerized countries do not yet fully share this awareness and some have weak or no laws against breaking into computers. Those with strong laws find it difficult to engage in fruitful cooperation with those without.

In order to improve international cooperation in the prosecution of computer crimes, the United States has joined international efforts to raise public consciousness about computer crime and encourage other countries to enact or strengthen their computer crime laws. In fact, other countries have been working both domestically and internationally in this area, particularly Denmark, England, Australia and Germany.

Consistent with this international effort, the Organization for Economic Cooperation and Development's Guidelines for the Security of Information Systems require prompt assistance by all parties in cases where information security has been breached. Additionally, the Council of Europe is currently addressing procedural problems that arise in information technology crimes, such as how to quickly get international trap and trace information.

Appendix E

The First Public Meetings: Provider and User Security Concerns

The first public meetings solicited discussion with a broad range of NII participants, both users and providers of NII services. Regardless of the commercial, industrial, or public interest use represented, the participants shared a number of concerns. These concerns included: the potential inability to control secondary uses of information; questions of liability for loss or inappropriate access to or use of information; a mistrust of government's use of information; the desire to protect one's own system from outsiders, whether by hostile attacks or junk mail; and risk of system failure at times of critical need. The most-heard concern was that personal information, such as information pertaining to an individual's finances, health, or purchasing habits, could be disclosed to or manipulated by an unauthorized user. These shared concerns were generalized in developing the security tenets described above.

In addition, some participants seemed to desire a greater government role, such as censorship of defamatory or pornographic information transmitted over the NII, or additional funding for national security and emergency preparedness programs. Other participants seemed to desire a lesser government role. For example, some participants desired open access to and use of virtually all information and systems without interference. Other participants criticized the Federal government's export control policy, which limits the export of powerful cryptographic systems.

Still others were suspicious of the technology underlying the NII and how it would be used. Some witnesses were also concerned that government's involvement could create greater inefficiencies, increase susceptibility to invasions of privacy and risk of fraud, and contribute to the depersonalization of society.

The following summarize the concerns and needs heard at each of the public meetings. Transcripts are available on the IITF Website (<http://www.iitf.nist.gov>.)

1. Entertainment, Software, and Computer Services

Images, movies, music, software, and a variety of products that can be transmitted in digital form can be easily altered or copied. The protection of intellectual property rights in an electronic age requires technology, legal protection, and institutions that promote fair use, support licensing and payment, and prevent unauthorized copying, alteration, or distribution. There was considerable discussion about effective legal protection and institutions. A thorough treatment of intellectual property on the NII will be found in the IITF White Paper. The report was issued in June, 1995 and is available at the U.S. Patent and Trademark Office Website (<http://www.uspto.gov/web/offices/com/doc/ipnii/>).

Appendix E

A number of possible technological approaches were described at the meeting, including software that is programmed to be disabled after a span of time if the software is not paid for. Another technique described was to distribute an encrypted movie with a key that can decrypt it (for viewing) one time only. One intellectual property entrepreneur electronically distributed his work -- visual images -- in encrypted form and then sold the decryption key through the regular mail. This solution allowed him to distribute digital images electronically, but it did not prevent the buyer from redistributing the work after they decrypted it. Generally, participants indicated that adequate technical capability was being developed to protect their own products. Technical challenges remain, however, including the need for an automated copyright management system for digital works. In addition, several witnesses raised a concern about government barriers to the development and sale of technologies such as export control laws.

2. Health and Education Information and Services

Health care will be improved by computer-based patient records, on-line databases, consumer health information, and remote treatment and advice. However, improved access to information also brings with it a risk of improper disclosure, alteration, or use of highly personal information. Patients' well-being will become dependent on the integrity and reliability of such information in the NII. In particular, the reliability of such computerized medical records systems will be of critical importance as the health care system shifts away from paper. Similarly, educational records can have a substantial effect on individuals' economic well-being.

Participants suggested that the technology will need to promote information integrity, and to ensure that access is provided on a need to know basis, that records that serve different functions are separated, and that the records are destroyed when they no longer serve their function. Concern was also raised about the availability of pornographic material on the Internet and the need to protect children from exposure to it.

3. Financial, Insurance, and Commercial Services

The financial and insurance sectors have relied for decades on closed networks in order to reliably transfer funds and share information. As their networks become more open, new security tools and techniques will be needed to protect the confidentiality and integrity of valuable commercial information. Questions of liability will also arise if improper disclosure of customer information occurs while it is being transmitted over the public switched network.

As consumers use the NII to conduct business, they will want to verify that a payment or order was received correctly. Without a face-to-face transaction to verify the authenticity of the customer and of the vendor, the potential for fraud increases for both parties, requiring methods of electronic notarization, digital signatures, and date-stamping.

Appendix E

The advent of so-called digital cash involves a different challenge. It requires a technical method to avoid forgery and authenticate the current owner. On the other hand, some witnesses favored the ability to anonymously execute transactions. A number of products are already being tested to provide "electronic cash" on the NII.

One witness pointed out that the vast majority of technical solutions address the issue of protecting an organization's data from individuals, while little attention has been paid to the problem of how the individual's data can be protected from organizations. This situation is illustrated by the way in which data about an individual's purchasing habits is bought and sold in private markets. Other personal information which is generally publicly available, such as marital status, home ownership, and status in legal proceedings, is collected by the private sector and sold as a commodity. Some individuals expressed a desire to exercise greater control over the use of this information, or to be reimbursed for its use. The IITF's Privacy Working Group has developed principles to guide policy development in this area. See these principles at the IITF Website (<http://www.iitf.nist.gov/ipc>).

4. Intelligent Transportation

Intelligent transportation systems include applications such as electronic toll collection, in which a toll payment is automatically deducted from a card with a computer chip so that cars won't have to stop as they pass through toll booths. Such systems may also help monitor traffic patterns and road conditions through cameras or other sensors, and provide drivers with information in their cars about the quickest route.

A basic security concern with electronic toll collection is funds control and integrity. In addition, there are concerns that the information collected in these transactions, including information about the owner of the vehicle, how fast he or she was driving, and where he or she was headed, could be used inappropriately. Access to this information could disclose commercial proprietary information or compromise personal privacy. Furthermore, as transportation becomes more dependent on automated control systems, the movement of people becomes subject to security risks. For example, a security breach could allow mischief such as switching all the traffic lights to green, thus promoting accidents.

5. Government Information and Services

Use of the NII is becoming integral to virtually every Federal program, and Federal agencies are becoming dependent upon that use for execution of their missions. The NII will support programs as varied as air traffic control, compilation of the decennial census, response to natural disasters, and delivery of social security benefits.

Appendix E

This use of the NII in Federal operations promises improved efficiency of governmental program delivery. However, it also introduces new and varied security vulnerabilities, not unlike those faced by other users of the NII. The difference, of course, is that addressing these security vulnerabilities is a direct responsibility of the Federal government, since such vulnerabilities could degrade Federal program effectiveness and resource safeguards, and affect the integrity, confidentiality, and/or availability of government information.

At the meeting, the use of "smart cards" or electronic debit cards for delivering food stamps was discussed in depth. Smart cards provide the advantage of on-time payment, increased dignity, and improved efficiency in program administration. However, cards can be lost, and there are opportunities for fraud by converting the credits to cash. Other concerns include the potential for counterfeiting such cards or otherwise manipulating the value of the cards. Unauthorized access to individual purchasing records could violate personal privacy. Users of these cards need confidence that the benefits will be available when they expect them to be, and that associated information will not be abused by those with access to it.

6. The Public Switched Network and the Internet

As new technologies are integrated into the public network, new vulnerabilities are introduced. Some technologies are more vulnerable than others. For example, wireless communications are particularly vulnerable to eavesdropping, while cable and satellite television providers face an ongoing battle to protect the commercial information they are sending to consumers.

As individuals and organizations become more reliant on the NII to conduct personal and business transactions, the availability and reliability of the network is of greater importance. These concerns vary from the risk of major network outages to the minor irritant of slow or noisy network connections. Users need assurances that the NII will be there when they need it. If it isn't, they want meaningful recourse. For certain transactions, users also desire an assurance that information was received by the intended recipient, analogous to "certified mail."

Users will depend not just on the availability and reliability of the information itself and of the system on which it resides, but indirectly on the availability and reliability of the network which transports the information between systems. From the perspective of the providers of network services, security threats include natural disasters such as fires, floods, or hurricanes; physical attacks, such as bombs; electronic attacks, such as computer viruses; and unintentional errors, such as design flaws, software bugs, and human error. Network services providers are addressing these threats as an integral part of their business. During the public meetings, some participants were open to appropriate Federal involvement in this area, while others were more cautious about the Federal role in this area.

Appendix E

Other concerns include the risk that hackers may intentionally compromise the security of personal or organizational computer systems, or maliciously gain access to information while it is moving from place to place within the NII. These fears are grounded in well-publicized incidents on the Internet and public switched network, but actually comprise only a small fraction of computer security incidents. The majority of incidents are caused by authorized individuals doing unauthorized activities. There was some discussion of the need to share information among providers concerning the outside threats to networks, as well. Other security concerns included the need to verify whether information was altered accidentally and the need to ensure availability of networks in the event of natural disasters.

Appendix F

Roles and Responsibilities: NII Security Issues Forum

June 14, 1994

The Role of Government in NII Security:

Government has an important mission to support the secure use of the National Information Infrastructure (NII). The NII is an interconnecting network of networks, which includes the information content and the information system. Government must cooperate with the private sector and with the public-at-large in setting legal and policy ground rules for the security in the NII. This responsibility is shared among the Federal government and State, local, and Tribal governments. In addition, the Federal government should also assess the security implications for the NII presented by a global information infrastructure. It should also serve as a facilitator and catalyst for private sector and other governmental activities.

The Role of the NII Security Issues Forum:

The NII Security Issues Forum will provide leadership for Federal NII Security activities. It will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various committees of the Information Infrastructure Task Force (IITF) and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

Strategy:

The Committees of the IITF will work with the public to identify the security needs of various users of the NII. Committees should solicit input and initiate dialogue with their constituent users. This dialogue should help define the security requirements for the NII in order to determine needed policy, technology, and managerial controls, and what the Federal role will be to assure that those needs are fulfilled. To accomplish this, an initial Public Meeting to stimulate this dialogue is being planned.

The Forum will also collect information concerning the impact of civil case law on security in electronic environments and will analyze the sufficiency of Federal criminal law. It will then foster the development of corrective legislation, if needed.

Finally, the Forum will collect and disseminate information about public and private sector security technology and management controls in order to ensure that the needed security capabilities will be available.

Appendix F

Organizational Responsibilities:

The Forum will conduct outreach activities, assess current policies, and act as a clearinghouse for the security activities of the IITF and of other Federal government entities.

I. The Forum will:

- Initiate and maintain a public dialogue involving individuals, organization, industry, and State, local, and Tribal governments in discussions of the needs for legal aspects of, and techniques for security of the NII.
- Assess the sufficiency of the current criminal statutory regime; notify the participants of movement on relevant legislation; report on developments in civil case law relevant to computer security; and consider the need for amendment to statutes or new laws.

II. The Forum will coordinate the following IITF activities:

- The Telecommunications Policy Committee, the Information Policy Committee, and the Committee on Applications and Technology of the IITF will identify security requirements for their constituents, as appropriate. For Example:
- The Intellectual Property Rights Working Group and the Privacy Working Group, through the Information Policy Committee, will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.
- The Network Reliability and Vulnerability Working Group, with the assistance of the National Communications System and through the Telecommunications Policy Committee, will advise the Security Issues Forum on (1) protection for all users from catastrophic failure of the public switched network and the information services it provides, along with mechanisms for recovery from threats ranging from natural disasters to overt attacks, and (2) national security and emergency preparedness requirements.
- Other working groups in the Committee on Applications and Technology will identify sector-specific user requirements for security, such as those in the areas of health information and education.

Appendix F

- III. The Forum will draw together technical and analytical support throughout the federal Government. In particular, the Forum will coordinate the efforts of the following Federal government entities:
- National Institute of Standards and technology (NIST) will encourage the Computer System Security and Privacy Advisory Board to assist NIST in the assessment of security tools and techniques in the use outside of the Federal government.
 - NIST, and other agencies where as appropriate, will assess where research and development on security technology would be useful for the NII.
 - NIST, working with other agencies, will identify Federal security products, techniques, and practices that will be useful in the NII (e.g., recent EDI security guidance).
 - NIST will work with the Forum of Incident Response and Security Teams to assess how private entities conduct emergency response and how the efforts of government can be coordinated with them to ensure a "911" capability for the NII.
 - National Communications System, in coordination with the industry's National Security Telecommunications Advisory Committee, will work with the Network Reliability and Vulnerability Working Group to ensure that the National Security and Emergency Preparedness needs are accommodated in the NII.
 - National Security Telecommunications and Information Systems Security Committee will identify useful security tools and techniques in the national security community that may be applicable to the NII.
 - Working Group on Encryption and Telecommunication s will develop Policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps. This will require development and evaluation of technologies and policies that balance law enforcement's need for access with the need for strong security.
 - The High Performance Computing and Communications Program will assure development and testing of new technologies for computer security suitable to a High performance environment.
 - The Federal Networking Council, a multi-agency committee federal research networks, shall explore specific issues relating to security of the Internet.