NISTIR 4734

Foundations of a Security Policy for Use of the National Research and Educational Network

Arthur E. Oldehoeft

Chairman
Computer Science Department
Iowa State University

for the

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems laboratory
Computer Security Division
Gaithersburg, MD 20899

February 1992

U.S. DEPARTMENT OF COMMERCE
Rockwell A. Schnabel, Acting Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
John W. Lyons, Director

Foreword

Security has become a topic of national importance as more and more information is being processed in distributed computer systems and networks. This report explores some underlying considerations in the development of a security policy for the evolving National Research and Education Network (NREN).

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines for the protection of unclassified but sensitive information processed by Federal organizations. NIST standards include technical methods for providing security in cost-effective, interoperable ways. NIST guidelines outline management responsibilities and procedures for effectively and securely using and operating the computers. However, it is the responsibility of each Federal organization to establish its own security policy or policies, to identify and justify the security needed and to establish a security program for implementing and managing the security mechanisms selected.

The National Research and Education Network is one part of a Federal program establishing a comprehensive set of computing and communications services throughout the nation's scientific and educational communities. It consists of a large number of Federal, State and commercial entities providing and using a wide range of services. As such, it will be organized as a cooperative with a membership including service suppliers and users with a distributed management structure. Basic security services will be expected by most users with special security services required by others.

Specifying security policies, procedures, methods and mechanisms in a loosely coupled, multi-faceted, distributed network such as the NREN will be difficult. Scientific research and education professionals have become accustomed to open access to many computers and data bases without restriction. Simultaneously, they have expected reliable services with a high level of availability, data with a high degree of integrity and communication with some implied level of confidentiality. In practice, there are no assurances of any of these security services and there presently exists no written policy which could be used as a basis for providing them. Future networks must provide easy access to information and information processing services to all those who are authorized in a simple, user friendly manner. Simultaneously, future networks must count on the cooperation of users in order to assure a reasonable level of integrity and availability of processing services and integrity, availability and confidentiality of information to properly authorized users.

This report is the result of a research activity sponsored by NIST. Dr. Arthur Oldehoeft is the Chairman of the Computer Science Department at Iowa State University. During a six month sabbatical leave from Iowa State, he worked at NIST investigating the status of NREN and exploring alternative foundations of a security policy for the NREN. He has analyzed existing security policies and codes of ethics that have been established in several government organizations and university environments. He has coordinated with several leaders in network technology in investigating security policies and provisions that could be acceptable to network implementors, users and managers. However, it has not been reviewed by a large number of users and is not endorsed by any organization having authority over such a network.

This report is the result of a research activity and should not be interpreted as a NIST standard

or guideline established through the Federal Information Processing Standards process. The report is intended for discussion purposes by the people and organizations sponsoring the development and use of the NREN. It will be provided as input to the Federal Networking Council for its deliberations on what security provisions should be expected and provided in the Interagency Interim National Research and Education Network (IINREN). Other security policies and provisions should be expected as this evolves to national and international information networks in the future.

The draft policy outlined in the report is considered a level 1 policy in a theoretical hierarchy of policies. This hierarchy ranges from information technology codes of ethics through a number of refined levels of policies down to implementation specifications for security mechanisms, procedures and protocols that support and enforce the policies. Future research is planned to explore this range of policies in a number of security domains that can be defined within a broad distributed network.

Dennis K. Branstad, Ph.D.
NIST Fellow
Project Advisor

Executive Summary

The National Research and Education Network (NREN) is an integral part of the planned High-Performance Computing and Communication (HPCC) infrastructure that will extend throughout the scientific, technical and education communities. The projected vision is one of desks and laboratory benches as entry points to a nation-wide electronic network of information technologies with shared access to services and resources such as high-performance computing systems, specialized software tools, databases, scientific instruments, digital libraries, and other research facilities.

The problem of computer and network information security (one of the major computing issues of the day), will be complicated by the diversity of requirements as the NREN is designed, developed, and operated in collaboration with potential users in government, industry, research laboratories, and educational institutions. One major impediment to improved security is the lack of a clearly stated security policy for general computing. In recognition of this problem, national organizations are beginning to develop and publish codes of ethics for the use of computers. An Internet working group has recently published guidelines for the secure operation of the Internet.

Recent Congressional legislation for HPCC reaffirms the role of the National Institute of Standards and Technology as the agency that is "responsible for developing and proposing standards and guidelines needed for cost-effective security and privacy of sensitive information in Federal computer systems."

The purpose of this report is to explore the foundations of a security policy and propose a security policy for the NREN, one that is applicable to and identifies responsibilities of all major network constituents: end users, system administrators, management at all levels, vendors, system developers, service providers, and the Federal Networking Council.

In order to establish an appropriate context for the development of a national network security policy and also provide for an understanding of the culture of open computer networks, this report first traces the evolution of "national" networks in the U.S. From the structure and operation of the existing NSFNET and Internet, the probable characteristics of the evolving NREN are projected. Foundations for specification of a policy are established through a review of the basic concepts of "security" and "security policy" and through the examination of existing policies, codes of ethics, and Federal legislation regarding computer information security. A draft policy is then abstractly stated, one that is independent of current technologies and organization-specific practices. Since the development of a widely-accepted and meaningful security policy requires the participation of all major constituents, this draft policy is intended to provide the basis for continuing discussion and further development.

Acknowledgements

The author is pleased to acknowledge helpful discussions with many individuals including Robert Aiken, Dennis Branstad, Vinton Cerf, Steve Crocker, Robert Kahn, Stuart Katzke, Jerry Linn, Robert Rosenthal, and Steve Squires.

Contents

1 Introduction 1
- 1.1 Background . . . 1
- 1.2 Purpose and Scope of Report . . . 1
- 1.3 Overview of Report . . . 2

2 Evolution of the NREN 3
- 2.1 Introduction . . . 3
- 2.2 Early DARPA Sponsorship . . . 4
  - 2.2.1 National Science Foundation Sponsorship . . . 5
  - 2.2.2 Supercomputing Initiative . . . 5
  - 2.2.3 Development of a Higher Capacity Backbone . . . 5
  - 2.2.4 Experimental Gigabit Networks . . . 6
- 2.3 The Internet . . . 7
- 2.4 Present Federal Interest and Initiatives . . . 8
  - 2.4.1 Federal Councils, Committees and Information Offices . . . 8
  - 2.4.2 High Performance Computing and Communications Initiative . . . 9
  - 2.4.3 Mandate for a National Research and Educational Network . . . 9
  - 2.4.4 Pending Questions on General Policy . . . 11
- 2.5 Projected View of the NREN . . . 11
  - 2.5.1 Long-Range View . . . 11
  - 2.5.2 Fundamental Characteristics . . . 12
  - 2.5.3 Constituency . . . 13
  - 2.5.4 Network Topology and Security Considerations . . . 14
- 2.6 Conclusion . . . 15
- 2.7 References . . . 16

3 Foundations for a National Network Security Policy 18
- 3.1 Introduction . . . 18
- 3.2 Computer Information Security and Security Policies . . . 18
  - 3.2.1 Concept of Computer Information Security . . . 18
  - 3.2.2 Specification of a Security Policy . . . 19
- 3.3 Ethical and Legal Considerations . . . 19
- 3.4 Need for a National Network Security Policy . . . 20
- 3.5 Examples of Existing Organizational Policies . . . 22
  - 3.5.1 A Federal Agency Policies . . . 23
  - 3.5.2 University Departments and Research Laboratories . . . 24
- 3.6 Draft Policy for Secure Operation of the Internet . . . 27
- 3.7 Conclusion . . . 29
- 3.8 References . . . 30

4 Proposed Security Policy for Use of the NREN 33
- 4.1 Objectives . . . 33
- 4.2 Scope of the Policy . . . 33
- 4.3 Vulnerabilities and Threats . . . 34
- 4.4 Responsibilities . . . 36
- 4.5 Examples of Second-Level Refinements of Responsibilities . . . 39

4.6 Definitions 41
4.7 References 43

5 Future Work **44**

6 Conclusion **45**

1 Introduction

1.1 Background

After more than two decades of research, security in computer information systems remains one of the "major issues" of the day. While significant technological advances have been (and continue to be) made, the general problem of security has assumed larger and more complex dimensions – attributed in a large part to the development and pervasive use of computer networks.

Computers in industry, universities, and government laboratories are now commonly part of local area networks which are in turn connected to larger regional, national and international networks. Many computers in businesses and homes have dial-up accessibility to other computers in this same web of interconnected networks.

Major efforts have focused on the development of network communication protocols for efficient and reliable transmission of information while less attention has been devoted to the problems of security. In response to a universal acknowledgement of the need for information security, circumstances are changing and increasing attention is being given to security. This need for security is counterbalanced by an equal need to provide functionality for information sharing, distributed computation, file transfer, and electronic mail.

Most of the current research deals with the technical issues of enforcing specific aspects of security - e.g. access controls and encryption. Comparatively little attention has been given to the development of a meaningful and generally accepted "policy" for information security that would be applicable to a diverse set of users and computers in interconnected networks.

The U.S. Congress has recently passed legislation that defines important new initiatives in High Performance Computing and Communications (HPCC). An integral component of the HPCC program is the development of a high-speed "National Research and Educational Network (NREN)" that is intended to link together research and educational institutions, libraries, government laboratories, and industry.[1] As the NREN continues to evolve, the problem of computer information security is expected to become more acute.

1.2 Purpose and Scope of Report

The purpose of this report is to explore the foundations of a national network security policy and propose a draft policy for the NREN. Within this context, a network is defined to be a collection of autonomous computers interconnected by some communication media. The term security refers to computer and network information security. References to the NREN are generally intended to include not only the backbone transmission facilities, but also entities connecting to the NREN: local networks, host computers, and end users themselves. To that end, the scope of the proposed

[1] The NREN is envisioned as the evolution of existing networks, including those of the Federal Agency currently being developed as the Interagency Interim National Research and Education Network (IINREN), to a multi-gigabyte/second network that is expected to mature by 1996.

security policy is broad, addressing the responsibilities of users, managers, system administrators, system developers, vendors, network service providers, and a national coordinating body.

The policy presented here is at an abstract "first-level", somewhat higher than typical policies or directives that establish organization-specific requirements and depend on technology-specific security mechanisms. In order to derive actual security practices from the security policy, further refinements are necessary. Properly addressed, these refinements should culminate in the formulation of formal specifications for security services and supporting mechanisms. Such specifications could be used by service providing organizations or entities, in addition to user organizations, for uniformity and interoperability purposes in providing required protection.

The development of a widely-accepted and meaningful policy is normally an evolutionary process that requires the participation of all major constituents that will be affected by the policy. Therefore, the policy specified in this report is intended to establish a basis of discussion among these constituents on what security services could or should be expected in such a network, what overall security objectives should be pursued in the development of such a network, and who should be responsible for what parts of security.

This report is submitted to the National Institute of Standards and Technology (NIST) as fulfillment of the research effort specified above. It is the result of a six month research activity sponsored by NIST. Under the provisions of the Computer Security Act of 1987, NIST is responsible for developing standards and guidelines for security of unclassified information in Federal information systems. NIST also participates in numerous Federal activities coordinating the use of computer systems in Federal computer networks and in national activities coordinating the use of Federal and commercial systems. This report was developed under sponsorship of NIST (Contract 43NANB112737) as part of its research program in computer security and as a contribution to the Federal Networking Council for its work on the Interagency Interim National Research and Educational Network (IINREN). It is not a proposed standard and has not been reviewed or endorsed by any organization having policy authority over the NREN or IINREN.

1.3 Overview of Report

Chapter 2 traces the evolution of the concept of a "national" network, from its origin to present day considerations. Included is a discussion of the involvement of various Federal agencies and committees. Some projections are made about the ultimate nature of the NREN and its topology in terms of administrative structure that would have impact on the feasibility and enforcement of a national network security policy.

Chapter 3 is a discussion of the foundations for a broad security policy. Basic concepts of security and security policy are reviewed. The need for a national policy is established by noting various codes of ethics, congressional acts, and the diversity of existing organizational policies. Included is a summary of the currently proposed guidelines for secure operation of the Internet.

Chapter 4 is a presentation of the proposed security policy for the NREN. It includes a discussion of scope, vulnerabilities and threats, and responsibilities of the various constituents.

2 Evolution of the NREN

2.1 Introduction

The history of data transmission networks in the U.S. is characterized by astonishing growth, massive innovation, and rapid change. Continuing technological developments indicate that the current pattern of growth will not diminish in the foreseeable future. The NREN, as a next major phase in U.S. research and education networking, is an integral part of the current HPCC Initiative.

As stated in [OSTP91], this initiative has three strategic priorities:

- extend U.S. technological leadership in high-performance computing and communications;
- provide wide dissemination and application of the technologies both to speed the pace of innovation and to serve the national economy, national security, education, and global environment; and
- spur gains in U.S. productivity and industrial competitiveness by making high-performance computing and networking technologies an integral part of the design and production process.

The NREN is the basic component in this planned information infrastructure that will extend throughout the scientific, technical, and educational communities. Its creation is dictated by [BELL88, OSTP91]:

1. the mushrooming demand for electronic communication and sharing of information, including the exchange of more comprehensible supercomputer output and high-quality graphical data;
2. the need for a "collaboration technology" to facilitate cooperation between geographically separated researchers;
3. the Federal interest in maintaining U.S. leadership role in science and technology;
4. the requirements for solving the so-called "Grand Challenges" - defined in [CONG91a] to be fundamental problems in science or engineering with economic and scientific impact, whose solutions will require the application of high performance computing resources;[2] and
5. the need to serve many sectors of government, research, and education.

The vision projected is one of desks and laboratory benches as entry points to a complex high-speed electronic network of information technologies, services and resources, providing access to specialized

[2] In technical terminology, a partial list of challenges would include (Cf. [OSTP91, OTA91]): 1) computational fluid dynamics for the design of hypersonic aerospace or efficient automobile bodies, 2) computer-based weather and climate forecasts and understanding global environmental changes, 3) electronic structure calculations for the design of new materials such as chemical catalysts, immunological agents, and superconductors, 4) plasma dynamics for fusion energy technology and for safe and efficient military technology, 5) calculation to improve the understanding of the fundamental nature of matter, including quantum chromodynamics, and condensed matter theory, 6) machine vision to enable real-time analysis of complex images for the control of mechanical systems

computers, supercomputers, application programs and software tools, specialized databases, experimental apparatus, digital libraries (books, journals, pictures, sound recordings, films, and other types of information media), computer conferencing systems, bulletin boards, and electronic mail [OTA89].

The HPCC Initiative and the NREN have been the subject of discussion of numerous committees and councils, representing the interests of government, industry, and academia. The Congress of the United States has recently passed legislation that further defines this initiative and determines the responsibilities to be assigned to various government agencies.

This chapter first describes past and current Federal sponsorship in the development of a "national" network for the U.S. "research and education" communities. Although relevant to the development of the networking technology, there is no attempt to describe the multitude of proprietary and special interest networking efforts of the various State and Federal agencies, U.S. industries, and other commercial enterprises. The reader is referred to [QUAR86, QUAR89, QUAR90] for a history of such developments. Second, the current Federal interest in developing the NREN is cited along with a description of recent legislation. Some interesting questions, that ultimately require answers, are raised about the scope, management, and operation of the NREN. Finally, some projections are made about the character of the NREN along with the potential impact on information security.

2.2 Early DARPA Sponsorship

As stated in [HURA90], the ideas for a national research network are traceable to studies by the Rand Corporation in the 1960's. By 1969, the first prototype U.S. network was created by Bolt, Beranek and Newman under sponsorship of the U.S. Advanced Research Projects Agency (ARPA), now called the Defense Advanced Research Projects Agency (DARPA). Sharing of computing resources among researchers was the primary objective. This network, called ARPANET, was an experiment in using leased-line communication media to interconnect a collection of host computers and switching computers. Despite heavy military involvement, the resulting ARPANET turned out to be a fairly open network. It provided the test bed for the development of communication protocols to support functionality such as transmission of graphical data, remote login, file transfer, and electronic mail.

Perhaps the most important aspect of the DARPA development was the research it inspired in packet switching and end-to-end communication across multiple networks, leading to the present-day, widely-implemented Transport Control Protocol/Internet Protocol (TCP/IP). Using "store-and-forward" packet-switching technology, there is no dedicated network path for transmitting a message; rather a message is broken into packets, each of which is independently and dynamically routed through a network, and reassembled at the final destination. The IP protocol serves to connect networks within an internet and the TCP protocol provides reliable end-to-end communications between different machines in an internet.

In response to an overload of traffic on the ARPANET, the Department of Defense in 1983 split off the operation of its military traffic into a separate network called MILNET [MARS89]. The two networks collectively formed what was referred to as the "Internet". Since 1983, with TCP/IP

as the primary protocol, there has been an explosive growth in the number of networks that have connected to and become part of the Internet.

2.2.1 National Science Foundation Sponsorship

2.2.2 Supercomputing Initiative

With funding from Congress, the National Science Foundation established in 1984 a program intended to improve the availability and use of high performance computing to the science research communities.

In 1985-86, NSF selected five sites as National Supercomputing Centers with computing facilities remotely accessible by other researchers through a backbone NSFNET. The selected centers were: San Diego Super Computer Center – located by the University of California at San Diego and operated by General Atomics; National Center for Supercomputing Applications – operated by the University of Illinois; Cornell Theory Center – located at Cornell University; Pittsburgh Supercomputing Center – operated jointly by the University of Pittsburgh, Carnegie Mellon University and Westinghouse Electric Corporation; and John von Neumann Supercomputer Center – located in Princeton, New Jersey.

Promoted as providing backbone connectivity to supercomputer centers, the network traffic of NSFNET was soon dominated by use of general services such as electronic mail, remote login, and file transfer.

With the creation of the Federally funded NSFNET in 1985, ARPANET was eventually phased out and replaced by a new Defense Research Internet (DRI) for unclassified military information that would make use of NSFNET. ARPANET and MILNET became the main constituents of a TCP/IP internet DDN (Defense Data Network) – a subset of the Internet operated by the Department of Defense. Other networks in DDN include DISNET (Defense Integrated Secure Network), SCINET (Sensitive Compartmented Information Network) and WINCS (WWMCCS Intercomputer Command and Control System) of the World Wide Military Command and Control System [QUAR90].

2.2.3 Development of a Higher Capacity Backbone

In an attempt to keep pace with the enormous increases in data traffic (200 million packets/month), the initial backbone network was de-commissioned two years later (1988) in favor of a new backbone [WOLF88]. By July 1988, seven new regional university-based research networks were added and the transmission speed of the backbone was increased from 56 Kbits/sec to 1.544 Mbits/sec (T1). The NSFNET backbone interconnected multiple autonomously administered mid-level networks, which in turn connected to autonomously administered networks of universities and research centers. Multiple peer network infrastructures of other Federal agencies are also connected to NSFNET.

In 1989, NSFNET connected three levels of networks [MARS89, WULF89]:

- the cross-continental NSFNET backbone with 13 gateways (supercomputer site or regional network center) –

BARRNET - Bay Area Regional Research Network (Palo Alto, CA),

JVNCNET - John von Neumann Supercomputer Center Network (Princeton, NJ),

MERIT - Merit Corporation (Ann Arbor, MI),

MIDNET - Midwestern States Network (Lincoln, NE),

NCSANET - National Center for Supercomputing Applications Network (Champaign, IL),

NORTHWESTNET - Northwestern States Network (Seattle, WA),

NYSERNET - New York State Education and Research Network (Ithaca, NY),

PSCNET - Pittsburgh Supercomputing Center Network (Pittsburgh, PA),

SDSCNET - San Diego Supercomputer Center Network (San Diego, CA),

SESQINET - Sesquicentennial Network (Houston, TX),

SURANET - Southeastern Universities Research Association Network (College Park, MD),

USAN - National Center for Atmospheric Research Satellite Network (Boulder, CO), and

WESTNET - Southwestern States Network (Salt Lake City, UT);

- regional networks connecting to the backbone; and
- campus and research organizations.

In 1990, NSFNET consisted of more than 1000 state, regional, and institutional networks, including well over 100,000 computers [GOUL90]. In 1991, the NSFNET backbone was upgraded to 16 nodes operating at 45 Mbits/sec (T3). Its planned protocol base consists of the TCP/IP suite of protocols and also the ISO CLNP (connectionless network protocol).

Numerous other government networks have gateway connections (existing or planned) to NSFNET – including the NASA Science Internet (NSINET), the Energy Science Network (ESNET), and others. In general, the Federal agencies have a vested interest in the Internet.

NSFNET is presently managed by the Merit Corporation under a cooperative agreement with NSF. The operation of NSFNET is contracted to a private nonprofit subsidiary, Advanced Networks and Services, formed by the IBM Corporation, the MCI Corporation, and Merit.

Despite its enormous success, a number of challenging problems remain to be solved, including privatization of the network, priority routing, measurement of traffic and billing, and improved security.

2.2.4 Experimental Gigabit Networks

In June 1990, NSF announced a three-year research effort aimed at funding five test bed experimental networks of gigabit speed. Working in collaboration with DARPA, this was considered a first step in developing a wide-area broadband advanced communication capability.

In 1991, the Office of Science and Technology Policy (OSTP) presented its plan for HPCC in support of the 1992 budget proposed by the Executive Branch of the Government [OSTP91], including funding for the NREN. This plan along with recent congressional legislation calls for gigabit speeds by 1996.

2.3 The Internet

The U.S. portion of the Internet is made up of different parts [CERF91b]. There are Federally subsidized components such as NSFNET, NASA Science Internet (NSINET), Energy Sciences NET (ESNET) and DARPA Test Net (DARPNET) that have agreed to interconnect and carry each other's traffic. There are also commercial networks (PSINET, CERFNET, UUNET/ALTERNET) that are linked together via a commercial internet exchange (CIX) and, via some of its members, linked to the NSFNET backbone. Most midlevel networks are linked to NSFNET and/or commercial networks. International connections have been established through government agreements or through business negotiations by the commercial networks. In all, the U.S. portion of the Internet consists of several government or government subsidized backbones or regional networks, a couple dozen regional/mid-level networks. and thousands of private (industry, university and institutional) networks including private for-profit commercial mid-level and wide-area nets (commercial backbones).

As a first step toward ultimate commercialization[3], commercial networks are presently allowed to establish experimental messaging interconnections to the Internet via one of the mid-level networks. Conditions for interconnection by a commercial network include 1) transporting at no cost to Internet senders (recipients) messages to (from) recipients (senders) on the commercial network, 2) prohibition of use of the Internet for traffic between commercial systems that are not for purposes of research and/or education, 3) prohibition of Internet use for advertisements or solicitations except for services and support for scholarly research purposes – costs to be borne by individual or institutional subscription, 4) optionally making accessible to Internet users any public directory services which assist in identifying the users of commercial services, and 5) bearing any costs associated with physical interconnection. Commercial information providers are permitted to distribute services that support Federal Research and Education, on the Federally-sponsored portions of the Internet.

The global Internet community spans the entire U.S. with links to Africa, Canada, Western Europe, Japan, the Middle East, Australia, Central and South America, New Zealand, and others in the Pacific Rim, Eastern Europe, the USSR, etc. Its growth is so rapid that any estimate of its size is soon obsolete. For example, in 1990, it was estimated that the network included 150,000 connected hosts and millions of users [BENA90, CERF90a]. In 1991, as reported in [CHAR91, ANTH91], the network connected three million users on 350,000 host computers on 5,000 networks in 33 countries. In September 1991, according to [CERF91a], there were more than 5,000 networks connected to the Internet, consisting of more than 570,000 hosts (of which 450,000 are in the U.S. and 90,000 are in Europe).

For some years, the U.S. portion (non-Federal) of the Internet has developed under the informal

[3]Commercialization is defined to be the building of the network through use of commercial telecommunications services whenever feasible.

guidance of the Internet Activities Board (IAB) – a small group of communications experts who volunteered their services, and two subsidiary task forces – Internet Engineering Task Force and Internet Research Task Force [CERF90b]. In June 1991, a user group called the Internet Society was announced to be in operation by January 1992. The purpose of the Internet Society is to function as a professional society, to stimulate interest in and growth of the Internet, to educate the public about the use of the Internet, and to facilitate its continued evolution.

The Internet is expected to continue to operate in its present manner – that is, through its various component networks at various universities, State and Federal agencies, in cooperation with industries and commercial enterprises. According to [CERF91a], the IAB has for several years supported the development of multiple protocol support in the Internet. Presently, numerous protocols operate in various parts of the Internet (TCP/IP, OSI, DECNET, Novell Netware IPX, XNS, etc.). The most common, wide-area protocol is still TCP/IP but the adoption of ISO CLNP as a co-standard appears imminent.

2.4 Present Federal Interest and Initiatives

2.4.1 Federal Councils, Committees and Information Offices

The U.S. Government has since 1984 become increasingly aware of the essential role played by information technology in practically all areas of research and development. Bell reports [BELL88], the U.S. Congress requested in 1986 that OSTP study the potential development of a communications network for research computers, including supercomputers at universities and Federal research facilities. In recent years, a number of agencies, committees, and councils have been instrumental in the advising the government in its planning for HPCC and national networking –

1. Office of Technology Assessment (OTA) - advises the U.S. Congress on matters concerning science and technology;

2. Office of Science and Technology Policy (OSTP) - advises the President branch on matters of science and technology and coordinates interagency issues regarding science and technology; advice regarding HPCC and NREN (as a component of HPCC) is formulated primarily through its Federal Coordinating Council on Science and Technology (FCCSET); it will be assigned major responsibility in developing national plans for HPCC;

3. National Science Foundation (NSF) - a U.S. government funding agency charged with advancing research in science and technology;

4. President's Council of Advisors on Science and Technology (PCAST) - advises the President on matters of science and technology (membership is from the private sector);

5. Federal Research Internet Coordinating Committee (FRICC) - superseded by FNC (see below), this informal committee was formed to coordinate U.S. Government support for the development and use of the Internet; government agencies initially included the Department of Energy (DOE), the Defense Advanced Research Projects Agency (DARPA), the National Aeronautics and Space Administration (NASA), and the National Science Foundation (NSF), along with observers from the Internet Activities Board; and

6. Federal Networking Council (FNC) - the successor to and enlargement of FRICC, this is an independent interagency group; it coordinates the use of the U.S. portion of the Internet by Federal agencies and provides liaison with OSTP; some members of the FNC are also members of the Coordinating Committee for Intercontinental Research Networks (CCIRN); the FNC has representatives from numerous Federal agencies – OMB (Office of Management and Budget), NSA (National Security Agency), DISA, NOAA, DOE, DARPA, HHS, OSTP, NIST, EPA (Environmental Protection Agency), USGS, GSA (General Services Administration), NTIA (National Telecommunications and Information Administration), NASA, NSF and the Department of Education; advisory committee members come from the IAB, higher education, national research laboratories, computer and communications corporations, and private industry.

2.4.2 High Performance Computing and Communications Initiative

Recent reports issued by OSTP and OTA [OSTP91, OTA91] address the HPCC requirements to sustain and extend U.S. leadership in all advanced areas of computing and networking and to meet the so-called "Grand Challenges".[4] Congressional legislation [CONG91b] identifies four components of the program:

1. hardware - development of more powerful supercomputers and networking technologies;
2. software - development of higher performance software to effectively apply the power of supercomputing;
3. education and basic research - training of computational scientists to effectively use supercomputing technology and training of computer scientists and engineers to develop new supercomputer hardware and software; and
4. networking - deployment of a national computer network capable of transmitting information at multi-gigabit speeds to allow for the appropriate communication and access to shared resources.

2.4.3 Mandate for a National Research and Educational Network

Both the OSTP and OTA identify the development of the NREN as an essential component of a HPCC program. Such a network is required to provide distributed computing capability to the U.S. research and educational community (government agencies, industry and research laboratories, universities, libraries) and would further advance research on very high-speed networks and computer applications. In this role, the NREN component will dramatically expand and enhance the research and educational aspects of the U.S. portion of the larger Internet. The intent is to provide a wide-spread, uniform, high-performance (gigabits/second) national infrastructure and also provide

[4] A layman's list would include 1) forecasting severe weather events, 2) human genome research, 3) predicting new superconductors, 4) air pollution, 5) aerospace vehicle design, 6) energy conservation and turbulent combustion, 7) microsystems design and packaging, 8) predicting directions and consequences of changes in the earth's biosphere, 9) development of gigabit networks, and 10) education using a national network.

a basis for the development of new and higher-level computing capabilities. Long-range plans include expanded interconnectivity to support applications requiring terabit transmission speeds.

The U.S. Congress has recently passed legislation [CONG91b] entitled the "High Performance Computing Act of 1991"[5], authorizing funding for the HPCC program for fiscal year 1992. The 1992 budget prepared by the Executive Branch of the U.S. Government includes funding for HPCC. Quoting from this bill, the Act states (among other things) that the NREN shall:

1. be developed and deployed with the computer, telecommunications, and information industries;
2. be designed, developed, and operated in collaboration with potential users in government, industry, and research and educational institutions;
3. be designed, developed, and operated in a manner that fosters and maintains competition and private sector investment in high-speed data networking within the telecommunications industry;
4. be designed, developed, and operated in a manner that promotes research and development leading to development of commercial data communications and telecommunications standards, whose development will encourage the establishment of privately operated high-speed commercial networks;
5. be designed and operated so as to ensure the continued application of laws that provide network and information resources security measures, including those that protect copyright and other intellectual property rights, and those that control access to databases and protect national network security;
6. have accounting mechanisms that allow users or groups of users to be charged for their usage of copyrighted materials available over the Network and, where appropriate and technically feasible, for their use of the Network;
7. ensure interoperability of Federal and non-Federal computer networks, to the extent appropriate, in a way that allows autonomy for each component network;
8. be developed by purchasing standard commercial transmission and network services from vendors whenever feasible, and by contracting for customized services when not feasible, in order to minimize Federal investment in network hardware;
9. support research and development of networking software and hardware; and
10. serve as a testbed for further research and development of high-capacity and high-speed computing networks and demonstrate how advanced computers, high-capacity high-speed computing networks, and databases can improve the national information infrastructure.

[5]The House-Senate compromise version of S.272 was passed by the House on November 20, 1991 and by the Senate on November 22, 1991. It was signed by the President on December 9, 1991.

Specific responsibilities for the NREN are assigned to several Federal agencies. In particular, the National Institute of Standards and Technology will, among other things continue to be responsible for "developing and proposing standards and guidelines to assure the cost-effective security and privacy of sensitive information in Federal computer systems."

2.4.4 Pending Questions on General Policy

As the NREN continues to evolve, there are numerous pending policy issues:

1. management of the network - e.g. who will be responsible – Federally chartered nonprofit corporations, lead roles for agencies, interagency consortium, competitive commercial offerings, etc.;
2. management relationships among diverse networks - to what extent standardization and centralization is desirable;
3. policies needed for network service offerings (e.g. databases and databases searching services, news, publication, software, directory services);
4. economic and legal policies needed for reference services, commercial information industry, Federal data banks, university data resources, libraries, publishers, etc.;
5. the effect on the conduct of science - e.g. pattern of research collaboration, communication, and education, issues of intellectual property rights, export control of information, publication of results, cross-disciplinary communication, equity of access to scientific resources, control of scientific information flow, cost and capitalization of conducting research, public access to researchers and research information, dissemination of scientific information, legal issues such privacy, ownership, and copyright; and
6. standards needed for networks and network-accessible services and host interfaces, interface requirements for common carriers, interoperability requirements across heterogeneous collections of computers and systems, user interfaces, requirements of reliability and bandwidth, measurement of access and usage along with accompanying charges, methods to enhance security.

2.5 Projected View of the NREN

2.5.1 Long-Range View

Currently, the NREN involves many public and private actors with vested interests and spheres of capabilities [OTA89]:

1. universities;
2. networking industry, the telecommunications, data communications, computer, and information service companies that provide networking technologies and services;

3. State enterprises devoted to economic development, research, and education;
4. industrial research and development laboratories; and
5. the national laboratories and research-funding agencies of the Federal Government.

While one can only speculate on the long-term nature of the NREN, it appears to be the next logical stage in the development of a total information infrastructure. Ultimately, national network services will likely emerge from the "convergence" of the public telephone system, the cable television distribution system, and computer communication networks such as the Internet [KAPO91].

2.5.2 Fundamental Characteristics

Some fundamental aspects of the NREN are projected by Cerf [CERF90c].

1. The NREN will evolve from the existing Internet base and will have to fit into an international environment sponsored or owned by non-U.S. organizations.
2. Special purpose networks and mission-oriented networks (sponsored by the U.S. government) will need to link with, if not directly support, the NREN.
3. The architecture must accommodate the use of commercial services, private and government-sponsored networks.
4. The architecture will continue to be layered set of protocols although it may differ from present Internet and planned OSI structures in some respects.
5. The system will support multiple protocols, including at least full TCP/IP and OSI protocol stacks, on an end-to-end basis.
6. The architecture must accommodate local areas networks (LANS), metropolitan area networks (MANS), regional networks, and wide-area networks (WANS) – some of which will support transit (pass through) traffic originating and terminating in other networks.
7. A variety of current and evolving technologies may be used including such things as high-speed Fiber Data Distributed Interface (FDDI), Distributed-Queue Dual Bus (DQDB), broadband Integrated Services Digital Network (ISDN) utilizing Asynchronous Transfer Mode (ATM) switching as well as conventional Token Ring, Ethernet, and other technologies.
8. Services accessible through the NREN will include various kinds of servers for general support (network management facilities, name servers, electronic mail, database servers, multicast routers, cryptographic certificate servers), collaboration support tools (video/teleconferencing), and other groupware facilities. Accounting and access control mechanisms will be necessary.
9. The NREN will continue to evolve (as has the Internet) as it incorporates new technologies. Interconnection of experimental facilities must be supported.

The interests and needs of the various constituencies and stake-holders are expected to affect the evolving architecture.

2.5.3 Constituency

Based on recommendations of various working groups and testimonies presented at congressional subcommittees, a diverse constituency is expected.

1. The Users

   As mentioned in documents that describe the Federal initiatives, and as enumerated by Cerf, users will consist of colleges and universities, government research organizations, non-profit and for-profit research and development organizations, Federally funded research centers, research and development of private enterprise, and library facilities of all kinds [CERF90c].

2. Service Providers

   Cerf points out that the present-day support consists of a mixture of government-sponsored backbone, private local area networks, and intermediate level networks (collections of commercially-produced routers and trunk or access lines which connect LAN facilities to the government-sponsored backbones). Since the intent of Federal funding is to provide "seed money", the existing Federally-funded backbone services can be expected to give way to commercially-operated high-speed backbones. A similar statement can be made about the Federally-funded mid-level networks [CERF90c].

3. Vendors

   The technology available to users and service providers will come, for the most part, from commercial sources. Cerf notes an important consequence – namely, the NREN architecture should be fashioned so that it can be constructed from technology available from commercial suppliers and in a manner compatible with the plans of common carriers [CERF90c].

4. Management

   Several divergent ideas have emerged regarding the management of the NREN. The National Research Council[6] points out that good management is needed for maximizing the effectiveness of the investment in a national network [NRC88]. The recommendations are for a long-term management structure that is funded through normal government channels, an oversight committee from a variety of disciplines to oversee the government's investment, and an experienced research executive from the private sector to handle the day-to-day management of the operational aspects.

   An alternate (and seemingly more widely-espoused) view does not endorse centralized day-to-day control of operations. Rather the operations would be the responsibility of the various service providers. Some guiding control might be vested in a government-sponsored group that would specify the technical requirements and interfaces to be met by successful service

[6] More precisely, the National Research Network Review Committee, Computer Science and Technology Board, Commission on Physical Sciences, Mathematics, and Resources of the National Research Council.

providers who are given subsidies by the Federal government or who sell services to subsidized users. In this way, many commercial concerns (managing their own operations) may engage in building and operating a system whose architecture and interfaces are approved by the Federal government.

2.5.4 Network Topology and Security Considerations

The NREN is expected to evolve from some subset of the present Internet (including NSFNET), retaining many of its characteristics – specifically the interconnection of autonomous networks. Within the context of routing protocols, Estrin [ESTR89a] describes two possible topological models for the future Internet. These models serve as a basis for useful ideas. Both models assume the network to be a collection of interconnected administrative domains (ADs), each of which is a collection of hosts and network resources governed by a common policy (e.g. agency, division, company).

1. **Simple AD Topology**
   - Public carriers provide pervasive, competitively priced, high-speed data services.
   - The network is an hierarchically organized collection of (stub) ADs connected to regional backbones, which in turn interconnect via multiple, overlapping long-haul backbones. The primary concern of a stub AD is communication to and from its own hosts. There are no lateral connections between stub ADs or regional networks and no vertical bypass links.
2. **Complex AD Topology**
   - The topology of ADs agrees in many respects to the previous model.
   - The pure hierarchy is, however, violated by unavoidable and persistent exceptions – many stub-ADs will retain private lateral links for political, economic, technical, and reliability reasons.[7]

The prevailing opinion seems to be that the second model more accurately describes the topology of the Internet (and the eventual topology of NREN). It implies the existence of a collection of a diverse, but compartmentalized, policies involving resource usage, charging, routing, and security. The existence of lateral links tends to complicate the operation of the network, including the overall security.

With regard to security requirements, the projected models suggest that collections of users, hosts, and interconnecting networks will form various ADs – ranging from tightly controlled, consistent security requirements (e.g. a corporation) to loosely defined, inconsistent security requirements (e.g. a LAN of university research computers). The realization of security in open heterogeneous environments appears to be a complicated undertaking and may ultimately require the implementation of

[7] For example, a company or organization may have special technical requirements not provided by public carriers.

such things as security perimeters (as defined by trusted computing bases [NRC91]), autonomous regions or security domains [ESTR87], logical networks for communication and collaboration of entities in separate domains (with access permissions controlled through visas [ESTR89a]), and policy-based routing [ESTR89b]. [8]

In attempting to extrapolate from the projected Internet models, a potentially useful view of the total infrastructure is one of 1) a collection of primary backbone networks operated by commercial (and competing) enterprises and nonprofit agencies that provide high-speed transmission services as well as value-added services and 2) connecting customer networks which themselves consist of local backbones, interconnecting networks, hosts, and end users. Under this scheme, the service providers would interconnect and cooperate with each other (satisfying technical interface requirements). Levels of service, including security, may be available on a subscription basis. Gateways would be required for the purpose of protocol and security negotiations between various service providers and with interconnecting customer networks and international networks.

The security provided by customer networks will likely have a large variance, ranging from none to very high levels. As a result, the service providers would view customer networks with suspicion – unless some contractual agreement provides the necessary level of trust. In turn, it is possible that customer networks with high security requirements could view the service providers with suspicion. In order for this arrangement to be workable, it would appear that the service providers will have to provide satisfactory levels of security for the vast majority of participating customer networks. Even with acceptable levels of security from the service providers, end users in different customer networks would view each other's local network and hosts with suspicion, thereby underscoring the need for uniform policies and practices that are applicable at all levels of the infrastructure.

2.6 Conclusion

The NREN is evolving from the existing NSFNET and other portions of the Internet. As a networking concept, it is expected to have a profound impact on the conduct of research and education. Its ultimate structure, operation and management remains speculative although the prevailing opinion is that, it will eventually consist of backbone services provided by numerous competing commercial enterprises and interconnecting autonomous user networks. In any sense, it has to function as part of, or interconnect with, the International Internet. Security is a critical issue that has up to this point in time received relatively little attention compared with other network issues. Since the interconnecting networks will have diverse security requirements, the problem of end-to-end security (up to and including the user level) is one of major difficulty.

[8] The relationship between the notions of of security and reliability is discussed in [DOBS86].

2.7 References

ANTH91 Anthes, G.H., *Internet Society to guide research net,* Computerworld, p. 42, (August 3, 1991).

BELL88 Bell, G., *Gordon Bell calls for a U.S. research network,* IEEE Spectrum, pp. 55-57, (February 1988).

BENA90 Ben-Artzi, A., A, Chandna and U. Warrier, *Network management of TCP/IP networks: present and future,* pp. 35- 43, (July 1990).

CERF90a Cerf, V., *Information infrastructure,* IEEE Network Magazine, 4(2), pp. 6-11, (March 1990).

CERF90b Cerf, V., *The Internet Activities Board,* Network Working Group, Internet RFC 1160, (May 1990).

CERF90c Cerf, V., *Thoughts on the National Research and Education Network,* Network Working Group, Internet RFC 1167, (July 1990).

CERF91a Cerf, V., *Private communication,* (1991).

CERF91b Cerf, V., *Another reading of the NREN legislation,* Telecommunications, pp. 29-30, (1991).

CHAR91 Charbuck, D., *Civilizing Internet,* Forbes Magazine, Vol. 148, No. 1, p. 90, (July 8, 1991).

CONG91a *Congressional Record of the United States of America, Proceedings and Debates of the 102nd Congress, First Session,* pp. S 12734 - S 12751, (September 11, 1991).

CONG91b *The High-Performance Computing Act of 1991,* Congressional Record of the United States of America, Proceedings and Debates of the 102nd Congress, First Session, (November 22, 1991).

DOBS86 Dobson, J.E. and B. Randell, *Building reliable secure computing systems out of unreliable insecure components,* Proceedings of the 7th IEEE Symposium on Security and Reliability, pp. 187-192, (1986).

ESTR87 Estrin, D. and G. Tsudik, *Visa scheme for inter-organization network,* Proceedings of the 8th IEEE Symposium on Security and Reliability, pp. 174-183, (1987).

ESTR89a Estrin, D., *Policy requirements for inter-administrative domain routing,* Internet RFC 1125, (November 1989).

ESTR89b Estrin, D. and G. Tsudik, *Security issues in policy routing,* Proceedings of the IEEE Conference on Security and Privacy, pp. 183-193, (1989).

GOUL90 Gould, S., *Computing and telecommunications in the Federal Government,* CRS Review, Vol. 11, No. 7-8, pp. 12-15, (July-August 1990).

HURA90 Huray, P and D. Nelson, *The Federal high-performance computing program,* EDUCOM Review, pp. 17-24, (Summer 1990).

KAPO91 Kapor, M., *Building the open road: the NREN as a test-bed for the national public network,* Internet Working Group, RFC 1259, (September 1991).

NRC88 National Research Council, *Toward a national research network,* National Academy Press, (1988).

NRC91 National Research Council, *Computers at risk - safe computing in the information age,* National Academy Press, (1991).

MARS89 Marshall, Eliot *NSF opens high-speed computer network,* Science, Vol. 243, pp. 22-23, (January 6, 1989).

OSTP91 Office of Science and Technology Policy, *Grand challenges: high performance computing and communications,* (1991).

OTA89 Office of Technology Assessment, Congress of the United States, *High performance computing and networking for science - background paper,* OTA-BP-CIT-59, U.S. Government Printing Office, Washington, D.C., (September 1989).

OTA91 Office of Technology Assessment, Congress of the United States, *Seeking solutions: high-performance computing for science,* OTA-BP-TCT-77, (April 1991).

QUAR86 Quarterman, J. and J. Hoskins, *Notable Computer Networks,* Communications of the ACM, pp. 932-970, (October 1986).

QUAR89 Quarterman, J., *Recent changes in North American networks,* Proceedings of the European Unix Users Group Conference, (Spring 1989).

QUAR90 Quarterman, J., *The matrix: computer networks and conferencing systems worldwide,* Digital Press, (1990).

WOLF88 Wolff, S., *The present networking situation in the USA,* Computer Networks and ISDN Systems, Vol. 16, pp. 89-91, (1988-89).

WULF89 Wulf, W., *Government's role in the national network,* EDUCOM Review, pp. 22-26, (Summer 1989).

3 Foundations for a National Network Security Policy

3.1 Introduction

The purpose of this chapter is to explore some foundational issues that contribute to the formulation of an information security policy for use of the National Research and Education Network (NREN). First, the basic concepts of security and security policy are reviewed within the context of computer information systems. Second, some remarks are made regarding ethical and legal considerations in enforcing security. Congressional legislation and various codes of ethics published by authoritative bodies are cited, as they tend to lend additional support to the need to develop a national policy. Third, several existing organizational policies are cited to demonstrate the diverse practices of the anticipated NREN user constituency and to further underscore the need for a national set of guidelines. This is followed by a summary of the current proposed guidelines for secure operation of the Internet – the first known U.S. attempt to establish broad-based guidelines that transcends organizational boundaries.

3.2 Computer Information Security and Security Policies

3.2.1 Concept of Computer Information Security

The generally accepted concerns of computer information security are the preservation of confidentiality, integrity, and availability of stored, processed, and transmitted information [CEC91, NRC91, DOD85]. It should be noted that a broader definition of computer security might include concerns that do not necessarily lead to a compromise of these three properties – e.g. preventing the unauthorized use of resources (processors, memory). Parker [PARK91] points out that precise definitions in this area are difficult to formulate.[9] While such foundational work continues, this report will adopt commonly cited definitions.

Confidentiality is defined to be the state that exists when information is held in confidence and protected from unauthorized disclosure. Integrity is that property of information that ensures that modifications have been made only in a specified and authorized manner.[10] Availability is a state of the system in which authorized users are assured of timely and continued access to information, resources, and services. These three properties assume an understanding of underlying concepts such as "users" and "authorization". A user is defined to be a person, organization, or other entity that may request and be granted access to computer resources or services. Authorization assumes that the identity of the user is unequivocally established and authenticated.

It should be noted that the three fundamental properties may conflict under certain circumstances. For example, in multilevel secure databases, hiding classified data from users with lower clearances may require the use of poly-instantiation – yielding multiple versions of data objects with the same

[9] See also the discussion in [STER91a].

[10] In the broader sense, integrity implies that all modifications are authorized and result in "correct" or "consistent" information. For recent papers on integrity, the reader is referred to [CLAR87, CLAR88, RUTH89, SCHE86].

name, but differentiated by security classification. As a result, the database as viewed at a particular classification may be inconsistent or incorrect, thereby violating the integrity [CAMP91].

Most research to-date has been concerned with the issue of confidentiality. A limited amount of work has addressed the issue of integrity and significantly less work has been done on availability.

3.2.2 Specification of a Security Policy

In the broad sense, Sterne, et al. [STER91b] define an organizational security policy to be set of laws, rules, and practices that regulate how an organization manages, protects, and distributes resources in order to achieve specific security objectives. An automated security policy is defined to be the set of restrictions and properties that specify how a computing system prevents information and computing resources from being used in violation of an organizational security policy.

The general consensus is that a computer security policy should be a "concise statement" of the requirements that must be met in order to satisfy security objectives. It should accurately reflect the laws, regulations, and general policies from which it is derived. To be useful it should address the range of circumstances under which the requirements must be met along with associated operating standards [NRC91], although this latter part might be realized through procedures and standards established as necessary to support the policy. The policy should assess the threats, assign a level of concern to each, and state specific policies in terms of what threats are to be resisted.

A recent publication by the National Research Council [NRC91] states that the specification of a policy should address the following points: 1) objectives, 2) scope, 3) specific goals, and 4) responsibilities for compliance and actions to be taken in event of noncompliance.

Violations of security may be due to a number of causes, including:

1. environmental hazards (fire, flood, static electricity, dust, power surges);
2. failure of hardware (processor, storage, communications devices);
3. failure of software (programming or data entry errors);
4. accidents, errors and omissions by users; and
5. intentional acts by users (fraud, theft, sabotage, misuse by competitors and employees).

Most automated information security policies focus on concerns 4 and 5.

3.3 Ethical and Legal Considerations

A range of policy and legal considerations for large computer communications networks, both national and international, is articulated by Hoffman [HOFF91]. The nonuniformity of privacy

laws among states and countries makes questions about data access and confidentiality difficult to address.[11] For a recent discussion of ethical considerations, the reader is referred to [SCHO91].

At this point in time, it is not known to what extent some of the practices and techniques used to enforce security are themselves an invasion of individual privacy as guaranteed by the Fourth Amendment to the Constitution of the United States. For example, intrusion detection techniques show high promise of developing into powerful tools to counter computer abuse [HUBB90, SNAP91]. These tools require the observation and analysis of human behavior in accessing objects and services. The degree to which individual behavior may be observed and audit histories maintained and analyzed are questions that must be ultimately addressed.

Other questions concerning rights and responsibilities include:

1. Should electronic mail be protected like first class mail?
2. Should bulletin board operators be legally responsible for messages posted on their boards?
3. Does the First Amendment to the U.S. Constitution protect the sender?
4. Should intellectual property protections be granted to electronic databases?
5. Should information services providers be responsible for incorrect data or illegal/immoral data?

In terms of general control over the services of a national network, the Federal Communications Commission has heretofore adopted a policy of nonregulation – as contrasted with its careful monitoring of connection to and use of the U.S. telephone system. While some control appears necessary, fears have been expressed that Federal regulation would cripple the pace of innovation and therefore should be avoided. Even with the existence of laws that apply to the use of Federal information systems (e.g. the Computer Fraud and Abuse Act), there is still little legal precedence in establishing rights and responsibilities of various parties – end users, network owners, and public carriers. Responsibility for promulgating the rules for use of present and future public networks appears, at this point, to be an open question.

3.4 Need for a National Network Security Policy

In general, commercial and other users are interested in increasing computer information security in order to reduce the element of computer crimes and to protect proprietary or sensitive data. The general need is made clear in a study by the Office of Technology Assessment [OTA87]. However, users have widely different perceptions of the possible threats and the level of protection needed. Also, the ability to provide the necessary personnel or vigilance may be limited by budgetary considerations. As a result, the security needs of two individuals, two sites, or two organizations may be distinctly different. Security requirements of one may be viewed by another as an unnecessary constraint that inhibits utility and increases cost.

[11] Privacy is taken to mean the rights of a party to maintain control over and confidentiality of information about itself.

In an attempt to impose order on this seemingly chaotic situation, one approach would be to require all networks that comprise and interconnect with the NREN to use hardware and operating system software that are certified at some minimum level of security. Extensive study is required to ascertain the feasibility of such a requirement.

A recent report by the National Research Council (NRC) points out that there is no clear articulation of a security policy for general computing and this is regarded to be a major impediment to improved security in computer systems [NRC91]. To remedy this deficiency, the report goes on to recommend the development of a set of Generally Accepted System Security Principles. Such principles would form a functional basis for specifying security requirements and would serve as a target in the specification of higher level policies.

In addition to the NRC report, the need for security policies at all levels, including a national policy, is made clear by:

1. a plethora of reports on security violations over the last two decades that have plagued private, State and Federal organizations;
2. the growing concern of the U.S. Government on the matter of computer security[12] –
   - Privacy Act of 1974 [USPL74] - [to amend title 5, United States Code ... to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes];
   - Small Business Computer Security and Education Act of 1984 [USPL84a] - [to amend Small Business Act to establish a small business computer security and education program, and for other purposes];
   - Computer Fraud and Abuse Act of 1984 [USPL84b] - [clarifies unauthorized access to Federal computers, explicitly making it a crime and establishing penalties for violation];
   - Computer Fraud and Abuse Act of 1986 [USPL86a] - [to amend Public Law 99-474 to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes (amends Financial Institutions Regulatory and Interest Control Act of 1978)];
   - Electronic Communications Privacy Act of 1986 [USPL86b] - [to amend Title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes] - updates previous wiretap and privacy laws to protect such things as remote computer services, electronic mail, and other communications technologies, including cellular phones and fiber-optic transmissions;
   - Computer Security Act of 1987 [USPL87] - [to provide for a computer standards program with the National Bureau of Standards, to provide for Government-wide computer security, and to provide for training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes] - defines sensitive information as any unclassified information which, if lost, misused, or accessed or modified without authorization, could affect the privacy of individuals; and

[12]The Federal Acts cited here along with subsequent amendments may be found in the U.S. Code [USC91].

- High Performance Computing Act of 1991 - [The High-Performance Computing Program shall provide "for the security requirements, policies, and standards necessary to protect Federal research computer networks and information resources accessible through Federal research computer networks, including research to establish security standards for high-performance computing systems and networks"]; and

3. ethics statements recently published by national organizations and working groups –

   - NSF Code of Ethics [NSF89] - cites as unethical any activity which purposely or through negligence
     - disrupts the intended use of the networks,
     - wastes resources through such actions (people, bandwidth, or computers),
     - destroys the integrity of computer-based information,
     - compromises the privacy of users, and
     - consumes unplanned resources for control and eradication;
   - Internet Code of Ethics [IAB89] - characterizes as unethical and unacceptable any activity which purposely
     - seeks to gain unauthorized access to the resources of the Internet,
     - disrupts intended use of the Internet,
     - wastes resources (people, capacity, computers) through such actions,
     - destroys the integrity of computer-based information, and
     - compromises the privacy of users; and
   - Educom Code for Software and Intellectual Rights [EDUC91] - among other things, it states that sanctions against members of the academic community may be warranted in the event of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations.

3.5 Examples of Existing Organizational Policies

The intent of this section is to illustrate the difference in security policies and practices among the constituency of the Internet and emerging NREN. This diversity underscores the need for a national set of guidelines that will serve as model for constituents to emulate and interpret.

Many industrial organizations, Federal agencies, universities, and research laboratories have developed, or are in the process of developing, security policies for their networks. Three such policies are singled out and summarized below – two from Federal agencies and one from a university academic department.[13]

[13]Policies from major industrial organizations were not available for study.

3.5.1 A Federal Agency Policies

The Federal agencies are required by public law and national policy to establish security programs in an effort to assure adequate security for their automated information systems, whether maintained in-house or commercially. As a result, security policy statements and associated practices in the Federal agencies tend to be very well-developed and comprehensive in their coverage. In developing organization-specific policies and practices, much information can be derived from approaches taken by the Federal agencies.

NASA

The National Space and Aeronautics Administration (NASA) is an example of a Federal agency that has a high need for security of unclassified information (as well as classified). As a result, NASA has developed well-defined security policies and practices – articulated in a collection of documents. Security documents exist for both general and installation-specific use.

Examples of general documents are:

1. Security Policy [NASA88b] - establishes policy and responsibilities for ensuring appropriate levels of security and integrity for NASA installations, systems, data, and related resources (applicable to NASA headquarters and field installations); and
2. Security Handbook [NASA90b] - covers computer security management processes to assure that scientific missions and business functions are carried out in an accurate, safe, accountable, and efficient manner (intended for use by Program Office and Center computer security managers and is applicable to all NASA organizations and NASA support contractors).

Another document [NASA90a] specifies a security policy and associated practices that apply to any automated information system (AIS) that is connected to the NASA Communications (Nascom) system. It is applicable to NASA centers, field organizations, program offices, contractors, and also to foreign countries that use any component of Nascom. The document specifies such things as

- policy for limiting unauthorized access of an AIS to Nascom,
- security requirements and practices of an AIS along with procedures for self-certification,
- common vulnerabilities, and
- procedures to follow for requesting waivers and new interfaces.

Two additional documents provide policy standards and guidelines for control and responsibilities for their Lewis Information Network [NASA88a, NASA88c].

The sample NASA documents demonstrate the existence of a detailed, comprehensive, well-articulated set of security policies and practices – successfully addressing the fundamental issues of objectives, scope, goals, responsibilities for compliance, and public law authorizations (which include consequences of violation).

DOC

The Department of Commerce (DOC) consists of several Federal agencies. Both policy statements and expected practices have been published in a single manual to serve as a comprehensive guide to developing an effective information technology security program [DOC88]. The manual is based on more general policies, promulgated by the Office of Management and Budget, that address the security of all Federal automated information systems [OMB85].

The DOC Information Technology Security Manual refers to its authority - statutory, regulatory, and policy framework and provides a brief description of scope and applicability. Individual sections are typically organized to contain first a general "statement of policy" for a specific area of concern, followed by expected practices and/or assignment of responsibilities. General responsibilities are described for the following levels: department, operating unit, information technology installation, and user. Areas of concern that are addressed in individual chapters of this manual include: personnel security, procedural security, physical security, environmental safeguards, software security, hardware security, telecommunications security, small systems/microsystems/office automation, operational security, and processing of classified information.

The policy contains statements for objectives, scope, specific goals, and responsibilities for compliance. Since authority is granted by primarily Federal laws, one may presume that these same laws specify penalties for violations.

3.5.2 University Departments and Research Laboratories

General Discussion

Compared with industry and the Federal agencies, the computer security of many university academic departments and research laboratories tends to be more lax. Several reasons for this can be cited.

1. Confidential administrative information such as student and personnel records, carry high levels of protection, but there is less concern about other information and computing facilities. Unless databases of general interest are being maintained, the information is usually not of interest to other individuals. The potential consequences of intrusion are less severe.

2. Academia and research, in general, are (sometimes falsely) viewed as "pinnacles" of honesty and integrity. Although there may be some concern about theft of research results, researchers and educators often tend to be complacent about security concerns.

3. Research results are ultimately shared with the world (temporarily delayed perhaps by copyright, patent, or publication acceptance considerations). This is contrasted with industry or the military environments where prolonged tight secrecy may be critical for competitive advantage or survival – economic or military.

4. Staffing for general computing is often limited and oriented to visible service. Low-cost budgets often do not allow for attention to be focused on security. Security may be viewed as costly

and of lower priority.

5. The distribution of computing facilities among numerous autonomous units makes it difficult to formulate and enforce an organizational policy.

As a result, many research and instructional laboratories, computing centers, workstations, and personal computers are at best protected only by the "login" authentication mechanism and standard file protection as provided by some operating systems. Auditing facilities are often not available or not enabled. Weak, if any, policy statements exist.[14]

A University Academic Department Policy

This section presents the existing Code of Ethics for the Computer Science Department at Iowa State University – chosen for its availability rather than for its redeeming virtues.[15]

Taken as a statement of policy, the Code of Ethics exhibits both deficiencies and strong points. On the positive side, it states how computer accounts are to be acquired and enumerates certain activities that are disallowed. It cites the Code of Iowa and University regulations as the authority for its existence. For specific penalties in the event of noncompliance, it refers to university documents dealing with academic dishonesty that are known to be complete and specific. On the other hand, the statement lacks organization which can lead to misinterpretation; the goals and objectives are somewhat vaguely stated; the particular threats are embedded in rules that itemize disallowed behavior; and responsibility for compliance is specified only for users - nothing is specified for system administrators and management.

[14] In university environments, academic departments often rely on a general university policy statement that covers all forms of academic dishonesty – with computer security violations regarded as a special case.

[15] No inference should be made on the existence or quality of policies of other departments, laboratories, or centers at Iowa State University or any other university.

COMPUTER CODE OF ETHICS
DEPARTMENT OF COMPUTER SCIENCE
IOWA STATE UNIVERSITY†

Modern computer technology places a huge amount of power and information in the hands of its users. This power carries with it an equal amount of responsibility. Computer information should be treated no differently than the written word. Viewing and using another person's computer files, program or data without authorized permission is an invasion of privacy. Such behavior, if used for personal gain, is considered plagiarism. Ethical standards apply even when material is left unprotected.

The following statements are considered guidelines for ethical use of the computing facilities in the Department of Computer Science at Iowa State University:

- Use of computers by an individual must be authorized by the Department of Computer Science. In the case of class accounts, such authorization is generally requested by the instructor on behalf of the students and accounts are established for the duration of the course. In the case of individual accounts that are not class-affiliated, the authorization must be requested by the individual or sponsoring professor from a designated department administrator.
- Once authorized and unless otherwise specified, the account becomes the responsibility of its owner and is to be used solely for authorized purposes. For example, a class account is to be used for purposes consistent with the requirements of the course with which it is associated. Use of the account by other individuals or on behalf of other individuals is prohibited.
- Users are expected to take reasonable precautions to guard against unauthorized use of their accounts or access to confidential information through careful selection of passwords and protection of files.
- Users must not browse, access, copy, or change private or public files for which they clearly have no authorization. Also disallowed is the modification of the computer system, damage or alteration of software, and the copying of software specifically licensed for use by the department or university.
- Computing facilities are a valuable resource and should be used as efficiently as possible in order to minimize any adverse impact on others, e.g. excessive game playing should be avoided and must be avoided entirely whenever it negatively impacts the accessibility of the computing resources.
- Sending rude, obscene, or harassing materials via any electronic mail facility is strictly forbidden. Also disallowed are random mailings and any message of commercial or political nature.
- Hardware, software, manuals, supplies, etc. must not be removed from computing sites.
- Abuse or misuse of any computer hardware or software resource will be regarded as illegal and/or unethical behavior. Any observed or suspected violations are to be reported to the instructor or department administrator.

Computer Science facilities are the property of Iowa State University and the State of Iowa and as such, their use is governed by departmental and university regulations and by State laws. Violation of this code of ethics will be treated like any other ethical violation as outlined in the *Student Information Handbook* and applicable faculty and staff handbooks. Violators may be billed for illegal use and may be prosecuted under Chapter 716A, *Computer Crime* of the Iowa Code.

---

†Adapted from the Iowa State University Computer Code of Ethics, September, 1988. Revised August, 1991. Reprinted with permission from the Iowa State University Department of Computer Science.

3.6 Draft Policy for Secure Operation of the Internet

In response to the need for a national network security policy, a set of security guidelines for operating the Internet has been recently proposed [PETH91]. This is apparently the first organized U.S. attempt to formulate a security policy for wide-area networks. As pointed out by Van Bokkelen [VBOK90], the Internet is a co-operative endeavor and its usefulness depends on reasonable behavior of every individual and on the secure operation of its components. The guidelines address the responsibilities of various constituents - users, host and site administrators, vendors, and computer and service providers.

The authors of the Internet document specify six security guidelines which serve as the fundamental policy along with an elaboration into a set of practices and procedures. They also present five additional guidelines for improving local security. The following is a description of the Internet security guidelines, paraphrased or summarized (and interpreted in minor ways) by the author of this report.

The six basic Internet guidelines are:

G1. Understand and respect security policies - individual accountability (users).

Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.

G2. Employ available security mechanisms and procedures

Users have responsibility to employ available security mechanisms and procedures for protecting their own data. They also have responsibility for assisting in the protection of the systems they use.

G3. Maintain security of systems.

Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.

G4. Provide systems that embody security controls.

Vendors and system developers are expected to provide systems which are sound and embody adequate security controls.

G5. Cooperate to provide security.

Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.

G6. Seek technical improvements. Design and develop protocols with security considerations.

Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

The following is a description of the elaborations, paraphrased and/or summarized (and interpreted in minor ways) by the author of this report.

G1. Understand and respect security policies - individual accountability (users).

- G1.1. Do not exploit security weaknesses. Be aware of and adhere to security policies.
- G1.2. Obey all applicable national and state laws.
- G1.3. Assume responsibility for access to all assigned resources. Sharing of accounts and access to resources is discouraged. Specific rules governing sharing and protection are locally determined.

G2. Employ available security mechanisms and procedures (users).

- G2.1. Handle account privileges in a responsible manner.
- G2.2. Follow site procedures for security of personal data as well as for system.
- G2.3. Select and maintain good passwords.
- G2.4. Use file protection mechanisms to maintain appropriate file access control.

G3. Maintain security of systems (computer and network service providers).

- G3.1. Responsibility for security rests with owners and operators of subscriber components of the Internet.
- G3.2. Sites that operate an open, unprotected system may be providing a platform for attacks on other hosts. They are responsible for the behavior of systems' users and should be prepared to render assistance to other sites when needed. Whenever possible, sites should try to ensure authenticated Internet access.
- G3.3. Sites are encouraged to develop security policies and communicate them to their users and subscribers. The Site Security Handbook [HOLB91] should be freely consulted for guidance.

G4. Provide systems that embody security controls (vendors and system developers).

- G4.1. Evaluate security controls in systems prior to introduction into computing community. Each product should describe the security features it incorporates.
- G4.2. Repair security flaws in marketed systems. Cooperate with the Internet community in reporting security flaws and making fixes available.

G5. Cooperate to provide security (users, service providers, vendors).

- G5.1. Notify other sites if a penetration in progress at another site is detected. Sites should assist each other in responding to security violations.
- G5.2. Cooperate in finding the violator and assist in enforcement efforts.

G6. Seek technical improvements. Design and develop protocols with security considerations.

- G6.1. Improve basic mechanisms already in place - tools to administer password assignment, use of better authentication technology, gear defaults on delivered systems to technically unsophisticated users.
- G6.2. Extend security on protocol suite - network management, routing, file transfer, telnet, mail, etc.
- G6.3. Improve design and implementation of operating systems - more emphasis on security and the quality of implementation of security.

The following is a description of the Internet guidelines specific to local security, paraphrased or summarized (and interpreted in minor ways) by the author of this report.

A1. There must be a clear statement of local security policy which is communicated to users and other relevant parties.

A2. Adequates security controls must be implemented - at a minimum password control, sound management of passwords, and configuring the system to protect itself and information in it.

A3. There must be a capability to monitor security compliance and respond to security violations.

- A3.1. Logs of logins, attempted logins, other security-related events, along with a regular audit of these logs is recommended.
- A3.2. Connections and other events should be traced in response to penetrations.
- A3.3. Privacy of network users should be kept in mind.

A4. There must be an established chain of communication and control to handle security matters.

- A4.1. Responsible security contact persons should be identified and made known to all users, registered in public directories, and be easily discovered by computer emergency response centers.
- A4.2. Security contacts should be familiar with the technology and configuration of all systems under their jurisdiction or be able to reach such an individual.
- A4.3. Security contacts should be pre-authorized to deal with a security incident or able to contact such an authorized person.

A5. Sites and network should respond to reports of a security incident in a timely and effective manner.

- A5.1. Resources and capabilities should be allocated to identify the nature of an incident and limit the damage.
- A5.2. Upon identification of the the violator, appropriate action should be taken to ensure no further violations occur. The choice of sanctions depends on the nature of the incident and the site environment.
- A5.3. Sites and networks have the responsibility to respond to notifications of security flaws by installing fixes in their systems as they become available.

3.7 Conclusion

The lack of a formal national network security policy is considered an impediment to the improved security of information in computer and communication systems. The mandate to develop such a policy is clear from existing laws and statements of numerous authoritative bodies. An examination of several existing policies illustrates the diverse set of security requirements among the Internet constituency and underscores the need for national guidelines. The Guidelines for Secure Operation of the Internet appears to be the first organized attempt to address this deficiency.

3.8 References

CAMP91 Campbell, J., *From tuples to trusted databases in TDI: a brief tutorial on trusted database management systems,* Proceedings of the National Computer Security Conference, pp. 1-12, (October 1991).

CEC91 Commission of the European Communities, *Information technology security evaluation criteria (ITSEC), provisional harmonised criteria,* Office for Official Publications of the European Communities, Luxembourg, (June 1991).

CLAR87 Clark, D. and D. Wilson, *A comparison of commercial and military computer system security policies,* Proceedings of the 8th Symposium on Security and Privacy, pp. 184-194, (1987).

CLAR88 Clark, D. and D. Wilson, *Evolution of a model for computer integrity,* Proceedings of the National Computer Security Conference, pp. 14-27, (October 1988).

DOC88 U.S. Department of Commerce, *Information technology security manual,* Office of Information Resources Management, DOC, (August 1988).

DOD85 Department of Defense, *Trusted computer system evaluation criteria,* DOD 5200.28-STD, Washington, D.C., (December 1985).

EDUC91 EDUCOM, *The Educom Code – software and intellectual rights,* Educom Review, p. 13, (Spring 1991).

HOFF91 Hoffman, L. and P. Clark, *Imminent policy considerations in the design and management of national and international computer networks,* IEEE Communications Magazine, pp. 68-74, (1991).

HOLB91 Holbrook, P and J. Reynolds, *Site Security Handbook,* Internet RFC 1244, (July 1991).

HUBB90 Hubbard, B, et al, *Computer system intrusion detection,* E002 Final Report, Trusted Information Systems, (September 11, 1990).

IAB89 Internet Activities Board, *Ethics and the Internet,* Communications of the ACM, Vol. 32, No. 6, p. 710, (June 1989).

NASA88a NASA Lewis Research Center, *Lewis Information Network (LINK) - Guidelines for control and responsibilities,* NASA, F-44-897, (February 9, 1988).

NASA88b NASA, *Assuring the security and integrity of NASA automated information resources,* NMI 2410.7, NT/Information Resources Management Office, (July 8, 1988).

NASA88c NASA Lewis Research Center, *Lewis computer networking policy standards,* F-44-912, (August 26, 1988).

NASA90a *NASA communications (Nascom) access protection policy and guidelines,* (May 1990).

NASA90b NASA Information Resources Mangement Office, *NASA automated information security handbook,* NB 2410.9, (September 1990).

NSF89 National Science Foundation, *NSF poses code of networking ethics,* Communications of the ACM, Vol. 32, No. 6, p. 688, (June 1989).

NRC91 National Research Council, *Computers at risk - safe computing in the information age,* National Academy Press, (1991).

OMB85 Office of Management and Budget, *Management of Federal information systems,* Circular No. A-130, (December 12, 1985).

OTA87 Office of Technology Assessment, Congress of the United States, *Defending secrets, sharing data, new locks and keys for electronic information,* OTA-CIT-310, (October 1987).

PARK91 Parker, D., *Restating the foundation of information security,* Proceedings of the National Computer Security Conference, pp. 480-492, (1991)

PETH91 Pethia, R., S. Crocker and B. Fraser, *Guidelines for the secure operation of the Internet,* Internet RFC 1281, (September 30, 1991).

RUTH89 Ruthberg, Z. and W. Polk (editors), *Report of the invitational workshop on data integrity,* Special Publication 500-168, National Institute of Standards and Technology, (September 1989).

SCHE86 Schell, R. and D. Denning, *Integrity in trusted database systems,* Proceedings of the Ninth National Security Conference, pp. 30-35, (September 1986).

SCHO91 Schou, C. and J. Kilpatrick, *Information security: can ethics make a difference?,* Proceedings of the National Computer Security Conference, pp. 305-312, (October 1991).

SNAP91 Snapp, S., et al, *DIDS (distributed intrusion detection system) - motivation, architecture, and an early prototype,* Proceedings of the National Computer Security Conference, pp. 167-176, (October 1991).

STER91a Sterne, D., *On the buzzword "security policy",* Proceedings of the IEEE Symposium in Security and Privacy, (1991).

STER91b Sterne, D., M. Branstad, B. Hubbard, B. Mayer, and D. Wolcott, *An analysis of application specific security policies,* Proceedings of the Annual Computer Security Conference, pp. 25-36, (October 1991).

USC91 United States Code Annotated, *Title 18 crimes and criminal procedures, Section 1030, 1991 Cumulative Annual Pocket Part,* pp. 222-226, West Publishing Company, St. Paul, MN.

USPL74 *Privacy Act of 1974,* PL 93-579, U.S. Statutes at Large, Vol. 88, Part 2, pp. 1896-1910, (1974).

USPL84a *Small Business Computer Security and Education Act of 1984,* PL 98-362, U.S. Statutes at Large, pp. 432-434, (1984).

USPL84b *Computer Abuse and Fraud Act of 1984,* PL 98-473, U.S. Statutes at Large, (1984).

USPL86a *Computer Fraud and Abuse Act of 1986,* PL 99-474, U.S. Statutes at Large, pp. 1213-1216, (1986).

USPL86b *Electronic Communications Privacy Act of 1986,* PL 99-508, U.S. Statutes at Large, pp. 1848-1873, (1986).

USPL87 *Computer Security Act of 1987,* PL 100-235, U.S. Statutes at Large, pp. 1724-1730, (1987).

VBOK90 Van Bokkelen, *Responsibilities of host and network managers - a summary of "oral tradition" of the Internet,* Internet RFC 1173, (August 1990).

4 Proposed Security Policy for Use of the NREN

4.1 Objectives

As described by recent Federal legislation, the NREN will be a cooperative endeavor that will affect the U.S. research and education communities in many ways – economic, social, and cultural. Its usefulness will depend on the reliable operation of its components and on the reasonable behavior of those who use, manage, and operate it.

Stored, processed, and transmitted information is vulnerable to compromises of security – confidentiality, integrity, and availability. The relative importance of security varies among individuals and organizations as does the reasons for its importance - legal, ethical, competitive advantage, fiducial, military, and personal. Security measures tend, over time, to be proportional to the degree of reliance on the information and associated systems, and on the magnitude, probability and costs associated with loss of security. As a result, one can expect significant variances in the security measures implemented by autonomous interconnecting networks.

In order to establish a common basis for trust between communicating end users, it is imperative that a security policy for use of the NREN be developed, one that can be adopted by all major constituents. The objective is to provide a framework for:

1. establishing guidelines for protecting information, computer systems, and telecommunication systems that
   - will safeguard the rights of individuals with regard to personal privacy and protect intellectual and industrial property rights, and
   - is effective and acceptable to both the public and private sector;
2. encouraging responsible security practices in all sectors and at all organizational levels; and
3. developing generally agreed upon minimum guidelines for secure communication and information sharing in a distributed network environment that
   - can be interpreted and implemented according to the needs of individual constituents, and
   - will motivate vendors (in terms of the products they produce) and users (in terms of the products they purchase).

4.2 Scope of the Policy

This security policy is concerned with the confidentiality, integrity, and availability of all stored, processed, and transmitted information as it applies to use of the NREN. The focus is on the potential compromise of these properties that may result from accidental or deliberate acts of users. Discussion of expected professional and ethical behavior that does not directly impact security should appear in a more encompassing "Code of Ethics."

This policy addresses the use of all components of the NREN, both hardware and software (e.g. PCs, workstations, hosts, routers, gateways, transmission links, etc.) and applies to all individuals and organizations (at the local, regional, and national levels) who may affect or be affected by the security:

- vendors and system developers - suppliers of software/hardware for user terminals and hosts, routers, gateways, backbones, and other network components;
- service providers - public carriers and other commercial enterprises that provide basic services or value-added services for operation of the NREN;
- individuals and organizations - end users, system administrators, security officers, management at all levels; and
- the Federal Networking Council (FNC) as the national steering organization

For purposes of this report, it is assumed that the latter committee will be charged with asserting this policy, deriving its authority from an appropriate agency or body of the Federal government.

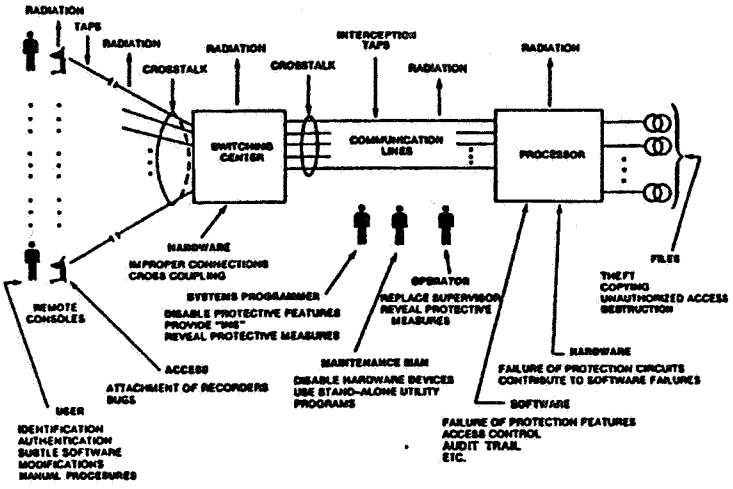
4.3 Vulnerabilities and Threats

It is generally conceded that it is not possible, using current technology, to build a system that is invulnerable to high-grade threats [NRC91] – characterized by:

1. extensive available resources in terms of money, personnel, and technology;
2. sustained patience and motivation;
3. a capability of exploiting a successful attack for maximum long-term gain;
4. a capability of circumventing physical and procedural safeguards and an access to clandestine technology; and
5. deliberate exploitation of the most obscure vulnerability hidden in the darkest corner of a system.

An alternative to total elimination of vulnerabilities or threats is "Risk Management (RM)" [FITE89, KATZ87]. It is considered by many to be "necessary" for any effective comprehensive security program and it may be employed at any level - networks, sites, hosts, and end workstations or personal computers.

The RM process requires defining the inter-relationships of threats, threat frequencies, vulnerabilities, safeguards, risks, outcomes, etc. as they apply to a specific operational environment. Because of subjectivity in such things as the valuation of assets and calculations of risks, two teams performing risk management may come up with different sets of solutions. In order to maintain credibility, participation of key individuals at all levels of an organization is recommended – from technical specialists as advisors through executives as the ultimate decision makers.



According to [KATZ87], risk management is the process of

- risk analysis - estimating potential losses due to the use of or dependence upon automated information system (AIS) technology;
- vulnerability analysis - analyzing the vulnerabilities of the AIS that contribute to loss; and
- implementing safeguards - selecting and implementing cost-effective safeguards that reduce the risks to acceptable levels.

Depending on the needs of the individual or organization, RM determines the safeguards that must be installed to minimize the risk of intrusion – installing security alarms in secure areas, placing backup tapes in fire proof vaults, training personnel in security awareness, implementing internal audit controls in a computer system, installing password management systems, retrofitting operating systems to meet specific levels of security, etc.

In a typical computer installation or network, there may be numerous points of vulnerability. The threat of exploitation of a particular vulnerability will vary from one computer/network to another. At any particular point, the type of attack (active or passive) that may take place is directly related to the particular characteristics of the hardware (e.g. processor, storage device, printer, transmission media), security of the software (application program, operating system, communication packages), and the trustworthiness of key personnel. Representative points of vulnerabilities and associated threats are pictorially represented in the diagram shown above.[16] The diagram can be readily extended to a general network and adjusted to reflect current technology. Elaborations would include

[16]Reproduced from [GSA88]. This diagram first appeared in [WARE67].

such things as threats to the integrity of files and message streams, and denial of availability to resources of all types. Specific details would depend on the nature of the resources and should be itemized in the RM process.

4.4 Responsibilities

This section describes a basic set of responsibilities that must be assumed in order to achieve a broad and consistent approach to the problem of security in using the NREN.[17] These responsibilities are grouped according to the users and organizations as identified in the scope of this policy. The responsibilities are purposely general, abstracting out details of the objects/operations and information to be protected and rising above (to the extent possible) currently employed protection technologies and organization-specific practices (The next level of refinement would begin to identify specific objects, practices, and technologies. See next section of this chapter for examples.).

1. Users

   Users are expected to be knowledgeable about and adhere to existing professional codes of ethics, security policies, and applicable laws. Users are ultimately responsible for their own behavior.

   U1. Responsible for knowing and respecting relevant State and Federal laws, codes of ethics, and applicable security policies and associated practices for systems they use.

   U2. Responsible for employing available security mechanisms for protecting the confidentiality and integrity of their own information when required.

   U3. Responsible for advising others who fail to properly employ available security mechanisms.

   U4. Responsible for notifying a system administrator or management if a security violation or failure is observed or detected.

   U5. Responsible for not exploiting security weaknesses.

   U6. Responsible for supplying correct and complete identification as required by system authentication processes.

   U7. Responsible for using the network and computing resources in an ethical manner.

2. Management (Multi-user Hosts and Sites)

   Host and site managers are responsible for the development and implementation of effective security policies that reflect specific host/site objectives. They are ultimately responsible for ensuring that computer information and communication security is and remains a highly visible and critical objective of day-to-day operations.

   M1. Responsible for implementing effective "risk management" in order to provide a basis for the formulation of a meaningful policy.

[17] The development of this section has been influenced by several sources [BRAN91, HOLB91, NCSC88, PETH91, NRC91].

M2. Responsible for ensuring the development of a security policy appropriate for the site and commensurate with global policies, State and Federal laws.

M3. Responsible for implementing a security awareness program for all users to insure knowledge of the site security policy and expected practices.

3. System Administrators

System administrators (or designated personnel) are expected to enforce (to the extent possible) local security policies as they relate to technical controls in hardware and software, the archiving of critical programs and data, and access to and protection of physical facilities.

S1. Responsible for rigorously applying available security mechanisms for enforcement of local security policies, implementing in a timely manner available improvements in security.

S2. Responsible for advising management on the workability of the existing policies and any technical considerations that might lead to improved practices.

S3. Responsible for securing computer systems and networks within the site and interfaces to global networks.

S4. Responsible for responding to emergency events in a timely and effective manner.

S5. Responsible for employing standardly available and generally approved auditing tools to aid in the detection of security violations[18] and actively participating in the continuing process of educating local users who, through carelessness or ignorance, are observed to violate security.

S6. Responsible for remaining informed on NREN policies and recommended practices and, when appropriate, informing local users and advising management of changes or new developments.

S7. Responsible for communicating and cooperating with other sites connecting to the NREN and emergency response centers for purposes of information exchange in response to perceived threats or observed security violations.

S8. Responsible for judiciously exercising the "extraordinary" powers and privileges that are inherent in their duties. Privacy of users should always be a major consideration.

4. Federal Networking Council

The Federal Networking Council (FNC) will serve as the principal body in coordinating security activities for the NREN. Its membership is expected to represent all major constituent groups that have a vested interest in NREN and its security - users, industry, Federal agencies, universities, research laboratories, and others. The responsibilities listed below may be delegated by the FNC to other appropriate agents.[19]

N1. Responsible for approving, modifying as necessary, and promulgating NREN security policies to the user communities, vendors, system developers, and service providers. Policies must be consistent with the need for interoperability with the larger Internet.

[18] Caution must be exercised to avoid violation of personal privacy.

[19] In this context, "agent" means an agency and/or working group with appropriate representation, authority, and resources to achieve the agreed upon objectives.

N2. Responsible for establishing standards for "interface" connectivity to the NREN.

N3. Responsible for establishing rules of access to selected portions of the NREN for the purpose of development and experimentation of improved hardware/software protocols.

N4. Responsible (through working committees) for interacting with various other agencies and groups (e.g. emergency response centers, vendors, system developers, and service providers) in order to insure effective dissemination of information and to remain apprised of problem areas and other developments.

N5. Responsible for interacting with national and international standards committees on networking and related security issues in order to assure interoperability with the at-large Internet.

N6. Responsible for preparing reports for appropriate government agencies as input to organizations responsible for Federal policy on such matters as regulatory practices, laws, and penal codes, and research agendas for Federal funding.

5. Vendors and System Developers

Vendors and systems developers are responsible for providing systems that embody adequate security controls to meet the needs of user organizations.

V1. Responsible for employing sound development methodology for secure software and systems.

V2. Responsible for seeking technical improvements to security of products.

V3. Responsible for correcting security flaws discovered in existing products and making the user community aware of these flaws in a timely manner.

6. Computer Network and Service Providers

Service providers are responsible for providing reliable, secure, and transparent services.

P1. Responsible for providing services commensurate with the security and reliability needs of major groups of users and making users aware of various available service options.

P2. Responsible for seeking technical improvements to security of components that individually and collectively impact the security of the NREN.

P3. Responsible for cooperating with the Federal Networking Council to provide network access for the development of new protocols.

4.5 Examples of Second-Level Refinements of Responsibilities

This section provides some examples of how the basic responsibilities (specified in the previous section) can be refined into "second-level" specifications.[20]

1. Users

U2.1. Handle accounts in a responsible manner.

U2.2. Follow site procedures for security of personal data as well as for the computer system. Use file protection mechanisms to maintain appropriate file access control.

U2.3. Select and maintain good passwords. Do not share accounts.

U3.1. Help to protect the property of other individuals. Notify them of resources (e.g. files, accounts) left unprotected.

U3.2. Notify the System Administrator of a suspected or observed violation.

U5.1. Do not intentionally modify, destroy, read, or transfer information in an unauthorized manner; do not intentionally deny others authorized access to or use of network resources and information.

U5.2. Provide the correct identity and authentication information when requested and not attempt to assume any other party's identity.

2. Management (Multi-user Hosts and Sites)

M1.1. Risk management requires identification of the assets to be protected, assessing the vulnerabilities, analyzing risk of exploitation, and implementing cost-effective safeguards. The participation of managers, system administrators, and technical personnel is recommended.

M2.1. All levels of an organization should participate in the development of a security policy to ensure that it is meaningful and implementable. Individual sites may place more value on some aspects of computer security than on others.

M2.2. The policy should be a concise high-level statement that includes 1) a citation of governing laws and higher level policies, 2) objectives, 3) scope, 4) specific goals, and 5) responsibilities for compliance and actions to be taken in event of noncompliance.

M2.3. At a minimum, a copy of the security policy and the site handbook (if any) should be given to each user prior to establishing an account for the user.

3. System Administrators

[20] The notation Xn.m indicates refinement m of responsibility Xn.

S4.1. Notify other sites if a penetration is in progress, assist other sites in responding to security violations.

S4.2. Cooperate, when appropriate, with other sites in finding violators and assist in enforcement efforts.

S5.1. Develop or adopt an existing site handbook that spells out specific practices and communicate the information to users.

S5.2. Conduct timely audit of system logs.

S7.1. Identity of System Administrator should be registered in a public director for easy discovery by computer emergency response centers.

4. Federal Networking Council

5. Vendors and System Developers

V1.1. To support identification and authentication of users in multiuser systems, implement operating system features (at a minimum) for password control and tools for sound management of passwords.

V1.2. For auditing of computer usage in multiuser systems, implement an operating system monitor for recording security related events (e.g. logins, attempt to non-owned files) or more sophisticated intrusion detection mechanisms.

6. Computer Network and Service Providers

P1.1. Responsible for providing reliable and transparent network services that support the transmission of encrypted and signed data, certificates, and security management information.

4.6 Definitions

Access Control: The process of limiting access to resources of a system only to authorized programs, processes, or other systems (in a network).

Accountability: The property of being able to trace activities on a system to individuals who may then be held responsible for their actions.

Administrative domain: A logical collection of hosts and network resources (e.g., department, building, company, organization) governed by common policies.

Authentication: 1) The process of verifying a claimed identity of a user, device, or other entity in a computer system; 2) the process of verifying the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized access.

Authorization: The process of initially establishing access privileges of an individual and subsequently verifying the acceptability of a request for access.

Availability: The state that exists when data can be accessed or a requested service provided within an acceptable period of time.

Confidentiality: The state that exists when information is held in confidence and protected from unauthorized disclosure.

Data: A representation of information as stored or transmitted.

Domain: A logical structure, group or sphere of influence over which control is exercised.

Information: Data that has semantic content (i.e. meaning) in a certain context.

Integrity: The property of information that exists when data has been modified only in a specified and authorized manner (e.g., not modified or destroyed in an accidental or unauthorized, intentional manner).

Manager: An individual responsible for network resources (people, data, processing capability) who is charged with conducting business of an an organization.

Non-repudiation: The inability to deny responsibility for performing a specific act.

Party: An individual, group or an organization participating in an action.

Policy: A statement of objectives, rules, practices or regulations governing the activities of people within a certain context.

Privacy: The right of a party to maintain control over and confidentiality of information about itself.

Risk Analysis: The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is part of risk management.

Risk Management: The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Security: The state in which the integrity, confidentiality, and accessibility of information, service or network entity is assured.

Sensitive: A descriptor of information whose loss, misuse, or unauthorized access or modification could adversely affect security.

Service Provider: A provider of basic services or value-added services for operation of a network - generally refers to public carriers and other commercial enterprises.

System Administrator: Individual or group responsible for overseeing the day-to-day operability of a computer system or network. This position normally carries special privileges including access to the protection state and software of a system.

System Developer: An individual group, or organization that develops hardware/software for distribution or sale.

Threat: Any circumstance or event with the potential to cause the security of the system to be compromised.

User: A person, organization, or other entity which requests access to and uses the resources of a computer system or network.

Vendor: A commercial supplier of software or hardware.

Vulnerability: A weakness in system security procedures, system design, implementation, internal controls, etc that could be exploited to violate the system security policy.

4.7 References

BRAN91 Branstad, D., *Private Communication,* (1991).

FITE89 Fites, P., M. Kratz and A. Brebner, *Control and security of computer information systems,* Computer Science Press, (1989).

HOLB91 Holbrook, P. and J. Reynolds, *Site Security Handbook,* Internet RFC 1244, (July 1991).

KATZ87 Katzke, S., *A government perspective on risk management of automated information systems,* Proceedings of the Computer Security Risk Management Model Builders Workshop, pp. 3-20, (May 1988).

NCSC88 National Computer Security Center, *Glossary of computer security terms,* NCSC-TG-004, Version-1, (October 21, 1988).

NRC91 National Research Council, *Computers at Risk - Safe Computing in the Information Age,* National Academy Press, (1991).

GSA88 *Information Technology Installation Security,* General Services Administration, Office of Technical Assistance, (December 1988).

PETH91 Pethia, R., S. Crocker and B. Fraser, *Guidelines for the secure operation of the Internet,* Internet RFC, (September 30, 1991).

WARE91 Ware, W., *Security and privacy in computer systems,* Proceedings of the Spring Joint Computer Conference, pp. 279-282, (1967).

5 Future Work

A high-level abstract security policy was presented in Chapter 4. Additional levels of refinement are required in order to map the Level 1 policy into a specification of procedures and practices. The process of refinement would lead to more detailed policies, that might be formally specified, and an enumeration of supporting security practices (e.g. intrusion detection mechanisms) that would reflect the application of current technology (e.g. use of passwords, call-back modems). Several levels of refinement may be required and it may be necessary to expand the Level 1 policy.

In Chapter 2, the Internet and NREN were topologically depicted as a collection of autonomous interconnecting administrative domains. From a security point of view, one can visualize interconnecting security domains, each defined by a security policy. Requirements for interdomain services or communication have been investigated in several publications of the European Computer Manufacturers Association. An area of further investigation would be to develop (or adopt) a formal specification language for describing the policies of security domains and lay the foundation for specifying formal rules of negotiation (mappings between policies) that would be required for communicating entities in two distinct domains.

6 Conclusion

The purpose of this report was to explore the foundations of a national network security policy and propose a draft policy for the National Research and Education Network. Since the projected use of the NREN is far-reaching into educational institutions, research laboratories, Federal agencies, libraries, etc., the policy presented in Chapter 4 is comprehensive in its scope and responsibilities are identified for end users, management at all levels, system administrators, vendors and system developers, network service providers, and the Federal Networking Council. In its assignment of responsibilities, the policy is similar in some respects to the guidelines that have been proposed elsewhere for use of the International Internet.

The policy statement in Chapter 4 is derived from foundational issues that were explored in Chapter 3. It is considered a "first-level" policy, abstractly stated in an attempt to to remain independent of organization-specific practices and current technologies. Further refinements are necessary in order to identify actual security practices.

This report is intended to provide a basis for continuing discussion and further development. It does not propose standards and has not been reviewed or endorsed by any organization having policy authority over the NREN.

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4734

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
FEBRUARY 1992

4. TITLE AND SUBTITLE
Considerations in the Development of a Security Policy for the NREN

5. AUTHOR(S)
Dr. Arthur E. Oldehoeft

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)
U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER
PO 43NANB112737

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

The National Research and Education Network (NREN) is an integral part of the planned High-Performance Computing and Communications infrastructure that will extend throughout the scientific, technical and education communities. The problem of computer and network information security is an important issue that is complicated by the diversity of users and interconnecting networks in the NREN environment. One major impediment to improved security in computer and network systems is the lack of a clearly stated security policy for general computing.

In order to establish an appropriate context for developing such a policy for the NREN, this report traces the evolution of a "national" network in the U.S., reviews the fundamental concepts of information security and policies, and identifies the need for developing a policy. A security policy is then proposed for the NREN; one that is intended to provide the basis for continuing discussion and further development. This draft policy identifies responsibilities of all major network constituents: end users, local system administrators, management at all levels, vendors, system developers, service providers, and a national council. It is abstractly stated in order to remain independent of current technologies and organization-specific practices.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
54

15. PRICE
A04

ELECTRONIC FORM