

NISTIR 4734

NISTR
@C100
U56
4734
1992

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

