Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

Series/Number:	NIST Special Publication 800-11
Title:	The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security
Publication Date(s):	February 1995
Withdrawal Date:	
Withdrawal Note:	

Superseding Publication(s)

The attached publication has been **superseded by** the following publication(s):

Series/Number:	
Title:	
Author(s):	
Publication Date(s):	
URL/DOI:	

Additional Information (if applicable)

Contact:	Computer Security Division (Information Technology Lab)
Latest revision of the attached publication:	
Related information:	http://csrc.nist.gov/
Withdrawal announcement (link):	

Date updated: June 9, 2015

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

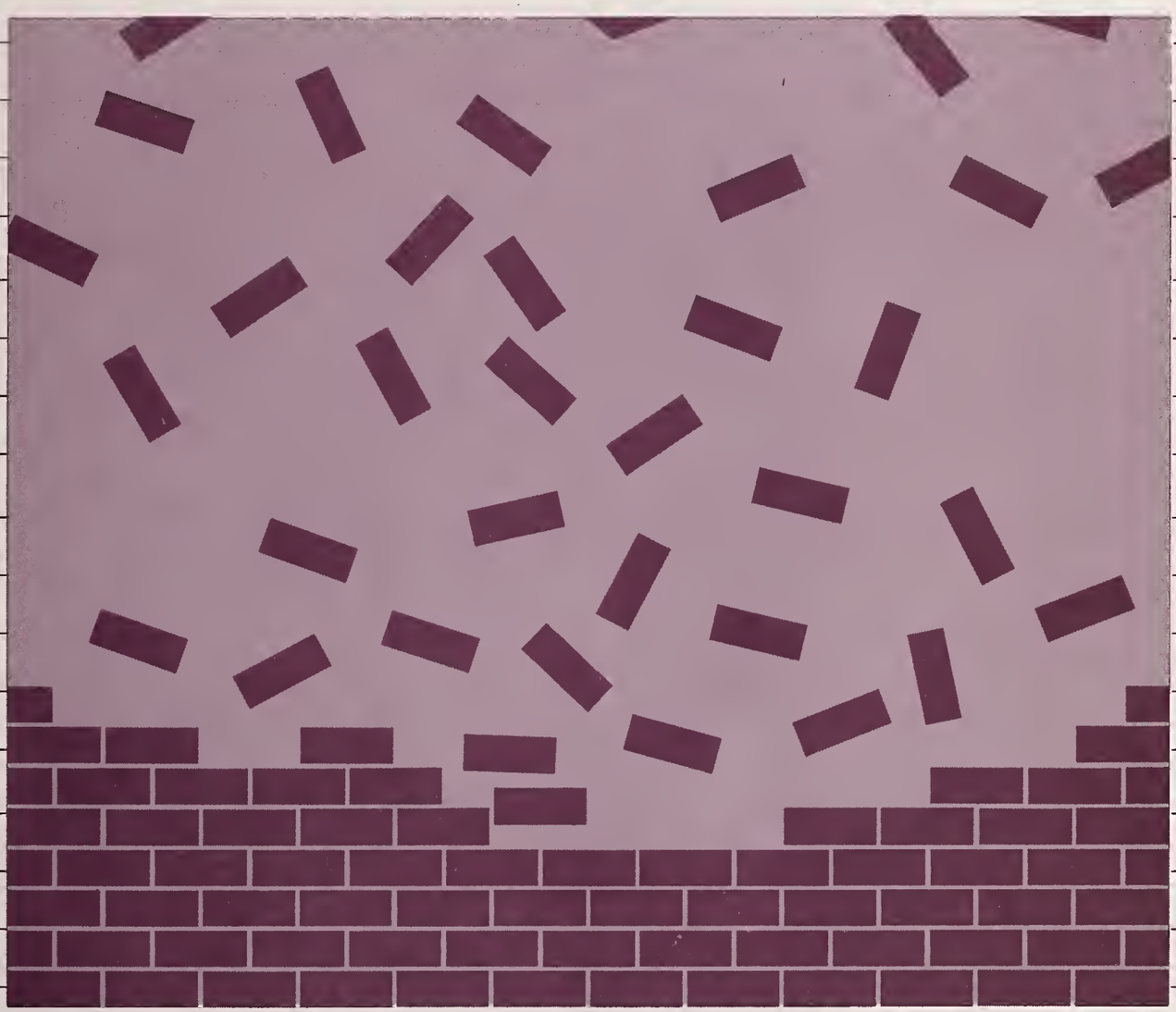
NIST Special Publication 800-11

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security

Karen Olsen and John Tebbutt

COMPUTER SECURITY



NIST

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Office of the Director
- Advanced Technology Program
- Quality Programs
- International and Academic Affairs

Technology Services
- Manufacturing Extension Partnership
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Kinetics and Thermodynamics
- Analytical Chemical Research
- Process Measurements[2]
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Intelligent Systems
- Manufacturing Systems Integration
- Fabrication Technology

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Safety
- Fire Science

Computer Systems Laboratory
- Office of Enterprise Integration
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 800-11

The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security

Karen Olsen and John Tebbutt

C O M P U T E R S E C U R I T Y

Computer Systems Laboratory

National Institute of Standards
and Technology
Gaithersburg, MD 20899-0001

February 1995

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 800 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 800-11
Natl. Inst. Stand. Technol. Spec. Publ. 800-11, 40 pages (Feb. 1995)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1995

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

Contents

Preface

A significant portion of National Security and Emergency Preparedness (NS/EP) telecommunications relies on the Public Switched Network (PSN). Therefore, NS/EP telecommunications is concerned with the protection of the PSN to ensure that telecommunications services are available and reliable. Service vendors, equipment manufacturers, and the federal government are concerned that vulnerabilities in the PSN could be exploited and result in disruptions or degradation of service. To address these threats, NIST is assisting the Office of the Manager, National Communications System (OMNCS), in the areas of computer and network security research and development. NIST is investigating the vulnerabilities and related security issues that result from use of the Federal Communications Commission's (FCC) Open Network Architecture (ONA).

This report provides an overview of ONA, describes NS/EP telecommunications security concerns, and describes NS/EP telecommunications security concerns that the FCC's ONA requirement introduces into the PSN. Conclusions are presented in Section 5.

1 Introduction

Open Network Architecture (ONA) is a regulatory framework imposed by the Federal Communication Commission (FCC) on communications carriers (the long distance telephone carriers such as AT&T and the Regional Bell Operating Companies (RBOCs)) which requires the carriers to provide competing service providers with access to basic communications services on an equal cost basis.

Because ONA involves access to communications networks by many external service providers who lie outside the administrative purview of the network owners, security concerns arise regarding such issues as authentication of the service user, control of the user's access to network facilities, and the delimitation of the scope of access to other networks granted to the user.

The aim of this paper is to assess whether the FCC's ONA requirement for nondiscriminatory access introduces additional security concerns into the Public Switched Network (PSN). Assuring the availability of National Security/Emergency Preparedness (NS/EP) telecommunications requires protection of the PSN. The targeted audience for this report includes general telecommunications managers and technical professionals in the telecommunications industry. The main body of the report was written for general telecommunications managers. Sections containing more technical information are located in the Appendix.

This paper is broken down as follows:

- Section 2 provides a description of ONA, the intent behind it, and the current state of play;
- Section 3 addresses NS/EP telecommunications security concerns, outlines assets to be protected, and describes security threats, potential impacts on NS/EP telecommunications, and sources of threats;
- Section 4 describes NS/EP telecommunications security concerns raised by the FCC's ONA requirement;
- Section 5 presents a summary of NS/EP telecommunications security concerns raised by the FCC's ONA requirement;
- A list of acronyms and references are provided; and
- Appendices A through E contain more detailed information pertaining to ONA.

2 The FCC's Open Network Architecture

In May, 1986, in its *Third Computer Inquiry*, also known as the *Computer III Decision* [1], the Federal Communications Commission (FCC) introduced the concept of an Open Network Architecture (ONA), which represents an attempt to create free market conditions within the telecommunications industry through regulation.

ONA is a regulatory framework imposed on the Regional Bell Operating Companies (RBOCs) and AT&T by the Federal Communications Commission (FCC) for the provision of enhanced communications services. ONA requirements were imposed on GTE in early 1994. Subsequent FCC orders have substantially reduced the applicability of unbundling and other aspects of ONA on AT&T. Currently, AT&T is not directly subject to ONA requirements, but is subject to Comparatively Efficient Interconnection (CEI) requirements.

Before initial ONA plans were filed, the RBOCs and AT&T were subject to Comparatively Efficient Interconnection requirements. Under Comparatively Efficient Interconnection requirements, the carrier is required to provide comparably efficient interconnection for each enhanced service that is offered, such that any Enhanced Service Provider (ESP) can access the elements of the basic telephone network in a manner that is completely equivalent to the method that carrier's enhanced services access the basic network. Comparatively Efficient Interconnection was initially used for determining interim approval of any specific enhanced service of a carrier prior to the implementation of ONA plans. For the purposes of this paper, the term *carrier* will be used to refer to those carriers subject to ONA or Comparatively Efficient Interconnection requirements.

Under Comparatively Efficient Interconnection, the set of basic service functions that a carrier uses in an enhanced service offering should be available to ESPs under tariff as a Basic Service Element (BSE) or a set of Basic Service Elements.[1] For example, if a carrier's enhanced service utilizes digital transmission, calling number identification, and specific signaling capabilities, then the Comparatively Efficient Interconnection for that service must include these basic services as a set of Basic Service Elements unbundled from other basic service offerings.

ONA mandates that the carriers should provide independent ESPs access to basic communications services on an equal basis and at an equal cost to those enjoyed by the carriers' own Enhanced Service operations. This so-called unbundling of services forces the carriers to relinquish their local monopolies on telecommunications services, creating an open market, and allowing various service providers to compete on an equal basis. The carriers are required to satisfy all ESP requests that meet the FCC's criteria of demand, utility, technical feasibility, and cost feasibility, regardless of whether the carrier plans to offer the enhanced service.

Basic services are limited to "the common carrier offering of transmission capacity for the movement of information" [21]. Enhanced Services consist of the combination of transmission and basic switching services with other services, such as services provided by computer application programs, to produce additional or restructured information, and/or involve subscriber interaction with stored information. Current examples are in the form of enhanced

[1]Note that each ONA plan describes a set of Basic Service Elements (BSEs), Basic Serving Arrangements (BSAs), and Complementary Network Services (CNSs). These services are described in more detail in Appendix C.

telephone services, such as call forwarding, voice mail, caller ID, and last number redial. In order to provide enhanced services, an ESP requires access to basic communications functions from the common carrier. Under ONA, these basic functions are unbundled from one another into tariffed basic building blocks known as Basic Service Elements (BSEs). ESPs are free to purchase these basic services individually in a way that best matches their requirements for the provision of a particular enhanced service.

Rutkowski [2] offers the following distillation of the ONA framework sketched out by the FCC in its *Computer III Decision*:

> ONA is the overall design of a carrier's basic network facilities and services to permit all users of the basic network, including the enhanced service operations of the carrier and its competitors, to interconnect to specific basic network functions and interfaces on an unbundled and equal access basis.[2]

The FCC declined to provide a specific standard for ONA [1, page 1067]. Rather, it placed the burden for the development of Open Network Architectures on the carriers. Initial ONA plans were filed with the FCC by February 1, 1988. ONA plans for each carrier are continually being amended to reflect changes in services offered and to comply with additional requirements of the FCC. Appendix A provides additional information on FCC Orders directing the development and evolution of ONA plans.

[2]Attributed to W.H.McElveen from his talk "ONA Overview and Forum Mission" given at the first national ONA Forum, Herndon, VA, Oct 28 - 29, 1986

3 NS/EP Telecommunications Security Concerns

The Public Switched Network (PSN) provides telecommunications services throughout the United States. The PSN consists of both voice and data communication networks and provides a wide range of services to a vast number of businesses, organizations, and individuals. National Security/Emergency Preparedness (NS/EP) telecommunications services are those used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States [3]. A significant portion of NS/EP telecommunications relies on the PSN, therefore, NS/EP telecommunications is concerned with the protection of the PSN to ensure that telecommunications services are available and reliable.

A 1989 report "Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness" by the National Research Council (NRC) addresses concerns that the nation's networks are becoming more vulnerable to serious network disruptions [4]. The report reached several conclusions and listed numerous recommendations to reduce network vulnerabilities. Several conclusions reached by the National Research Council are listed below:

- The evolution of switching technology is resulting in fewer switches, a concentration of control, and thus greater vulnerability of the public switched networks.
- The public switched networks are increasingly controlled by and dependent on software that will increase access to executable code and databases for user configuration of features, a situation that creates vulnerability to damage by "*hackers*," "*viruses*," "*worms*," and "*time bombs*".
- The power of optical fiber technology is diminishing the number of geographic transmission routes, increasing the concentration of traffic within those routes, reducing the use of other transmission technologies, and restricting spatial diversity. All these changes are resulting in an increase in network vulnerability.
- There is a progressive concentration of various traffic in and through single buildings resulting in increasing vulnerability. As a result this trend increases the potential for catastrophic disruption that may be caused by damage to even a single location.

In 1990, the National Security Telecommunications Advisory Committee (NSTAC) initiated the Network Security Task Force to address network security concerns. The findings of the Network Security Task Force are documented in the "Report of the Network Security Task Force" [5]. Some of the conclusions of this report are highlighted below:

- There are software security vulnerabilities in the public switched network. Some of these vulnerabilities could impact NS/EP telecommunications capabilities.
- There is a threat to the PSN in the form of computer criminals or intruders who penetrate the various systems of the PSN. The threat to software security is international and in some cases penetrations originate from overseas.

- The current risk, which is a function of vulnerabilities and threats, is highly uncertain. Until there is confidence that strong, comprehensive security programs are in place, the industry should assume that a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP telecommunications users.

As described above, reports from the National Research Council and the National Security Telecommunications Advisory Committee ([4], [5]) indicate that because of converging trends in technology, economics, and regulatory practice, the PSN is vulnerable to numerous security threats. It is possible that vulnerabilities in the PSN could be exploited and result in degradation or disruption of service. Disruption of NS/EP telecommunications services represents a threat to public safety and security. The report "Electronic Intrusion Threat to NS/EP Telecommunications" notes that hackers have the capability to launch sophisticated widespread attacks on the PSN and these types of attacks could result in significant degradation in the nation's NS/EP telecommunication capabilities, create significant public health and safety problems, and cause serious economic shocks [19].

3.1 Assets To Be Protected

This section lists many telecommunications assets that need to be protected. Assets are also referred to as PSN resources. Many of the assets that need to be protected are Operations, Administration, Maintenance and Provisioning (OAM&P) system assets. OAM&P is a set of functions used to administer/manage network elements and networks. Telecommunications assets requiring protection include the following:

1. Switches;
2. Customer, carrier, and ESP proprietary information;
3. Data, especially billing data and data that enables reconfiguration;
4. Application System software, firmware, hardware, administrative capabilities, and system functions for configuration, update, and maintenance of all hardware, firmware, and software;
5. Application System interfaces;
6. Application System control and management databases;
7. Attributes and features of each Application System component or element; and
8. Application System audit trail.

3.2 Security Threats

A *threat* is an accidental or deliberate action, event, or condition with the potential to compromise the quality, utility, or functionality of network services and operations. A threat is

the result of the exploitation of a vulnerability. For example, if a system is vulnerable because a default password is used, then it is a potential threat that an unauthorized user could exploit the vulnerability of the default password and impersonate another user. This section will focus on the most significant threats that result from the exploitation of vulnerabilities.

Threats that pose a risk to the PSN are of concern to NS/EP telecommunications because, especially when combined, they could impair the ability of the PSN to provide the full range of services required to meet NS/EP telecommunications services.

3.2.1 Denial of Service

The threat of denial of service involves actions that prevent a network element from functioning in accordance with its intended purpose. Network Elements may be rendered partially or entirely unusable for legitimate users. Denial of service may cause operations which depend on timeliness to be delayed. Examples of denial of service include:

- Unauthorized modification of existing network element resources (e.g. hardware, software, and databases) which affects the availability of the resource; and
- The degradation of network element service caused by a large volume of service requests.

3.2.2 Impersonating a User

The threat of impersonating a user, also known as masquerade, is an attempt to gain unauthorized access or greater privilege to a system, by posing as an authorized user. Examples of masquerade are using stolen logon ids and passwords, bypassing the authentication mechanism, and using security holes in programs. An example of a vulnerability that is likely to lead to masquerade is the use of weak authentication methods. Impacts on the PSN caused by threat of impersonating a user include the full range of impacts to NS/EP telecommunications described in section 3.3. Examples of potential impacts on the PSN include the deletion, disclosure, or modification of system software and data, and the deletion, disclosure, or modification of data that enables changes in routing information or reconfiguration of the network. An example of modification of system software is the re-programming of network element software to insert malicious code to steal passwords.

The threat of masquerade can occur from:

- Locally connected users;
- Outside users accessing network elements from the public network;
- Compromised administrator accounts that are configured for direct and remote access; and
- Use of dial-in modems;

3.2.3 Disclosure of Information

The threat of disclosure of information involves the unauthorized disclosure of data or information regarding network elements, either by deliberate action or by accident. Examples of disclosure of information include:

- Eavesdropping on phone conversations or on data transmission which could result in the disclosure of sensitive information such as passwords, data, and procedures for performing functions; and
- Unauthorized disclosure of routing or address information.

3.2.4 Message Stream or Data Modification

Message stream or data modification involves the deletion or modification of data. The deletion or modification of data may affect network element software or databases or it could affect network elements. Examples include:

- Unauthorized modification of billing information;
- Unauthorized modification of network element software or databases; and
- Unauthorized reconfiguration of network elements.

3.2.5 Traffic analysis

Traffic analysis is a form of passive attack in which an intruder observes data being transmitted and makes inferences from the calling and called numbers, and the frequency and length of the calls. Examples include:

- A corporate merger is deduced from the amount of traffic between two companies.

3.3 Potential Impact on NS/EP Telecommunications

As described in the previous section, there are many threats that can impair the ability of the PSN to provide the full range of services required to meet NS/EP telecommunication services. Threats can be categorized according to the following effects on assets of the PSN:

- Availability
- Privacy
- Integrity
- Fraud

The following sections describe the potential impact on NS/EP for each of the categories.

3.3.1 Denial or Disruption of Service

Denial or disruption of service attacks affect the availability of data, services, and network elements. In the past, computer intruders have crashed or disrupted signal transfer points, traffic switches, and OAM&P systems, reportedly planted destructive "time bomb" programs designed to shut down major switching hubs, and disrupted E911 services throughout the eastern seaboard [19]. For the most part, service disruptions caused by computer intruders have been brought about by accidental actions. Unintentional disruptions caused by computer intruders are much more common than malicious disruptions.

The "Report of the Network Security Task Force" presents the following conclusion [5]:

> A motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users.

3.3.2 Unauthorized Monitoring and Disclosure of Sensitive Information

This threat category covers all threats which involve the deliberate or accidental disclosure of sensitive information. The privacy of information is affected because information is exposed without authorization. The term *sensitive* not only refers to highly classified government information or proprietary information, but to all private data. Approaches used by intruders to capture data include electronic eavesdropping, use of network monitoring tools, and electronic intrusion on network elements.

3.3.3 Unauthorized Modification of Network Databases/Services

This threat category covers all threats which involve the deliberate or accidental modification of network databases and services. Threats in this category affect the integrity of data because data may have been corrupted. The integrity of network services is affected because the service may not function in accordance with its intended purpose.

The "Electronic Intrusion Threat to NS/EP Telecommunications" report notes the following about unauthorized modification of network databases/services [19]:

> Computer intruders have demonstrated a high level of technical skill in modifying PSN databases and subscriber services. They have added unauthorized accounts to service control points, service provisioning systems, digital cross-connect systems, and other network elements. They have added and modified user services, forwarded calls, modified service classes on circuits, and turned off billing on specific circuits. On data networks, computer intruders have changed the routing tables and service descriptions for specific users. This level of penetration and skill demonstrates that computer intruders could seriously compromise NS/EP telecommunications.

3.3.4 Fraud

In the past, computer intruders have been motivated by intellectual curiosity and a desire to understand the PSN. Today, computer intruders are discovering that they can sell their

services and are motivated by greed. The report "The Electronic Intrusion Threat to NS/EP Telecommunications" notes the following about fraud and financial loss [19]:

> Toll fraud is a multibillion-dollar-per-year business in the United States. Normally, the toll fraud threat is not seen as being related directly to the performance of Government agencies' ability to perform NS/EP missions. Because of the nature of this threat, toll fraud should be considered a significant problem, but one with undefined NS/EP implications [19].

3.4 Sources of Security Threats

Several reports, for example the National Research Council and National Security Telecommunications Advisory Council reports described earlier in this section ([4], [5]), have highlighted potential threats to the PSN. Primary sources of threats are employees/insiders, malicious hackers, natural disasters, foreign adversaries, and hostile attacks. In several cases, the areas for sources of threats may overlap. For example, hostile attacks may be performed by foreign adversaries or a disgruntled employee.

3.4.1 Employees/Insiders

Intentional and accidental errors and malicious acts by employees and insiders cause a considerable amount of the damages and losses experienced in the telecommunications industry. The range of employees spans from good intentioned employees that make accidental errors to disgruntled employees seeking revenge. Insiders, such as contractors who have administrative roles with respect to network service, that have a high level of knowledge and privileges pose a threat. The full range of employees and insiders increases the potential for acts that can severely impact the security of the PSN.

3.4.2 Malicious Hackers

As a result of their increasing knowledge and sophistication, hackers have the capability to affect NS/EP telecommunications services. Hackers have the capability to launch sophisticated widespread attacks on the PSN and these types of attacks could result in significant degradation in the nation's NS/EP telecommunication capabilities, create significant public health and safety problems, and cause serious economic shocks [19]. Hackers can cause a wide range of impacts on the PSN. Hackers can affect the availability of PSN components, and the integrity and privacy of all data and information. Fraud may also result.

The report "Electronic Intrusion Threat to NS/EP Telecommunications" identifies and analyzes the threat that electronic intrusion represents to the PSN and the resulting impact upon NS/EP telecommunications. The "Electronic Intrusion Threat to NS/EP Telecommunications" report notes that significant computer intruder threats arise from the following four categories: members of the computer underground, telecommunication industry insiders, industrial espionage operations, and foreign organizations. Computer intruders that are members of the four categories listed above tend to have similar motives and techniques.

For the remainder of this report, the term *computer intruder* will be used to mean those with hostile intent. Computer intruders perhaps represent the most potent source of threat

because computer intruders have the capabilities to cause the full range of threats described in section 3.2 as well as all of the impacts to NS/EP telecommunications described in section 3.3.

3.4.3 Natural Disasters

Natural disasters can impact the availability of the PSN. The primary impact of disasters such as hurricanes, floods, fires, earthquakes, tornados, and wind storms on the PSN is disruption and denial of service. Such disasters impact the timeliness and quality of the delivered services. The report "Natural and Technological Disaster Threats to NS/EP Telecommunications" provides a description of natural disaster threats and the probability of their occurrence [17].

3.4.4 Foreign Adversaries

The world's telecommunication networks reach beyond national boundaries and computer intruder activities have occurred internationally as well as throughout the United States. The number of attempted intrusions through international gateways from abroad is increasing and at least 20 foreign governments in Asia, Europe, the Middle East and Latin America have carried out economic intelligence gathering [6].

There have been few indications that computer undergrounds within foreign countries carry overt political agendas.

The report "Electronic Intrusion Threat to NS/EP Telecommunications" indicates that individual computer intruders probably would not launch orchestrated attacks on NS/EP systems and open source literature provides little significant evidence that foreign intelligence services have directly targeted, penetrated, or compromised the PSN in the United States [19]. However, there have been several cases of foreign computer intruders targeting systems in the United States and there is a large amount of circumstantial evidence and speculation regarding foreign adversaries, such as Libya, Iraq, and Iran, targeting networks in the United States [19].

3.4.5 Hostile Attacks

Through hostile attacks, it is possible to affect the availability of the PSN. The primary impact of hostile attacks such as coordinated nuclear attacks, limited/uncoordinated nuclear attacks, nuclear accidents, terrorism, electronic warfare, sabotage, and civil disorder on the PSN is disruption and denial of service. Such disasters impact the timeliness and quality of the delivered services. The report "Summary of the Threat to National Security and Emergency Preparedness Telecommunications" relies on classified source material and focuses on the hostile threat to NS/EP telecommunications [18].

It is possible for sabotage to be performed by disgruntled employees and members of adversary nations. Although the probability of sabotage is relatively low, the effect on NS/EP is high. The concentration of telecommunications resources increases the effects of strategic sabotage attacks because more telecommunication resources will be affected. The use of optical fiber increases the effects of strategic sabotage attacks because optical fiber technology is diminishing the number of geographic transmission routes, increasing the concentration of

traffic within those routes, reducing the use of other transmission technologies and restricting spatial diversity.

4 ONA NS/EP Telecommunications Security Concerns

ONA requires the carriers to provide competing service providers with access to basic communications services on an equal basis. Before ONA requirements, there were few telecommunication providers and the systems they used were built on proprietary platforms. ONA involves a shift from the *closed* telecommunications networks of the past to *open* telecommunications networks. In the past, telecommunications systems and facilities were under the exclusive control of the carriers. With ONA, the opening of the telephone network to vendors and customers of enhanced services involves significantly broadening access to telecommunications systems and facilities. In addition, varying levels of access are allowed to the telecommunications systems and facilities.

A Network Operations Forum (NOF) report notes that:

> While the advent of open systems interfaces has assisted the acceptance and international deployment of networking technology, it has also seen a downside in that it has become easier to intrude on networks designed with such open features. [7].

The communications protocols used between service elements and the majority of the services that were to become Basic Service Elements were already in existence prior to the ONA mandate. Some of the Basic Service Element offerings related to basic transport and signaling capabilities could be performed within the existing network without significant development work. Other Basic Service Element offerings, such as ISDN and OAM&P access, require modification of the existing network. Most enhanced service vendor and customer access to network signaling and information systems require additional protections to ensure security and the reliability and integrity of the network.

The National Research Council notes that ONA can increase network vulnerability in two ways:

> First, ONA increases greatly the number of users who have access to network software. In any given universe of users, some will be hostile. By giving more users access to network software, ONA will open the network to additional hostile users. Second, as more levels of network software are made visible to users for purposes of affording parity of network access, users will learn more about the inner workings of the network software, and those with hostile intent will learn more about how to misuse the network [4].

The National Institute of Standards and Technology's "Security in Open Systems" report [8] notes the following:

> Greater network access is changing the telecommunications industry to one where many third party service providers are building products that must work with products from other companies [10], [11], [12]. This new telecommunications environment has been characterized as one with: a large number of features; multi-media, multi-party services; partial knowledge of the feature set by service

designers; lower skill and knowledge levels of some service creators; multiple execution environments from different vendors; and distributed intelligence [15].

The FCC's ONA requirement for nondiscriminatory access introduces vulnerabilities into the PSN and these vulnerabilities pose a threat to NS/EP. The remainder of this section will provide a description of potential vulnerabilities introduced by the FCC's ONA requirement.

4.1 Network Elements

As a result of the open nature of ONA, network elements are potentially vulnerable to abuse. Network elements are analog and digital devices and supporting equipment that provide communication services such as switching, multiplexing, and transport services to subscribers.

All network element interfaces and ports that accept user command inputs are potentially vulnerable to unauthorized access. Security features, such as authentication, access control, audit, integrity, and administration, are necessary to protect network elements from various types of attacks leading to misuse and abuse of the software functions within a network element. If security features are not properly conceived, designed, implemented, tested, installed, documented and maintained, vulnerabilities are likely to result.

4.2 Identification and Authentication of Users

Identification is the process whereby a network element recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of a user. A user may be a person, a process, or a system (e.g., an operations system or another network element) that accesses a network element to perform tasks or process a call. A user identification code is a non-confidential auditable representation of a user. Information used to verify the claimed identity of a user can be based on a password, Personal Identification Number (PIN), smart card, biometrics, token, exchange of keys, etc. Authentication information should be kept confidential.

If users are not properly identified then the network element is potentially vulnerable to access by unauthorized users. Because of the open nature of ONA, ONA greatly increases the potential for unauthorized access. If strong identification and authorization mechanisms are used, then the risk that unauthorized users will gain access to a system is significantly decreased.

Section 3.2.2 describes the threat of impersonating a user in more detail.

The exploitation of the following vulnerabilities, as well as other identification and authentication vulnerabilities, will result in the threat of impersonating a user.

- Weak authentication methods are used;
- The potential exists for users to bypass the authentication mechanism;
- The confidentiality and integrity of stored authentication information is not preserved, and
- Authentication information which is transmitted over the network is not encrypted.

Computer intruders have been known to compromise PSN assets by gaining unauthorized access to network elements. It is possible for a person impersonating an authorized user to cause the full range of threats described in section 3.2. Impacts on the PSN caused by the threat of impersonating a user include the full range of impacts to NS/EP telecommunications described in section 3.3. The severity of the threat of impersonating a user depends on the level of privilege that is granted to the unauthorized user.

4.3 Resource Access Controls

In addition to greatly increasing the number of users who have access to telecommunications systems and facilities, ONA increases the levels of access to telecommunications systems and facilities. If a network element does not provide a level of granularity such that for each user allowed access to a resource it is possible to grant access rights to specific software, processes, databases, information, etc., then users authorized to use a network element may be able to uses resources for which they are not authorized. For example, if proper resource access control is not used then it is possible for a user authorized to use a network element to execute unauthorized commands, access unauthorized information, or access unauthorized network elements.

The exploitation of vulnerabilities associated with resource access control results in the threat of impersonating a user. The severity of the threat of impersonating a user depends on the level of privilege that is granted to the unauthorized user. Strong access control mechanisms must be combined with strong identification and authentication mechanisms to fully protect resources.

4.4 Data Integrity

The opening of the telephone network to vendors and customers of enhanced services involves the broadening of access to stored data/information. For example, information which previously was only accessible by the carrier may be accessible to vendors and customers of enhanced services. If data is not adequately protected, perhaps by use of passwords and partitioning, then the data is vulnerable and the integrity and privacy of the data may be compromised.

4.5 Software Vulnerabilities

Services supported by ONA networks require much more software than the traditional Plain Ordinary Telephone Services [10]. As an increasing number of network services are created and deployed, software will be an even more dominant component of telecommunications networks. ONA not only increases the amount of software used, ONA also greatly increases the number of users who have access to network software. By giving more users access to network software, ONA increases the potential for hostile users.

ONA also increases the number of levels of access to software. Software which previously was only accessible by the carrier may be accessible in varying degrees to vendors and customers of enhanced services. For example, ONA will require that access to existing switch call processing software be provided at an elemental service level [10]. If proper security

mechanisms are not used, the increasing accessibility of network software will provide hackers and saboteurs with the opportunities to impact the PSN. For example, the accessibility of network software may provide hackers and saboteurs with the opportunity to damage routing databases.

As noted in a study by the National Research Council, as more levels of network software are made visible to users for purposes of affording parity of network access, users will learn more about the inner workings of the network software, and those with hostile intent will learn more about how to abuse the network [4].

Vulnerabilities associated with software have an impact on the integrity and privacy of the software. As computer intruders learn more about how the network software is used, it is possible for computer intruders to have an impact on the availability, integrity, and privacy of network functions. Fraud may also result.

4.6 System Integrity

System integrity involves ensuring the integrity of network element systems and providing an acceptable level of service. Exploitation of vulnerabilities associated with system integrity may result in service denial or disruption, or the unauthorized modification of user or network information and network services.

The unbundling of services increases the real-time processing requirements and therefore services provided as a result of ONA requirements will require more real-time processing [10]. The paper "ONA: Demands on Provisioning and Performance" notes that the evolution of the public network to support enhanced services creates the need for planning the growth of real-time switch capacity in concert with the emergence of these new services. If carriers do not adequately plan for increased real-time switch capacity, the PSN is vulnerable to disruption and denial of service problems.

4.7 Fraud

The "Electronic Intrusion Threat to NS/EP Telecommunications" report states that because toll fraud is not seen as being directly related to the performance of Government agencies' ability to perform NS/EP missions, toll fraud is considered a significant problem, but one with undefined NS/EP implications.

The telecommunications networks resulting from ONA requirements are more vulnerable to fraud than networks existing before ONA requirements. If assets (e.g., application system services, network software, and switches) are not adequately protected, then many vulnerabilities exist. Exploitation of these vulnerabilities can result in fraud and financial loss. ONA implementations provide a large number and range of services. It is possible for computer intruders motivated by greed to exploit vulnerabilities in the PSN for financial gain by selling and using services that are not paid for. As a result of ONA, the services available to the general public represent a market in excess of $10B in 1988, growing to $30B in 1995 [10].

As computer intruders learn more about the inner workings of network software, and are able to use more and more services without charge, disruption or denial of service for authorized users, and integrity and privacy problems as well as fraud may result.

4.8 Computer Intruders

Section 3.4.2 described malicious hackers as a source of threat. As a result of their increasing knowledge and sophistication, malicious hackers have the capability to exploit the vulnerabilities associated with the use of ONA. Malicious hackers pose a significant threat to the PSN because of the wide extent of damage they can cause.

4.9 OAM&P

An important ONA consideration is the impact on Operations, Administration, Maintenance and Provisioning (OAM&P) systems and procedures. OAM&P includes functions required to provision, maintain and administer the telecommunications network, including both the local exchange networks and the interconnected networks of end-users and ESPs.

ESPs have requested access to BOC OAM&P functions. While many OAM&P functions are not part of the basic network, many are important to an enhanced service offering. Several of the FCC's ONA Orders have addressed access to Operations Support Systems (OSS) systems (see appendix D.2). An OSS is a system (hardware and software) that performs OAM&P functions in concert with telecommunications personnel.

Information available to the ESP must be comprehensive and identical to information available to the carrier's personnel. ESPs have requested comprehensive real-time control over all facets of services purchased from a carrier. An ESP must be able to use the carrier's network elements while appearing to its own customer as though it owns these network elements. In providing ESP access to OAM&P systems, safeguards must be maintained by the carriers to prevent inadvertent errors, or harm to the network and OAM&P databases by the accessing party [12]. Strong security mechanisms are needed to restrict access to OAM&P systems. Security restrictions for system functions and partitioning of systems and data bases are needed to provide for security and privacy of the network and ESP and end-user information.

An additional security consideration regarding the protection of OAM&P resources is securing the interface between the ESP and the OSS. As long as the carrier's enhanced services operations take the same access to OSS services as the access provided by the carrier to ESPs, the OSS services may be accessed either directly or indirectly. If an ESP is allowed direct access to the same data communications network that the carrier's telecommunications use, then additional potential vulnerabilities exist. Security concerns include securing access to the data communications network and the associated attached systems.

Implementation of new network functionalities will impact OAM&P systems and processes in a number of ways. The most evident is the aggregate impact on capacity, due to the increasing number of users and items to process through the system. As a result the threat of denial of service exists. Less evident is the impact on OAM&P systems and processes due to the increasing scope and complexity of requests. Billing of end-user services to ESPs, bulk resale, agency agreements, automated ordering by the ESP and the unbundling and repackaging of new and existing technologies and services are opportunities for improved end-user telecommunications value through "customization" of services [13].

4.10 Connectivity

PSN security depends largely on individual service providers. By connecting to a network owned by another carrier, vulnerabilities may be introduced. Weakness in one carrier's networks will insert vulnerabilities into another carrier's networks if the networks are interconnected. Section 4.16 describes vulnerabilities associated with ESPs connecting to the PSN.

4.11 Unbundling

Further unbundling remains a long-term objective of ONA. The FCC's Phase I Order required unbundling "to the extent technologically feasible"[25, para. 216]. The IILC was directed, in the BOC ONA Order, to address the potential technical and operational problems posed by more extensive unbundling of the network [22, pages 41-43]. The BOC ONA Amendment Order required each carrier to amend its plan to describe any change to its plans for developing and implementing new technologies such as SS7, ISDN, and IN technologies, including a description of (1) how it will unbundle the services provided through the use of such technologies and generally how those services will fit into the ONA framework; (2) ONA services that these technologies could support; and (3) its plans for offering such services [24]. With further unbundling of the network, many security concerns will arise.

IILC Issue 026 is titled Long Term Unbundling and Network Evolution. "This issue addresses the FCC directive to examine, through the IILC, the technical, operational and administrative issues associated with further unbundling and modular architecture. Since the February IILC meeting the task group has finalized and validated the identified physical points of interconnection, has developed a matrix of logical interconnection options, and is currently seeking validation of these logical interpretations"[28] This issue considered Issue 022 unbundling criteria, has resulted in several Unbundling Forums, and has been a topic of discussion since 1991. It is important that security concerns be taken into account for planning further unbundling of the network.

4.12 Distributed Intelligence

In the past, intelligence, such as features and call processing software, was located primarily at local central office switches. Today, new enhanced services being considered are likely to need network capabilities that are not necessarily located at local central office switches. The trend is evolving to provide additional intelligence in the Customer Premises Equipment (CPE) and various Network Elements [10] [20]. As Intelligent Network concepts are merged into networks based on ONA requirements, the number of services requiring distributed intelligence will increase.

The distribution of intelligence will require more resources to maintain functions. Services requiring distributed intelligence are likely to introduce vulnerabilities.

4.13 Intelligent Networks

The paper "Access Controls for Open Architecture in Intelligent Networks" [16] provides the following description of Intelligent Networks (IN).

> An Intelligent Network (IN) is a switched network whose service control is removed from the individual switches and whose service definition can be programmable. It aims at rapid and economical service provisioning and facilitates customer control of network services.

IN comes from the industry and ONA comes from the regulators. For the most part, IN and ONA have been investigated separately [16].

The opening of Intelligent Networks introduces significant security and integrity problems [16]. The report "The Impact of Intelligent Networks (IN) on NS/EP Telecommunications" presents an assessment of vulnerabilities and interoperability issues associated with IN technology [14]. The software-dependency of the Intelligent Network and the openness of its architecture brings expanded security concerns to the Government and Industry [14].

The IN concept allows ESPs to program their own enhanced services and IN will provide customized software-controlled network services that can be flexibly, rapidly, and cost effectively configured by the customer in response to unique requirements independent of service provider activities [14]. As Intelligent Network concepts are merged into networks based on ONA requirements, many vulnerabilities will result.

4.14 ONA Services

In addition to the more than 180 ONA services [9], ESPs continue to articulate their needs for new or expanded services to the carriers in various ONA forums.

As the result of ONA requirements, a wide range of services, including basic voice service, data services, and enhanced voice storage and retrieval services are available today. The current telecommunications environment has been characterized as one with: a large number of features; multi-media, multi-party services; partial knowledge of the feature set by service designers; lower skill and knowledge levels of some service creators; multiple execution environments from different vendors; and distributed intelligence [15]. As the number of ONA services increases along with the complexity of these services, the potential for vulnerabilities associated with ONA services also increases.

Section C provides a general description of ONA services. Section E describes specific ONA services that have a more direct impact on NS/EP.

4.15 Feature Interaction

Initial standardization efforts involved in the provision of the ONA plans by the carriers related primarily to the nature of the services offered, and not to the interactions between the different services or the nature of such interactions. This is because, in the large majority of cases, the services that were to become the Basic Service Elements were already in existence prior to the ONA mandate, and as such so were the communications protocols used between the service elements. The ONA mandate does not address how Basic Service Elements should interact, merely that they should be available on an individual basis to the ESPs and be nondiscriminatory.

Greater network access is changing the telecommunications industry to one where many third party service providers are building products that must work with products from other

companies [11], [12], [10]. ONA increases the potential for vulnerabilities associated with feature interaction problems. As more services are added to the network, the potential for undesirable feature interactions will increase. Feature interaction could disrupt a needed service or be targeted for intentional abuse by computer intruders.

4.16 Enhanced Service Providers

As each ESP connects to the PSN, weakness associated with the ESP's telecommunications networks and services will insert vulnerabilities into the PSN. Delimitation of the scope of access to the PSN is necessary to prevent ESP employees from gaining unauthorized access to PSN services.

Each carrier must provide a method for ESPs to access telecommunications systems and facilities. It is a concern to what degree a carrier will investigate the credentials of an ESP, as well as the degree of security provided by the ESP, before allowing the ESP access to the PSN. It is possible for malicious hackers to take on the appearance of an ESP to obtain access to the PSN.

5 Conclusions

The goal of the FCC's ONA is to create free market conditions within the telecommunications industry. ONA requires carriers to provide competing ESPs with access to basic communications services on an equal cost basis and in a nondiscriminatory manner. Telecommunications services are unbundled into services that are tariffed and may be purchased individually by enhanced service providers. The essense of the ONA plan created by each carrier is to describe which Basic Service Elements are Offered.[3]

In the Computer III Decision, the FCC noted that ONA was a long-term evolving process. The FCC was primarily concerned with providing unbundled services on an equal access basis and left the implementation details fundamental to providing those services up to the independent carriers. Security was not a driver for ONA and for the most part, the FCC has relied on the carriers to ensure that the services provided are secure. The FCC's requirements for security capabilities have resulted primarily from the requirement that ONA services be provided in a nondiscriminatory manner. For example, the FCC's requirement for the protection of Customer Proprietary Network Information was made to prevent the carriers, who had access to customer proprietary network information for subscribers of the carriers' basic network services, from having an unfair marketing advantage for enhanced services.

The exploitation of vulnerabilities introduced by the FCC's ONA can impact the availability of PSN resources and services, the integrity of data/information, the disclosure of data/information and the fraudulent use of services.

ONA creates network vulnerabilities because it greatly increases the number of users (some of whom will be hostile) who have awareness of the network architecture. In addition to broadening access to telecommunications systems and facilities, ONA increases the levels of access to telecommunications systems and facilities. As users learn more about the operation of network software, those with hostile intent will acquire knowledge that could assist them in abusing resources.

The following list summarizes the most significant vulnerabilities that ONA introduces into the PSN. Note that many of the vulnerabilities listed below existed prior to the FCC's ONA requirements. However, because of the open nature of ONA, these vulnerabilities are significantly increased.

- By giving more users access to the network, ONA increases the potential for unauthorized access of network elements if strong access mechanisms aren't used.
- If strong resource access control mechanisms aren't used, by increasing the level of access to network resources, ONA increases the potential for users authorized to use a network element to obtain access to resources other than those that are needed to perform the job function
- The opening of the network results in the broadening of access to stored data/information. If data is not adequately protected, then the data is vulnerable and the integrity and

[3]Note that each ONA plan actually describes a set of Basic Service Elements (BSEs), Basic Serving Arrangements (BSAs), and Complementary Network Services (CNSs). These services are described in more detail in Appendix C

privacy of the data may be compromised.

- Services supported by ONA networks will require more software than the traditional Plain Ordinary Telephone Services. New software may contain bugs. ONA not only increases the amount of software used, ONA also greatly increases the number of users who have access to network software, and the number of levels of access to the software. By giving more users access to network software, ONA increases the potential for hostile users.

- ONA increases vulnerabilities associated with system integrity. For example, if carriers do not adequately plan for the increased real-time switch capacity associated with the unbundling of services, the integrity of network element systems will be affected.

- ONA involves the provisioning of billable services, and thus ONA increases the potential for fraud and/or financial loss.

- Malicious hackers have the capability to exploit the vulnerabilities associated with ONA.

- Services requiring distributed intelligence are likely to introduce vulnerabilities.

- As Intelligent Network concepts are merged into networks based on ONA requirements, many vulnerabilities will result.

- As the number of new services increases and the complexity of new services increases, the potential for vulnerabilities associated with new services increases.

- ONA increases the potential for vulnerabilities associated with feature interaction problems.

- Weakness in one carrier's networks will potentially insert vulnerabilities into another carrier's networks if the networks are interconnected.

- As an ESP connects to the PSN, weakness associated with the ESP's telecommunications networks and services will insert vulnerabilities into the PSN.

- Depending on the degree that a carrier investigates the credentials of an ESP, as well as the degree of security provided by the ESP, before allowing the ESP access to the PSN, ONA increases the potential for unauthorized access.

- Each ONA implementation may have its own vulnerabilities.

- OAM&P systems and services may introduce new vulnerabilities.

- The implementation of new technologies and further unbundling will result in new NS/EP telecommunications security concerns.

Acronyms

ATIS	Alliance for Telecommunications Industry Solutions
BOC	Bell Operating Company
BSA	Basic Serving Arrangement
BSE	Basic Service Element
CEI	Comparatively Efficient Interconnection
CLC	Carrier Liaison Committee
CNS	Complementary Network Services
CPNI	Customer Proprietary Network Information
ECSA	Exchange Carriers Standards Association
ESP	Enhanced Service Providers
FCC	Federal Communications Commission
IILC	Information Industry Liaison Committee
IN	Intelligent Network
ISDN	Integrated Services Digital Network
NCS	National Communications System
NOF	Network Operations Forum
NRC	National Research Council
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NSTF	Network Security Task Force
OAM&P	Operations, Administration, Maintenance and Provisioning
OMNCS	Office of the Manager, National Communications System
ONA	Open Network Architecture
OSS	Operations Support Systems
PSN	Public Switched Network
RBOC	Regional Bell Operating Company
SS7	Signaling System 7

References

[1] Federal Communications Commission. *Third Computer Inquiry.* FCC, June 16, 1986.

[2] A.M. Rutkowski. "Open Network Architectures: An Introduction," *Telecommunications*, January 1987, pp30-40.

[3] NCS Manual 3-1-1. "Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness (NSEP) Service User Manual," July 9, 1990.

[4] National Research Council. *Growing Vulnerability of the Public Switched Networks.* National Academy Press, 1989.

[5] National Security Telecommunications Advisory Council. "Report of the Network Security Task Force," 1990.

[6] National Security Telecommunications Advisory Council. "Final Report of the Network Security Task Force," August 17, 1992.

[7] "Installation and Maintenance Responsibilities - SS7 Link and Trunk Installation and Maintenance Access Services; Network Operations Forum Reference Document," Issue 3, January 1993.

[8] B. Bagwill, et al. "Security in Open Systems," National Institute of Standards and Technology Special Publication 800-7.

[9] Bell Operating Companies. *ONA Services User Guide: Services Descriptions*, July 31, 1993.

[10] S. Homayoon, G. Giridharagopal. "ONA: Demands on Provisioning and Performance," *IEEE Globecom*, IEEE, 1988.

[11] S.E. Dolan. "Open Network Architecture from an Operational Perspective," *IEEE Globecom*, IEEE, 1988.

[12] L. Simpson. "Open Network Architecture: OAM Perspective, an RBOC's View," *IEEE Globecom* , IEEE, 1988.

[13] Benjamin Lisowski. "ESP Requirements for BOC Network Operations and Management Systems," *IEEE Globecom*, IEEE, 1988.

[14] Intelligent Networks Task Force. "The Impact of Intelligent Networks (IN) on NS/EP Telecommunications," November 7, 1990.

[15] F.S. Dworak. "Approaches to Detecting and Resolving Feature Interactions," *IEEE Globecom*, 1991.

[16] Che-Fn Yu. "Access Controls for Open Architecture in Intelligent Networks," *IEEE Globecom*, 1991.

[17] Office of the Manager National Communications System (OMNCS). "Natural and Technological Disaster Threats to NS/EP Telecommunications," November 1992.

[18] Office of the Manager National Communications System (OMNCS). "Summary of the Threat to National Security and Emergency Preparedness Telecommunications," June 1993.

[19] Office of the Manager National Communications System (OMNCS). "The The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications: An Awareness Document," September 30, 1993.

[20] Bell Communications Research. "Plan for the Second Generation of the Intelligent Network," Special Report, SR-NPL-000444, Issue 1, July 1986.

[21] *Final Decision*, 77 FCC 2d at 420. para 93.

[22] *Filing and Review of Open Network Architecture Plans*, 4 FCC Rcd 1 (1988) (BOC ONA Order).

[23] *Memorandum Opinion and Order on Reconsideration, Filing and Review of Open Network Architecture Plans*, CC Docket No. 88-2, Phase I FCC No. 90-134 (released May 8, 1990).

[24] *Memorandum Opinion and Order, Filing and Review of Open Network Architecture Plans*, CC Docket No. 88-2, Phase I FCC No. 90-135 (released May 8, 1990) (BOC ONA Amendment Order).

[25] *Phase I Order*, 104 FCC 2d.

[26] *Memorandum Opinion and Order, Filing and Review of Open Network Architecture Plans*, CC Docket No. 88-2, Phase I FCC No. 90-382 (released December 19, 1991).

[27] *Alliance for Telecommunications Industry Solutions* Annual Report 1993.

[28] "Information Industry Liaison Committee ONA News," May 1993, Vol. 3, No. 2.

A FCC ONA Orders

The FCC declined to provide a specific standard for ONA [1, page 1067]. Rather, it placed the burden for the development of Open Network Architectures on the carriers. In the event the standardization process for ONA became a process in which each of the carriers would submit an ONA plan, the FCC would rule on which aspects of the plan were acceptable and which were not, and return the plan to the carrier for revision. Several iterations of this process eventually produced a satisfactory initial plan for each carrier. In addition to FCC review, the ONA plans are subject to public comment. The FCC has taken into account numerous comments and petitions filed by parties of interest for reconsideration and/or clarification of ONA plans.

The FCC's Third Computer Inquiry directed the carriers to file initial ONA plans with the FCC by February 1, 1988. On November 17, 1988, the FCC adopted the BOC ONA Order [22]. Among other things, this order approved in part the ONA plans for each of the carriers, directed each carrier to file an amended ONA plan by May 19, 1989, and established procedures for oversight of the ongoing ONA process. On May 8, 1990, the FCC released the BOC ONA Amendment Order [24] which concluded that all the amended plans complied with the requirements of the BOC ONA Order. ONA plans for each carrier are continually being amended to reflect changes in services offered and to comply with additional requirements of the FCC.

B Committees of Interest to ONA

The work of standardization with regard to the physical implementation of the services described in the ONA plans is very much a current issue, with work being carried out in various committees of the Exchange Carriers Standards Association (ECSA). ECSA was created in 1983 with the mission to "promote the timely resolution of national and international issues involving telecommunications standards and the development of operation guidelines" [27]. In October 1993 ECSA was renamed the Alliance for Telecommunications Industry Solutions (ATIS) and its membership was expanded to include all domestic providers of telecommunications services with a plant investment in transport and/or switching equipment. ATIS currently oversees eight committees including those described below.

In the Third Computer Inquiry, the FCC stated that private standards organizations, such as the T1 Committee, should play a major role in resolving issues of interest to carriers and enhanced service providers [1, page 1067]. Committee T1 was established in 1983 and is accredited by the American National Standards Institute. This committee "provides a proactive role in establishing consistent telecommunications standards worldwide to facilitate the deployment of interoperable telecommunications systems and services" [27]. Current areas of technical focus include Signaling System 7 (SS7) Interconnection, Integrated Services Digital Network (ISDN), Intelligent Network (IN), and Switch Survivability. Two committees that have addressed ONA issues are the T1M1 and T1E1 Committees.

The T1M1.5 Committee, whose focus is on access in a network-network interconnection context, has been working on security requirements for interconnected Telecommunications Management Networks (TMNs). T1M1.5 work is relevant to ONA because work on securing operations environments is needed to support ONA.

The Information Industry Liaison Committee (IILC) was established in 1987 as a forum to exchange information on ONA. Participation in the IILC is open to all parties interested in ONA. The mission of the IILC is to obtain industry consensus on technical, operational, and administrative issues related to ONA. Requests for ONA services are accepted as *Issues*. Issues remain active until consensus is reached or a lack of overall interest in the issue is demonstrated. Resolved issues become voluntary recommendations that IILC participants generally adhere to. It is possible for each carrier to tailor an IILC recommendation.

In specific cases, for example the Operations Support Systems (OSS) capabilities issue (see section D), the FCC has directed the carriers to work through the IILC. In the BOC ONA Order, the FCC directed the carriers to amend their ONA plans to reflect progress in the IILC. The IILC is the primary forum used to resolve ONA issues.

The IILC has touched upon a few security related ONA issues. Any member of the IILC is allowed to propose new issues for requested services. Therefore, the framework is in place for additional services to be incorporated into ONA, including services that support NS/EP. Specific requests for enhanced services are evaluated based on expected market demand, their utility as perceived by ESPs, and the technical and cost feasibility of unbundling and providing those services.

Members of the IILC have worked together to resolve many ONA issues. Implementation of services based on IILC recommendations can be complicated. Many services are not offered due to lack of customer demand, cost or operational difficulty. For example, Issue 012 (Ability to Detect Breaks in Telco Lines Within 60 Seconds) was adopted on March 22,

1989 however today only four carriers offer this service. Issue 003 (ESP/Customer Access to BOC Network Management Systems (OSS)) was adopted March 15, 1988 however only one carrier currently offers this service.

Forums under the Carrier Liaison Committee (CLC) may address areas of interest to ONA. Forums that may cover areas related to ONA include the Ordering and Billing Forum and the Network Operations Forum. The Network Operations Forum (NOF) covers Toll Fraud Prevention and SS7 Network Testing. The NOF has done security work relevant to ONA in the following areas:

1. Security baseline for interconnected SS7 networks.

2. Security information sharing among carriers and vendors supplying equipment to the carriers for use in SS7 networks. The sharing is focused on holes found in vendor products.

C ONA Services

Carriers are required to satisfy all ESP requests for services that meet the FCC's criteria of demand, utility, technical feasibility, and costing feasibility. Each ONA plan describes a set of *Basic Service Elements (BSEs)*, *Basic Serving Arrangements (BSAs)* and *Complementary Network Services (CNSs)* supplied by the service provider and based on a set of requests for services placed by the ESPs. Basic Service Elements are optional unbundled features, such as calling number identification, that ESPs may require in providing an enhanced service. Basic Serving Arrangements are fundamental switching and transport services. ESPs obtain access to various Basic Service Elements through Basic Serving Arrangements. An example of a Basic Serving Arrangements is the physical connection to the telephone network. Complementary Network Services are optional unbundled basic service features that an end user may obtain from a carrier in order to use an enhanced service. Call forwarding is an example of a Complementary Network Service. Basic Serving Arrangements, Basic Service Elements, and Complementary Network Services cannot be ordered until appropriate tariffs are effective. The carriers are required to satisfy all ESP requests that meet the FCC's criteria of demand, utility, technical feasibility and costing feasibility.

BOC ONA Special Report Number 1, Issue 2 (October 1987) listed 118 ONA services requested by ESPs prior to the filing of initial ONA plans. A few ONA services are no longer offered and many new services have been added. Currently, there are over 150 services. Amendments to an ONA plan must be filed before a carrier is allowed to offer a new service. An example of a representative set of services can be found in "ONA Services: Names, Descriptions, Cross References" [9]. This document is also known as the "ONA Services User Guide."

It should be noted that the initial standardization efforts involved in the provision of the ONA plans by the carriers related primarily to the nature of the services offered, and not to the interactions between the different services or the nature of such interactions. This is because, in the large majority of cases, the services that were to become the Basic Service Elements and Basic Serving Arrangements were already in existence prior to the ONA mandate, and as such so were the communications protocols used between the the service elements. The ONA mandate does not address how Basic Service Elements/Basic Serving Arrangements should interact, merely that they should be available on an individual basis to the ESPs and be nondiscriminatory.

In various orders, the FCC addressed two types of uniformity: availability of services and technical uniformity. After reviewing initial ONA plans, the FCC noted significant differences in ONA services offered by the carriers. Of the 118 services requested by ESPs, in the original ONA plans, the carriers offered 29 common services with an average of 54 services offered by each carrier. In an attempt to increase the uniformity of services offered among the carriers, the FCC required each carrier to review other carriers' plans and to try to increase the number of ONA services offered by each carrier's ONA plan [22]. The amended plans indicated that 37 services were offered on a nationwide basis and that each carrier proposed to offer an average of 70 services [24].

Today, the number of services offered by the carriers has increased, but there is still considerable difference in the number of services offered by the individual carriers. The Services Descriptions section of "The ONA Services User Guide" [9] represents an agreement on the

part of the carriers for uniform names and technical descriptions of the Basic Serving Arrangements, Basic Service Elements, and Complementary Network Services. For each ONA service, a table is provided that lists the generic name of the ONA service or Basic Serving Arrangements, which carrier plans to offer the service, the individual carrier's product name, and whether the carrier classifies the service as Basic Serving Arrangements, Basic Service Elements, or Complementary Network Service. The "ONA Services User Guide" directs the reader to refer to the individual BOC ONA plans and amendments for information on BOC availability and deployment plans for ONA services.

Although the FCC noted that technical uniformity in the initial offerings would be difficult to achieve because of the differences in embedded technology and uncertainties in market demand, the FCC directed the carriers to continue working through the IILC to develop procedures for achieving uniformity in key services areas. In the BOC ONA Amendment Order, AT&T expressed concern about the carriers' use of different technical means of providing similar ONA services.

D ONA Security Capabilities

The FCC has relied on the carriers to develop their own open network architectures and the FCC relies on the carriers to ensure that the services provided are secure. A review of the implementation of each ONA plan is needed to determine the level of security provided by each ONA implementation. The FCC's requirements for security capabilities have resulted primarily from the requirement that ONA services be provided in a nondiscriminatory manner. The primary purpose of ONA security capabilities required by the FCC was not to provide security in the traditional sense, but to prevent a marketing advantage.

Current ONA security related capabilities which provide some degree of confidentiality and integrity of information fall into two areas: protection of Customer Proprietary Network Information and provision of Operations Support Systems services.

D.1 Customer Proprietary Network Information

In the Third Computer Inquiry, many commenters argued that the BOCs had an unfair marketing advantage for enhanced services because the BOCs had access to the customer proprietary network information (CPNI) for subscribers of the carrier's basic network services. Other parties argued that the BOCs could use their databases to generate aggregate information on usage levels and traffic patterns for network services and that this information would be of substantial value in the technical and economic design of enhanced services.

The BOC ONA Amendment Order required that a password/ID system be used to restrict CPNI access for certain databases routinely accessed by enhanced services marketing personnel. This order did not require that the BOCs implement password/ID systems for auxiliary databases that contained fragmented CPNI or are not routinely accessed by enhanced services marketing personnel[24, pages 58, 63].

Although the password/ID systems provide a certain degree of confidentiality, the initial purpose of the password/ID systems was not to provide security in the traditional sense, but to prevent a marketing advantage.

D.2 Operations Support Systems

Operations Support Systems (OSS) include diagnostic, maintenance, and network management capabilities that are of use to ESPs in controlling their telecommunications services efficiently. Computer Inquiry III did not require the BOCs to offer OSS services, however, the BOC ONA Order directed the BOCs to amend their plans to specify OSS services that could be offered to ESPs in the near term [22, para. 110]. Recognizing that a number of issues associated with OSS services might need to be resolved before customers can access the BOCs internal systems, the FCC directed the BOCs to examine, through the IILC, the most feasible means of providing OSS access for ESPs [22, para. 110].

For the most part, access to and control of OAM&P functions support the network. However, these functionalities are not an essential part of the network required to convey customer information from point to point, and are therefore beyond the requirements of ONA [12]. The BOC ONA Order defined ancillary services to be unregulated, competitive services useful to ESPs. Depending on the criteria, OSS services may be offered either as

ONA services or as tariffed services not subject to ONA requirements. The following list groups OSS services into four categories:

1. Service Order Entry and Status

   Services requested by ESPs include a service to speed up and automate the service order process by placing service orders electronically and a service to determine the status of service orders electronically.

2. Trouble Reporting and Status

   Services requested by ESPs include a service to enter a trouble report into a carrier database and subsequently check its status.

3. Traffic Data Collection

   This capability refers to information ESPs need to analyze traffic volume and congestion on their lines.

4. Diagnostics, Monitoring, Testing, and Network Reconfiguration

   Services requested by ESPs include services for testing and reconfiguration abilities.

The carriers proposed providing indirect access to OSS services for ESPs, yet direct access for themselves. Keeping comparably efficient access in mind, in the BOC Amendment Order, the FCC required that the carrier's enhanced services operations take the same access to OSS services as the access provided by the carrier to ESPs. This issue is commonly known as the *OSS same access* issue.

ONA plans revolve around Basic Service Elements (BSEs), Basic Serving Arrangements (BSAs), and Complementary Network Services (CNSs). The BOC ONA Amendment Order requirement for OSS same access only applies to Basic Service Elements and Basic Serving Arrangements. There is a requirement for OSS access for Complementary Network Services, however the carrier's enhanced services operations are not required to take the same access to OSS services as the access provided to the ESPs. OSS access for Complementary Network Services will require stricter security than OSS access for Basic Service Elements and Basic Serving Arrangements because Complementary Network Services include access to customer lines.

On February 22, 1990, the IILC reached consensus on Issue #003 - ESP Customer Access to BOC Network Management System. "The resolution identifies OSS capabilities useful to ESPs, and establishes a commitment to develop a generic software gateway interface"[26]. As directed by the FCC in the BOC ONA Order, at its April 1993 meeting, the IILC accepted Issue #039 - ESP Needs for OSS Capabilities Associated with End-User Complementary Network Services. "The purpose of this issue is to determine ESP needs for OSS capabilities for Complementary Network Services associated with end-user lines, and to develop methods as to how those needs could be met through some kind of indirect OSS access"[28].

A gateway approach was considered by the carriers and the IILC to allow access to OSS services but consensus has not been reached on this issue. Depending on the configuration, a gateway could either be used to deter or assist unauthorized ESPs and end-users in accessing OSS services.

Several articles (e.g. [11], [12], [13]) have addressed OAM&P aspects of ONA. Many of these aspects can be categorized by the four areas of OSS services defined by the FCC. Appendix E describes several OSS ONA products that are listed in the "Ona Services User Guide". Note that additional OSS services may be offered to ESPs as tariffed services not subject to ONA requirements.

E ONA Services of Interest to NS/EP

As the number of ONA services increases along with the complexity of these services, the potential for vulnerabilities associated with ONA services also increases. Although there are over 100 ONA services, all of which have the potential to impact NS/EP in some form (e.g., if an ONA service contains vulnerabilities, exploitation of the vulnerabilities may affect the availability and reliability of the PSN), this section will describe a few ONA services of particular concern to NS/EP. The following list describes OSS ONA services as they are described in the July 1994 "ONA Services User Guide." The services are grouped according to the four categories considered by the FCC to be basic OSS services. Services are listed according to their generic ONA service name. As noted in section 4.9, in providing ESP access to OAM&P systems, safeguards must be maintained by the carriers to prevent inadvertent errors, or harm to the network and OAM&P databases by the accessing party. Vulnerabilities associated with ONA services that support OAM&P functions have the potential to affect the availability and reliability of the PSN. Some of the services listed below support NS/EP by providing a way to monitor and respond to problems in the PSN.

1. Service Order Entry and Status

   - Access To Operations Support Systems Information

     This service will offer the ESPs a common, mechanized presentation system for access to Network Management products, such as network reconfiguration, while also providing ESP customer access to internal operations support systems for additional information and control of their network.

     This service will provide a secure and user friendly interface to ESP customers in providing capabilities and support in some or all of the following areas of service management: (1) Administration, (2) Security, (3) Performance, (4) Fault Management, (5) Reconfiguration, and (6) Accounting.

   - Access to Order Entry System

     This capability will allow ESPs to provide basic ordering information to the business office through a mechanized interface.

2. Trouble Reporting and Status

   - User Initiated Diagnostics

     This capability will allow ESPs to electronically report and check the status of local and access, circuit line troubles into support systems.

3. Traffic Data Collection

   - Traffic Data Reports

     This capability provides ESPs with periodic printed summaries of traffic data on their network facilities that are associated with central office switches. Traffic data reports include traffic information such as number of call attempts, number of blocked calls, and usage by ESP trunk group.

4. Diagnostics, Monitoring, Testing, and Network Reconfiguration

   - Dedicated Alert Transport Basic Serving Arrangement

     The dedicated alert transport Basic Serving Arrangement using derived local channel technology would offer ESPs a 24 hour supervised monitoring capability using existing local loop access lines.

   - Verify Integrity of Subscriber Lines

     This capability allows an ESP to be signaled by central office equipment every 60 seconds or less to report on the integrity of the ESP's client's lines that are being monitored for breaks.

   - Network Reconfiguration

     This feature provides ESPs flexibility in managing and reconfiguring their dedicated facilities.

   - Access To Operations Support Systems Information

     The product currently available for this ONA Service supports network reconfiguration.

The following is a list of a few ONA services that are not OSS services, but are of interest to NS/EP. The following list describes ONA services as they are described in the July 1993 "ONA Services User Guide." These services are categorized by their generic ONA service name. While vulnerabilities associated with the services listed below have the capability to negatively impact NS/EP, these services can support the availability of the PSN.

- Alternate Routing

  When all the circuits in an ESP's circuit switched trunk serving arrangement with alternate route capability are busy due to traffic volume the network will attempt to complete subsequent calls to an alternate route served by that switch as previously specified by the ESP.

- Automatic Protection Switching

  Automatic Protection Switching provides the ability to monitor a non-switched facility between the ESP premises and the wire center serving the premises and to automatically switch to a spare facility if the performance of the original facility degrades or fails.

- Route Diversity

  Route Diversity provides an increased safety factor for ESP facilities that could be subject to disruption from cable cuts and other unavoidable catastrophes. It provides for diverse routing when necessary in order to comply with special ESP requirements.

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SECURITY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 800-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899–0001