THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NETWORK GROUP
Internet Report
An Examination of the NS/EP Implications of Internet Technologies

JUNE 1999

INTERNET REPORT
TABLE OF CONTENTS

CONTINUED

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Much like the private sector, the Government is using the Internet more extensively for day-to-day functions such as e-mail, procurement, outreach and information sharing. However, as the Government also expands its Internet use to more critical applications, such as supporting national security and emergency preparedness (NS/EP) functions, concerns arise about how a severe disruption of Internet service might affect NS/EP operations. This issue arose during discussion at the National Security Telecommunications Advisory Committee (NSTAC) XX meeting in December 1997, and the Industry Executive Subgroup (IES) subsequently tasked the Network Group (NG) to examine this issue further.

Purpose and Approach

The purpose of this report is to examine how a severe disruption of the Internet could affect NS/EP operations over the next 3 years. The report focuses on the current Internet infrastructure and anticipated near-term enhancements, and recognizes traditional threats and vulnerabilities, such as equipment malfunctions, natural hazards, sabotage, and physical design. It addresses potential concerns as new technologies and regulatory mandates affect the evolution of the Internet. Additionally, the growing threat from malicious intruders is considered.

The approach to this study involves these tasks:

- Examine the extent to which NS/EP operations will depend on the Internet over the next 3 years
- Identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the Public Switched Network (PSN)
- Examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

Conclusions

The NG reached the following conclusions:

- Agencies with NS/EP responsibilities are using the public Internet mostly for outreach, information sharing, and electronic mail (e-mail).

- The NS/EP community's direct dependence on the public Internet for mission-critical operations is currently modest.

- NS/EP dependence on the Internet is likely to grow over the next several years because the public Internet offers a cost-effective, efficient means of communications, the Government is rapidly adopting electronic commerce, and federal policies promote use of the Internet.

- The NS/EP community is more likely to depend on dedicated Transmission Control Protocol/Internet Protocol (TCP/IP) networks (also called intranets) for mission-critical NS/EP operations at present.

- Because of the interconnected nature of the public Internet, a disruption or degradation of Internet operations could also affect the operations of dedicated TCP/IP networks/intranets.

- Critical infrastructures, such as medical services, banking and finance, gas and electric industries and telecommunications, are increasingly using the public Internet for various processes, including exchange of business, administrative and research information.

- The Internet is a conglomeration of interexchange points (IXP) and national, regional, and local Internet Service Providers (ISP) serving end users and organizations. With the Internet's highly diverse architecture and complex interconnection arrangements, consisting of thousands of ISPs, it is *unlikely* that the failure of any single node or transmission facility would cause a major Internet service disruption.

- The informal and distributed management of Internet functions, the Domain Name System (DNS), Internet software including Berkeley Internet Name Domain (BIND), and procedural errors and unintentional actions invite potential vulnerabilities that could contribute to a disruption of Internet service.

- At present, the reliability and security of the public Internet is generally considered inadequate for NS/EP mission-critical functions.

- Today, there are no Internet technologies or applications that facilitate the same type of end-to-end NS/EP-related services available in the PSN (i.e., priority access, routing, and transport).

- Although certain ISPs currently offer in-network quality of service (QoS) standards, there are no end-to-end QoS offerings available via the public Internet (e.g., level of availability and performance).

- There are currently no economic incentives for ISPs to develop and offer NS/EP service enhancements over their networks.

- A number of factors (e.g., lack of NS/EP demand, market factors, and lack of regulatory mandates) preclude the availability of NS/EP services over the Internet for the foreseeable future.

NSTAC Recommendations to the President

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:

  - Work with the NS/EP community to increase understanding of evolving Internet dependencies by:

    a. Evaluating the extent of their current and future direct and indirect dependence on the public Internet for NS/EP mission-critical operations.

    b. Developing a thorough understanding of their physical intranet architectures and connections to the public Internet to identify and protect against potential vulnerabilities.

    c. Developing plans and programs to implement long-term goals related to NS/EP dependence on the public Internet.

    d. Defining Internet security and reliability requirements needed to support NS/EP operations.

  - Work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements.

  - Interact with the appropriate Internet organizations and initiatives to investigate, develop, and employ NS/EP-specific Internet priority services, such as priority access, end-to-end routing, and transport.

  - Examine the potential impact of IP network-PSN Convergence on PSN-specific NS/EP priority services (e.g., Government Emergency

Telecommunications Service and Telecommunications Service Priority).

- Recommend that the President direct the appropriate Government departments and agencies to make use of existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

NSTAC Direction to the IES

The NSTAC directs the Industry Executive Subcommittee (IES) to examine the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services (e.g., Government Emergency Telecommunications Service and Telecommunications Service Priority).

1.0 INTRODUCTION

1.1 Background

Much like the private sector, the Government is using the Internet more extensively for day-to-day functions such as electronic mail (e-mail), procurement, outreach, and information sharing. However, as the Government also extends its Internet use to more critical applications, such as supporting national security and emergency preparedness (NS/EP) functions, concerns arise about how a severe disruption of Internet service might affect NS/EP operations. This issue arose during discussion at the President's National Security Telecommunications Advisory Committee (NSTAC) XX meeting in December 1997, and the Industry Executive Subcommittee (IES) subsequently tasked the Network Group (NG) to examine this issue further.

The NSTAC was established in September 1982 to provide advice and expertise to the President and the Executive Agent, National Communications System (NCS), on issues and problems related to implementing NS/EP telecommunications policy. Because the NCS serves as the focal point for joint industry/Government planning, the NSTAC and NCS have developed a close partnership. The NCS, under Executive Order 12472—*Assignment of National Security and Emergency Preparedness Telecommunications Functions*, is required to ensure that a national telecommunications infrastructure is developed that is responsive to the NS/EP needs of the President, Federal departments, agencies, and other entities[1] and which is capable of satisfying priority telecommunications requirements under all circumstances.[2] Additionally, the NCS is required to develop and test programs and procedures for the Nation's telecommunications resources, including federally and privately owned facilities, to meet NS/EP telecommunications requirements.[3]

1.2 Purpose

The purpose of this report is to examine how a severe disruption of the Internet could affect NS/EP operations over the next 3 years. The report focuses on the current Internet infrastructure and anticipated near-term enhancements, and recognizes traditional threats and vulnerabilities, such as equipment malfunctions, natural hazards, sabotage, and physical design.[4] It addresses potential concerns as new technologies and regulatory mandates affect the evolution of the Internet. Additionally, the growing threat to the Internet from malicious intruders is considered. Although this report is primarily focused on the Internet within the United States, the

[1] Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, Section 1(c)(1).
[2] *Ibid.*, Section 1(c)(2).
[3] *Ibid.*, Section 1(g)(1).
[4] Although this report acknowledges the Year 2000 (Y2K) computer problem, it was not addressed in detail because other groups and organizations, such as NSTAC, the Internet Engineering Task Force, and the Network Reliability and Interoperability Council are analyzing the Y2K issue as related to public networks.

management technologies, architecture, and vulnerabilities described in this report apply to the entire global Internet. It is recognized that international emergencies could affect the global information infrastructure (including the Internet) that could in turn affect U.S. NS/EP telecommunications capabilities.

1.3 Definitions

1.3.1 National Security and Emergency Preparedness Services

NS/EP services are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, and international), which causes or could cause harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States.[5]

1.3.2 Severe Disruption

For this report, a severe disruption is described as a sustained interruption or severe degradation of Internet service that could have potential strategic and/or service integrity significance to Government, industry, and the public. Such an event would likely affect Internet service in at least one region of the country, including at least one major metropolitan area. It would not only involve multiple Internet Service Providers (ISP) and significantly degrade the functionality of at least one critical infrastructure in the affected area, but also have an impact on the availability and integrity of Internet service for at least a significant portion of a business day.

1.3.3 Reliability

Reliability is the assurance that a given system will perform its mission adequately under expected operating conditions.

1.3.4 Availability

Availability is the assurance that a given resource will be usable during a given time period.

1.4 Approach

The approach to this study involves three tasks:

- Examine the extent to which NS/EP operations will depend on the Internet over the next 3 years

[5] FCC 88-341, *National Security and Emergency Preparedness Telecommunications Service Priority System*, November 17, 1988.

- Identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the Public Switched Network (PSN)

- Examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

This Internet study approach provides a broad operational and design framework to examine how NS/EP operations might be affected by Internet failures over the next 3 years.

2.0 NS/EP OPERATIONS AND INTERNET TECHNOLOGIES

This section discusses the NS/EP community's use of and dependence on Internet technologies, i.e., dedicated Transmission Control Protocol/Internet Protocol (TCP/IP) networks as well as the public Internet. It is important to clarify the relationship between *use* and *dependence*. For one thing, *use* does not necessarily imply *dependence;* e.g., using the Internet as an alternative method for distributing documents is merely a convenience, and not a mission-critical dependency. For another, *use* and *dependence* are not discrete concepts, but are actually different points along a continuum; historically, as a technology becomes more prevalent and user confidence grows, its *use* evolves into *dependence*.

Therefore, for this report, NS/EP *use* of Internet technologies denotes employment of TCP/IP networks to support *non-mission critical* functions that, if disrupted, *would not impair* the ability to fulfill NS/EP responsibilities. Examples of NS/EP non-dependent use of Internet technologies include outreach and information sharing.

NS/EP *dependence* on the Internet technologies exists when a *mission-critical function* is significantly impaired by the severe degradation of a TCP/IP network. Therefore, for this report, NS/EP dependence on Internet technologies means the use of TCP/IP networks to support:

- *Mission-critical operations* necessary to respond to an NS/EP event or crisis, or
- General operational activities that, if disrupted, *could impair* the agency's ability to fulfill its NS/EP responsibilities.

2.1 Background

As evidenced by information provided to NSTAC, although the NS/EP community uses the public Internet for nonmission-critical functions, its dependence on the public Internet to support or fulfill NS/EP-related responsibilities is currently modest. Instead of using the public Internet for such critical functions, the NS/EP community depends more on dedicated TCP/IP networks. However, based on current trends, the Government's dependence on the Internet is likely to grow steadily over the next several years. Many departments and agencies, driven by cost and operational benefits, are now moving toward greater dependence on the Internet.[6] In fact, the General Services Administration's (GSA) Chief Information Officer (CIO) has urged the Government to utilize the Internet more.[7] The Department of Defense (DOD) has thousands of computers tied to the Internet and is expected to increase its dependence on the Internet for non-classified communications. It is apparent that the Internet has become as significant a technology as the telephone or the personal computer (PC). It has touched every aspect of American life from education to health care to business to emergency preparedness to weather

[6] "Feds Eye VPN to Lower Remote Access Costs," *Federal Computer Week*, January 19, 1998.
[7] "GSA's Thompson Urges Feds to Use the Internet for EC," *Government Computer News*, June 30, 1997.

forecasting.[8] It is therefore no surprise that the Government is becoming more reliant on Internet technology, on both dedicated TCP/IP networks and the public Internet, for business operations, information sharing, and communications.

This report discusses two types of TCP/IP networks, the public Internet and dedicated networks (also called intranets[9]). Although the public Internet is the primary focus of this report, it is also important to examine the NS/EP community's dedicated networks, which rely on the same protocols, architecture, applications, and hardware as the public Internet and are frequently connected to the Internet. Consequently, intranets may be subject to the same vulnerabilities as the public Internet, which are identified in this report. Additionally, these dedicated networks may rely on the public Internet for some of their functionality, including transport and connectivity functions. Therefore, public Internet vulnerabilities and failures could also affect intranets. Table 1 provides a comparison of the public Internet and intranets.

Table 1
Internet and Intranet Comparison

	Public Internet	Dedicated TCP/IP Networks/ Intranets
Architecture	The Internet consists of more than 100,000 interconnected TCP/IP networks in over 100 countries.[10] The Internet functions via a series of backbone networks, routers, and root servers.	An intranet belongs to a specific organization and consists of routers, servers and Web sites that are separated from the public Internet by firewalls.
Protocols	TCP/IP	TCP/IP
Management	No centralized management.	Centralized enterprise management.
Security*	Disparate security policies and standards focused on individual Internet components and end-user systems.	Enterprisewide security policies and standards can be implemented.
Access Control	Not restricted, the public at large has access.	Restricted to authorized users.
Routing, Connectivity, and Transport	Occurs over the 100,000 interconnected networks via publicly accessible backbones, switches, routers, and the PSN.	Occurs over dedicated fiber optic lines and other dedicated network elements including switches and routers. Can also occur via the public Internet infrastructure (e.g., the public backbone network and the PSN for transport).

*Please see Section 4.0 for information on potential Internet security vulnerabilities and implications.

The following sections address the range of the NS/EP community's dependence on TCP/IP networks.

[8] "The Whole Wired World," *Federal Computer Week*, March 30, 1998.
[9] An intranet is a private network that uses Internet-related technologies to provide services within an organization. (Source: www.netdictionary.com).
[10] http://webopedia.internet.com/TERM/Internet.html

2.2 NS/EP Community's Dependence on Dedicated TCP/IP Networks

Although the focus of this report is on NS/EP dependence on the public Internet, it is useful to acknowledge NS/EP community dependence on dedicated TCP/IP networks for reasons outlined in Section 2.1. A dedicated network, which is physically and/or virtually separate from public networks, is used by only specified entities, as opposed to the Internet, which can be used by all. The architecture of these networks mirrors that of the public Internet, including root servers and routers. Therefore, these networks are subject to vulnerabilities inherent to the public Internet, albeit on a smaller scale. Additionally, some dedicated networks also rely on the PSN for their underlying infrastructure (e.g., fiber optic lines for transport). This dependence offers additional vulnerabilities, inherent to the PSN, which subsequently could affect TCP/IP network functionality.

Despite these vulnerabilities, dedicated networks offer organizations more ability to implement and control security measures than the public Internet. Therefore, agencies are more inclined to depend on dedicated networks for their mission-critical NS/EP operations at this time. Following are some examples of dedicated TCP/IP networks in use within the NS/EP community.

2.2.1 NIPRNET and SIPRNET

DOD runs and relies on two of the largest TCP/IP dedicated networks: Nonclassified Internet Protocol Routing NETwork (NIPRNET) and Secure Internet Protocol Routing NETwork (SIPRNET). NIPRNET supports unclassified but sensitive applications, whereas SIPRNET supports applications that are classified Secret or below. Though these networks primarily support DOD, they are also used by seven civilian agencies with NS/EP functions. SIPRNET and NIPRNET are dedicated intranets, and therefore are not directly dependent on the Internet for functionality. NIPRNET, however, does provide connections to the Internet, which is a major source for downloaded material on the network. Additionally, NIPRNET relies on the PSN for transport capabilities, which makes it subject to PSN-related vulnerabilities.

2.2.2 Joint Worldwide Intelligence Communications System

The Joint Worldwide Intelligence Communications System (JWICS) is a global network designed to support Top Secret/Sensitive Compartmented Information (TS/SCI) level applications. JWICS is managed by the Defense Intelligence Agency (DIA), provisioned by the Defense Information Systems Agency (DISA), and used for secure data networking, broadcasting, and video teleconferencing. In addition to DOD, JWICS supports 15 civilian agencies with NS/EP functions.

2.2.3 Intelink

Intelink is an intelligence community intranet service that is used by DOD and 13 civilian agencies to coordinate and share intelligence information in a secure manner. Intelink operates over three security level TCP/IP-based networks. The Top Secret Intelink service operates over the JWICS backbone and consists of 121 hardware platforms and 198 virtual (nondedicated) servers.[11] The Secret Intelink service operates over the SIPRNET backbone and consists of 166 hardware platforms and 205 virtual servers.[12] The Unclassified Intelink service consists of 36 servers and operates using the Internet and a dedicated backbone.[13] Although Intelink is not directly dependent on the Internet for mission-critical information sharing, the Top Secret and Secret Intelink services use IP-based technologies deployed within the Internet. The use of this technology exposes Intelink to many of the same vulnerabilities as the Internet.

2.2.4 Open Source Information System

The Community Open Source Program Office (COSPO) of the intelligence community operates an intranet called Open Source Information System (OSIS). OSIS, currently managed by the Foreign Broadcast Information Service (FBIS), allows access to and sharing of open source, sensitive, but unclassified U.S. Government information among a network of interconnected agencies.[14] OSIS uses an Internet architecture (Web-based) and is structured as a virtual private network protected by firewalls. The network connects with the Internet only at the firewall locations. Agencies can access OSIS through a direct connection, a dial-in connection through a firewall, or through the public Internet via desktop tunnels facilitated by encrypting routers. Additionally, the OSIS Extranet enables International agencies to access the OSIS intranet via a proxy server.

OSIS does not depend solely on the public Internet for its functionality. However, OSIS relies on Internet architecture (including its own Domain Name System [DNS] server and is therefore subject to vulnerabilities affecting the public Internet. Additionally, OSIS relies on a commercially provided virtual private network infrastructure for its operations. This infrastructure also supports Internet and other data traffic, as well as PSN traffic. Therefore, OSIS could be affected by a severe disruption in Internet service.

2.3 NS/EP Community's Current Dependence on the Internet

Most Federal departments and agencies now use or have a presence on the Internet. However, few agencies currently depend on the public Internet to support mission critical NS/EP operations. Some agencies do depend on Internet applications, including remote access and

[11] Intelink Management Office, briefing to the Network Group, July 14, 1998.
[12] *Ibid.*
[13] *Ibid.*
[14] Community Open Source Program Office Open Source Information System Briefing, December 8, 1998.

secure Web sites, which, if impaired, could affect certain administrative and coordinating capabilities in support of NS/EP operations and functions.

2.3.1 Remote Access

Several agencies, including the Departments of Agriculture, Justice, and State, use the Internet for remote access to agency networks. The Department of State, for example, now uses America Online (AOL) as an international Internet Service Provider (ISP) to provide access to the Department's unclassified network for the Secretary of State and her staff while traveling overseas. In this instance, the Internet helps support an important communications function.

2.3.2 Secure Web Sites

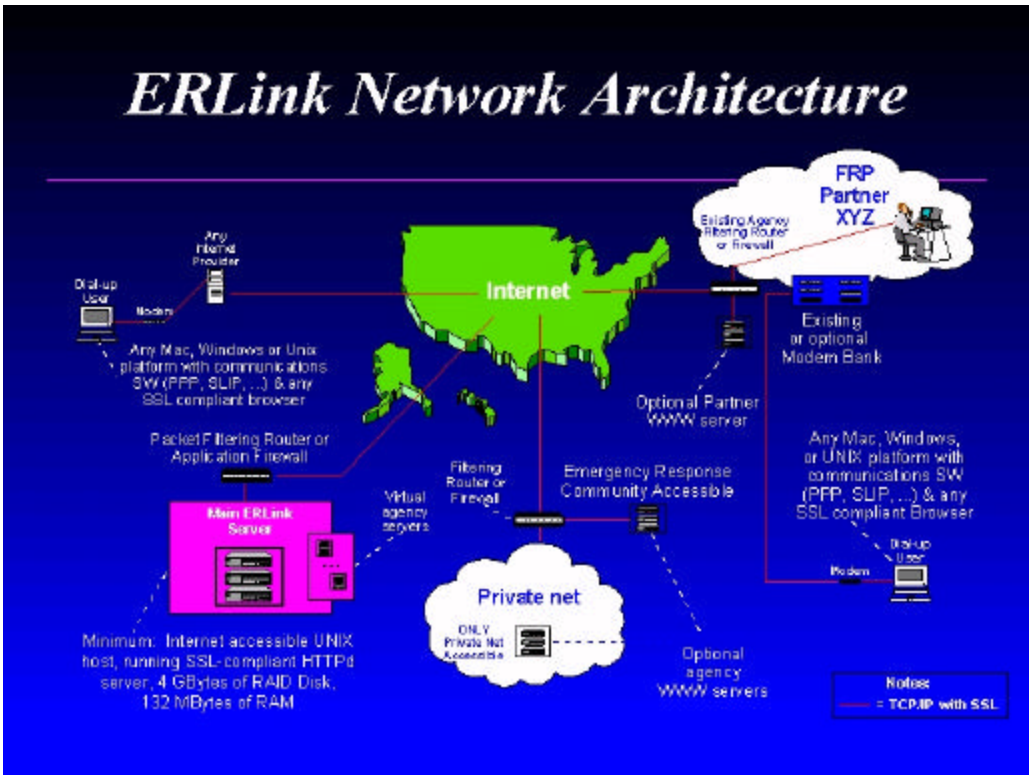
In addition to remote access, a number of departments and agencies have employed secure servers to place proprietary/sensitive data on the Web. Authorized users, through use of various protocols, can access these secure sites remotely via the Internet. An example of such a protocol is Secure Socket Layer (SSL), which is built into most Web browsers, including Netscape and Microsoft Internet Explorer. This protocol provides 128-bit encryption for secure data transmission across the Internet. Examples of secure NS/EP Web sites include those for Emergency Response Link (ERLink) and the National Security Telecommunications and Information Systems Security Committee (NSTISSC).

2.3.2.1 ERLink

ERLink was initiated and is maintained by the NCS. It is a controlled access Web site that is accessible via the Internet and dial-up modem. ERLink was established to enable electronic information sharing and rapid exchange of information in support of disaster response planning and operations among the participants in the Federal Response Plan (FRP) and State and local governments.[15] FRP agencies can upload and download emergency response reports, documents, and related disaster information. Several agencies with NS/EP responsibilities (e.g., Federal Emergency Management Agency [FEMA], GSA, NCS, and the Nuclear Regulatory Commission [NRC]) use ERLink to view disaster information from Government agencies and the response procedures used, identify agencies responsible for the 12 emergency support functions (ESF), and identify points of contact (POC) in the various ESF-defined regions across the country. In addition, ERLink mirrors data from the National Hurricane Center and hosts the FEMA Daily Report, which is a synopsis of current activities, status of declarations, and observations of pending events.[16] Figure 1 illustrates the ERLink network architecture.

[15] http://www.ncs.gov/erlink.html
[16] *Ibid.*

Figure 1
ERLink Network Architecture



Source: NCS Web Site

2.3.2.2 NSTISSC

NSTISSC is also beginning to use a secure Internet Web site to coordinate policy review and approval among its members. Policy issuances are placed on the Web site, and committee members can post their comments and vote on the issuances. This enhanced efficiency and coordination is particularly important for NSTISSC because policies are now expected to undergo more frequent revisions to keep pace with rapid technological advances.

2.3.3 Conclusion

Although these examples demonstrate the NS/EP community's dependence on the public Internet to perform important agency functions, most mission-critical operations are currently carried over dedicated intranets. However, as agencies consider adopting Internet technologies more extensively over the next several years, and as technological advances increase security and reliability of the public Internet, some mission-critical activity may eventually take place via the Public Internet. As this change takes place, a severe disruption of Internet service could have a significantly greater effect on NS/EP operations and services.

2.4 NS/EP Community's Current Use of the Internet

Agencies with NS/EP missions are currently using public Internet Web sites mostly for outreach, information sharing, and e-mail. These types of functions do not support mission-critical operations. Therefore, if a severe disruption of Internet service occurs, loss of these capabilities would not affect an agency's ability to respond to an NS/EP situation or perform functions considered critical to NS/EP operations. These capabilities are, however, included in this report to convey a general understanding of the primary current uses of the Internet, and to illustrate that the NS/EP community is increasingly using the Internet for a variety of general functions. The agencies discussed in this section are the NCS, FEMA, DOD, and GSA.

2.4.1 National Communications System

The National Communications System (NCS) has a Web site that provides information on and links to various NS/EP programs and services, including Government Emergency Telecommunications Service (GETS) and TSP. The TSP home page (http://tsp.ncs.gov) includes important information regarding the administration and operation of the TSP System. It also provides access to electronic versions of TSP user and vendor documents and forms.

2.4.2 FEMA

FEMA also uses the Internet for outreach and information sharing. For instance, the FEMA Web site provides storm information during hurricane season. FEMA posts timely information on storm tracks and offers fact sheets outlining what residents can do to prepare for storms. Additionally, FEMA posts Operation Center locations and Emergency Support team information on its site. The popularity of this service was evident during a recent hurricane. The high volume of people seeking emergency weather information caused access delays to FEMA's Web site.[17]

2.4.3 DOD

DOD is also relying on the Internet for information sharing. To accelerate its move to paper-free business operations, DOD is increasingly relying on the concept of Internet-based publishing for many of its publications. For instance, most recent DOD Directives and Instructions and DOD procurement regulations are available on the Web.[18] In fact, DOD's use of the Internet for information sharing has become so widespread that the department recently revised its Web security policy. The department announced measures to remove data from sites related to military plans and exercises, unit locations, military installations, and personal data on service

[17] "Hurricane Watchers Clog Weather Web Sites," *New York Times* Web site, http://www.nytimes.com/library/tec…08/cyber/articles/27hurricane.html, August 26, 1998.
[18] *Defense Reform Initiative Report*, November 1997, p. 5.

members.[19] The move was a response to concerns that terrorists and other hostile forces might be able to gather sensitive information on U.S. forces from the department's estimated 1,000 Web sites.[20] It also serves as an acknowledgment of the pervasiveness of the Internet and the World Wide Web (WWW).

2.4.4 GSA

Recently, GSA established Commerce, Internet, and E-mail Access (CINEMA) Services, a contract vehicle that provides a comprehensive package of value-added electronic services including electronic commerce, Internet services, and electronic messaging for the Federal Government. CINEMA simplifies the procurement process for Internet-based services, and subsequently may encourage increased Internet use among departments and agencies. "CINEMA is the Federal Government's 'Ticket to the Future' to help agencies conduct more of the Government's business electronically," said GSA's Federal Telecommunications Service Commissioner Bob Woods.[21]

2.4.5 Other Agencies

Other agencies in the NS/EP community, including the Department of Commerce (DOC) and the Department of Energy (DOE), provide extensive information on their respective Web sites including general agency information, press releases, and agency reports. Most sites also offer e-mail and additional contact information for various agency personnel.

2.5 Future NS/EP Dependence on the Internet

Although the Federal Government is still heavily reliant on dedicated TCP/IP networks, its dependence on the public Internet is likely to grow over the next several years. Numerous Federal chief information officers (CIO) have gone on record indicating the Federal Government's need to utilize the Internet. For instance, GSA's CIO noted that the cost and operational benefits of employing the Internet are too significant to ignore. In his words, "Agencies must start building corporate network infrastructure (based on the Internet) or risk being left out of the emerging global electronic commerce system."[22]

Even organizations with significant security concerns, such as the U.S. Navy, are encouraging the use of the Internet for communications. In February 1998, the Pacific and Atlantic fleets established an Internet policy promoting the widest permissible use of their systems and

[19] "DOD's Hamre Spells Out Web Rules," *Federal Computer Week*, September 28, 1998.
[20] "DOD Reels in Content on Web Sites," *Federal Computer Week*, September 21, 1998.
[21] GSA News Release, World Wide Web, http://post.fts2k.gsa.gov/cinema/.
[22] "GSA's Thompson Urges Feds to Use the Internet for EC," *Government Computer News*, June 30, 1997.

networks to access the Internet, surf the WWW, and communicate through Internet based e-mail.[23]

The Federal Government is also beginning to recognize the potential benefits of Internet-based commerce. The *Defense Reform Initiative Report*, released in November 1997, states that in the future DOD intends to use Internet technology for commercial contracting and procurement.[24] Vendor items will be made available online, and prospective purchasers can browse through electronic catalogs or search electronic "malls" that provide one-stop shopping, with access to multiple catalogs. The initial focus will be on base facility support items, whereas future enhancements will include adding more vendors and catalogs to improve logistics support to DOD customers.[25]

The State Department has made expanding the use of Internet resources a priority. A formal risk analysis of expanding the Internet throughout the department has been conducted, and known risk factors are being considered in the Internet expansion.[26] The network will be segmented, controlled interfaces will be implemented, and the processing and transmission of sensitive unclassified information will be restricted.[27]

2.5.1 Evolving Technologies and Applications

Some of the evolving Internet technologies and applications of particular interest to the NS/EP community are discussed in this section. These technologies and applications may directly or indirectly stimulate increased NS/EP dependence on the Internet by offering added functionality, diversified capabilities, and increased security and reliability of networked communications and applications. The topics discussed include Virtual Private Networks (VPN), packetized voice, videoconferencing/streaming, Internet Protocol Version 6 (IPv6), Internet Protocol Security (IPSec), priority Internet traffic, and the Next Generation Internet (NGI).

2.5.1.1 Virtual Private Networks

One of the more promising technologies is virtual private networks (VPN), which uses the Point-to-Point Tunneling Protocol (PPTP) across the Internet to create an encrypted "tunnel" between two locations. This allows users to access a network remotely while ensuring the confidentiality of data transmitted across the Internet. Sophisticated digital certificates provide stringent access control to identify and authenticate users.

[23] "Navy Urges Use of the Net for Most Data Comm," *Government Computer News*, March 16, 1998.
[24] *Defense Reform Initiative Report*, November 1997, p. 5.
[25] *Ibid.*
[26] *Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations*, GAO/AIMD-98-145, May 1998, p. 18.
[27] *Ibid.*

Like most Internet technologies, the benefits of VPN are both operational and cost-based. VPNs can reduce the cost of dial-up access via modems or leased lines. Furthermore, since VPNs can function in many respects like dedicated networks, a number of agencies are considering using VPNs instead of buying their own hardware and software to build voice or data networks.[28] In general, Federal use of VPN technology has been limited to pilot projects in the defense and intelligence agencies. For example, the Defense Advanced Research Projects Agency (DARPA) has worked with Netscape Communications Corporation to set up a VPN, called Extranet for Security Professionals, that allows security officers from most Federal agencies to coordinate their activities. In addition, the National Security Agency (NSA) has begun testing a number of VPN products for use in the intelligence community.[29]

Civilian agencies are also beginning to investigate VPN technology. Officials at the Centers for Disease Control and Prevention are researching VPN technology to connect their internal networks to field offices and public health organizations, which supply the agency with crucial health data.[30] Other civilian agencies considering VPN technology include the National Oceanic and Atmospheric Administration and the Treasury Department.

2.5.1.2 Packetized Voice

Another promising technology is packetized voice, including voice over Internet Protocol (VoIP), voice over frame relay, and voice over asynchronous transfer mode (ATM) that enables real-time voice communications over data networks using cell or packet-based transport.[31] The absence of Internet regulation has enabled VoIP, or IP telephony, to flourish, since it is not subject to fees applied to common carrier based telephony. In addition, IP telephony technology is improving in quality and increasing in scope: today IP phone calls can be made from PC to PC, phone to PC and vice versa, and phone to phone. However, since this technology is less mature than VPNs, there is significantly less implementation of IP telephony. In addition, regulations may be imposed on Internet telephony that could increase costs for IP-based telephone calls and stifle the growth of VoIP. Despite the uncertain future of VoIP, a number of agencies are beginning to investigate using IP telephony, including DOD (for both the Internet and its dedicated TCP/IP networks) and DOE.

2.5.1.3 Videoconferencing/Streaming

Videoconferencing/streaming is similar in concept to IP telephony except that it also transmits video along with audio. Although the quality of video transmitted via this process is still fairly low, improvements in bandwidth and compression technologies are beginning to make this a viable application. The recently adopted international video "telephony" standard (H.320)

[28] "Feds Eye VPN to Lower Remote Access Costs," *Federal Computer Week*, January 19, 1998.
[29] *Ibid.*
[30] *Ibid.*
[31] "Voice Over IP," *Telecommunications*, March 1998, pg. 28.

promises to bring vastly more affordable video conferencing to the Internet. DOE is testing a video conferencing system based on the new standard and plans to use it to link its laboratories and university research facilities by the end of 1998.[32] This protocol and similar proprietary technologies and products may offer significant cost savings and operational benefits when fully implemented.

2.5.1.4 Internet Protocol Version 6 (IPv6)

IPv6 is Internet technology of interest to the NS/EP community. A proposed standard of the Internet Engineering Task Force (IETF), IPv6 promises to offer increased functionality and security capabilities for transmission of information over the Internet. The priority field in the header of IPv6 packets enables a source to identify the desired delivery priority of its packets, relative to other packets from the same source. This may enhance the efficient delivery of applications such as real-time communications and multimedia over the Internet.

2.5.1.5 Internet Protocol Security (IPSec)

A relatively new security development, IPSec, is nearing commercialization. IPSec is a suite of protocols designed to provide high-quality security for Internet traffic.[33] It provides security services at the Internetwork (Internet Protocol [IP]) layer by enabling a system to specify required security protocols, determine the algorithm(s) to use for the service(s), and put in place any crytographic keys required to provide the requested services.[34] Essentially, IPSec enables corporations to extend their extranets to trading partners for secure business-to-business electronic commerce and tie intranets to remote locations without concern about the compatibility of the security protocols utilized. IPSec acts as an umbrella for various encryption methods, ranging from public-key exchanges and digital certificates to secure tunneling.

A number of vendors (e.g., Cisco Systems Inc., TimeStep Corp., and RedCreek Communications, Inc.) are expected to follow with security products based on the latest IPSec specifications. In addition, the Automotive Network Exchange (ANX), a consortium of automakers, has been encouraging security vendors to ensure that IPSec products work together and are fully interoperable. ANX is building what could be the largest trading extranet in the world and is performing interoperability tests with several vendors. IPSec and other security technologies may help to promote the NS/EP community's use of IP networks and the Internet.

2.5.1.6 Priority Internet Traffic

The Department of Energy has tested a technology that may enable Internet users, especially Federal researchers, to speed delivery of marked high-priority information through a congested

[32] "Energy Aims Sights on ATM," *Government Computer News*, January 12, 1998.
[33] IETF Network Working Group, *Security Architecture for IP*, Internet Draft, July 1998.
[34] *Ibid.*

path on the Internet by bypassing traffic not marked for quick passage.[35] Such a priority Internet service could prove useful to the NS/EP community to support critical telecommunications requirements, including voice and video applications that require large quantities of bandwidth. For example, it could benefit military applications, such as testing weapon systems, by using simulations rather than physical prototypes.[36] Other uses could include electronic commerce and real-time applications such as telemedicine.

2.5.1.7 Next Generation Internet

Several Federal agencies, including DARPA, NSF, and NASA, are supporting the NGI, a project to develop a higher bandwidth Internet designed to support multimedia applications. NGI will facilitate new and more capable networking technologies to support Federal agency missions and will create a foundation for more powerful and versatile networks in the 21st century. NGI, and other technologies listed above, will be discussed in greater detail in Section 5.0, Internet Initiatives and Evolving Technologies.

2.5.1.8 Conclusion

Some of these evolving technologies and applications may improve certain aspects of Internet security (e.g., VPNs and IPSec will address confidentiality, integrity, and access control); others may address NS/EP requirements (e.g., IPv6 and DOE's priority Internet traffic may address priority services). Therefore, these applications and technologies may help to improve the robustness of individual components of the Internet. To the extent that an outage might be caused by the failure of a particular component, improving its robustness can improve the overall reliability and availability of Internet service. However, there is no overall, unified approach to ensuring Internet reliability and availability.

2.6 Critical Infrastructures' Dependencies on the Internet and Consequent Impacts on NS/EP Operations

Critical infrastructures, including medical services, banking and finance, and gas and electric industries, are increasingly using the Internet for various processes, including exchange of business, administrative and research information. Therefore, if the Internet experienced a severe disruption of service, critical infrastructures that depend on the Internet could also experience disruption in services. However, these infrastructures currently view the Internet as too unreliable and insecure to embrace it as a primary means of executing mission-critical activities. Because the reliability and security of these infrastructures can be essential to NS/EP, it is not prudent for them to abandon other more trusted methods of telecommunications (e.g., the PSN) for the Internet at this time. Additionally, the Internet is currently too vulnerable and

[35] "DOE Tests Tool to Speed Priority Internet Traffic," *Federal Computer Week,* April 20, 1998.
[36] *Ibid.*

untested to be a viable tool for managing the control elements of critical infrastructures.[37] Various critical infrastructures' use of the Internet is discussed below.

2.6.1 Financial Infrastructure

The Internet, which is the fastest growing sector of the financial and technology marketplace, is widely seen as a "must have" delivery channel for information, services, transactions, and commerce.[38] The utilization of the Internet for financial infrastructure noncritical systems and operations will likely continue to grow. However, the financial infrastructure currently views the Internet as too insecure and unreliable for use in mission-critical systems. In fact, most financial institutions view the Internet as a very high-risk environment, and isolate their Web sites from all internal systems.[39] Sites that allow customers to access account information and initiate transactions are not directly linked to the cash management systems holding their funds.[40] The Computer Emergency Response Team (CERT®) Coordination Center, Software Engineering Institute, Carnegie Mellon University, examined several financial institutions that use Internet connections to provide information to existing and potential customers. CERT® found that systems utilizing the Internet do not directly control financial transactions, but are connected through firewalls to networks that also support systems critical to financial transactions.[41]

Rather than rely on the public Internet for mission-critical operations, the financial industry relies heavily on dedicated networks for mission-critical systems and operations. This trend is likely to continue for the foreseeable future. The utilization of these dedicated networks lessens the impact of a severe service disruption of the public Internet upon the financial infrastructure. Although a severe disruption of Internet services may inconvenience a bank's customers, preventing them from performing tasks such as checking their balance, it would not affect essential, high-impact functions, including the transfer of funds between financial institutions, nor would it affect the bank's internal processes.

2.6.2 Gas and Electric Power Industries

The gas and electric power industries are also increasingly relying on the Internet for various business practices. The gas industry is moving from use of proprietary bulletin boards to the Internet to exchange business information, including information on transmission capacity availability. In 1996 the Federal Energy Regulatory Commission (FERC) under Order No. 587 required interstate pipelines to offer standardized electronic data interchange (EDI) over the Internet for key business functions. In addition, the electric power industry is rapidly evolving

[37] National Research Council, Computer Science and Telecommunications Board, *Trust in Cyberspace*, 1999, pp. 56-57.
[38] The President's National Security Telecommunications Advisory Committee (NSTAC) Financial Services Risk Assessment Report, December 1997, p. 47.
[39] *Ibid.*, p 35.
[40] *Ibid.*
[41] Report to the President's Commission on Critical Infrastructure Protection, CERT, January 1997, pp. 13-14.

toward use of real-time applications as the industry is operating under the mandate of the Electric Consumer's Power to Choose, which requires utilities to provide retail choice by December 15, 2000.

A 1995 FERC order (Order No. 889) required each public utility (or its agent) that owns, controls, or operates facilities used for the transmission of electric energy in interstate commerce to create or participate in an Open Access Same-time Information System (OASIS).[42] To take advantage of open-access nondiscriminatory transmission service, customers will need to have information such as the available transmission capacity and prices. OASIS will provide them electronic access to this information on a real-time basis.[43] FERC requires each utility to make its OASIS nodes available through the Internet via WWW browsers. For security purposes, all OASIS customers must satisfy a registration process prior to being offered access to transmission service information.

The Internet currently supports business activities of the energy infrastructures at a high level, but is not relied on to perform critical operational and business functions. However, as the Internet becomes more secure and reliable, electric power and gas industries are more likely to use it to support critical operational and business functions.

2.6.3 Telecommunications Industry

The telecommunications industry is also increasingly using the Internet for various business practices. However, at present there is no critical dependence on the Internet for the operational functioning of the PSN. Furthermore, Internet usage may present challenges for capacity management of the PSN, but the operation of the PSN is not dependent on the Internet.[44]

Some switch vendors are using the Internet as one means of offering software patches and updates to telecommunications service providers via encrypted links. Once the software is received, it is validated in the service provider's laboratories before being loaded into the PSN network. Although currently not a critical dependence on the Internet, it is important to monitor whether this delivery method will become a primary means of acquiring software. If this delivery method becomes predominant, a severe disruption of Internet service could impact the PSN.

However, the Internet may offer an immediate vulnerability for the telecommunications industry. In today's PSN, many testing and maintenance procedures on network elements are conducted remotely, with access provided over nondedicated TCP/IP networks.[45] This may provide

[42] Sandia Labs, briefing to the Network Group, August 11, 1998.
[43] FERC Order No. 889, http://www.ferc.fed.us/news1/rules/data/rm95-9-00k.txt.
[44] Internet/PN Interconnectivity and Vulnerability Report, August 1997, p. 5-1.
[45] Assessment of PSN Component's Critical Roles and Interdependencies in Call Processing, National Communications System, September 1997, p. 56.

opportunities for a backdoor connection to be established from the public Internet to a corporate intranet, thereby providing access to a carrier's network elements.[46]

2.6.4 Medical Services

The medical service field is using the Internet more to coordinate medical advice to local emergency health services nationwide in critical health situations, including the delivery of remote medical services.[47] This practice supports the public health, maintenance and welfare, a key NS/EP service.

2.6.5 Emergency Services

As mentioned previously, FEMA operates a Web site offering emergency preparedness information during natural disasters such as hurricanes. Other emergency response organizations use the information posted on various Web sites to assist in their response and recovery efforts. For instance, the emergency management coordinator of San Marcos, Texas, recently used - gathered, Internet-posted data to track flooding conditions on the nearby Blanco River that threatened the city's 60,000 residents. By using information on the U.S. Geological Survey's real-time water data Web page (water.usgs.gov), the coordinator was able to monitor river gauges for a portion of the Blanco River 10 miles upstream from San Marcos.[48] The coordinator was able to use the data to predict the height of the floodwaters and determine which areas would be affected. Such uses will likely increase in the future as more agencies establish a presence on the Internet. However, at this time emergency services agencies are expected to use the Internet primarily to augment, rather than replace, traditional communications networks for their mission-critical operations.

2.6.6 Conclusion

Before using the Internet for mission-critical operations and services, each critical infrastructure will need to determine and implement the appropriate security controls. Expanding Internet use without effectively mitigating the potential risk will likely increase agencies' vulnerabilities to individuals or organizations seeking to damage operations[49] and to increase their exposure to Internet infrastructure reliability and availability uncertainties, which could affect efficiency of operations. Critical infrastructures, such as electric power and telecommunications, must be held to a higher standard to ensure reliability, availability, and security of mission-critical services and information. NS/EP-related activities of these infrastructures may be subject to compromise and ineffectiveness if these standards are not met.

[46] Assessment of PSN Component's, NCS, September 1997, p. 56.
[47] Report to the President's Commission on Critical Infrastructure Protection, Carnegie Mellon University/SEI-97-SR-003, CERT Coordination Center, January, 1997, p. 13.
[48] The Whole Wired World, *Federal Computer Week*, March 30, 1998.
[49] *Computer Security*, GAO/AIMD-98-145, May 1998, p. 18.

2.7 Summary

Government dependence on dedicated TCP/IP networks is significant and continues to grow. Although NS/EP dependence on the public Internet is currently modest, it is also expected to increase in the immediate future. However, concerns regarding Internet security and reliability compared with traditional methods of communication (e.g., PSN) limit the scope of mission-critical applications that organizations are currently willing to conduct over the Internet. Nonetheless, the Internet's capabilities, as well as its operational and cost benefits, are too great to ignore. As the technologies and services employing TCP/IP networks mature, the Internet and other networks will provide services that go beyond traditional data transport. If current market trends are indicators, a significant portion of the voice and video traffic now carried by other networks will be transmitted via IP networks, especially the Internet. Therefore, concerns regarding security and reliability of the Internet must be addressed by not only those organizations planning to take full advantage of the capabilities of the public Internet, but also by those companies that provide Internet infrastructure and services. Most importantly, these issues need to be examined carefully by the NS/EP community to determine the feasibility of using the Internet and emerging networks to support critical NS/EP services and operations.

In the coming years, critical infrastructures may reduce dependence on other avenues of telecommunications in favor of the Internet in efforts to save money and to take advantage of the efficiencies of data communications and new applications (e.g., VoIP). If this "technology pull" occurs, it would be important for critical infrastructures to be aware of potential vulnerabilities and address them in their risk management models.

It must also be emphasized that even though the NS/EP community does not currently depend on the public Internet for mission-critical operations, intranets for such activity can also potentially be affected by Internet failures. If an intranet relies on the public Internet for transport or connectivity between nodes, or if an intranet provides a connection to the public Internet, the intranet may be affected by Internet failures. Therefore, it is important that the NS/EP community understand the topology of their intranets and the nature of their connections to the public Internet. This understanding is necessary to mitigate and respond to the potential effects of Internet failures.

3.0 INTERNET OVERVIEW

Today's Internet is an outgrowth of U.S. Government investments in packet-switching technology and communications networks under agreements with the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (NSF), and other U.S. research agencies. In 1969 DARPA launched ARPAnet, a packet-switched network linking research facilities across the United States. ARPAnet was a decentralized network, consisting of multiple pathways between nodes. Thus, even if several nodes were disabled, communications could still continue over alternate pathways. This was accomplished by using a system of protocols developed over the course of the research effort. These protocols, collectively known as Transmission Control Protocol/Internet Protocol (TCP/IP), enable internetworking of dissimilar systems. An open protocol of this type was needed to facilitate connectivity among ARPAnet's disparate networks. As TCP/IP and gateway technologies matured, more disparate networks were connected, and the ARPAnet became known as "the Internet."[50] In 1987, the National Science Foundation (NSF) began developing a high-speed backbone between its supercomputer centers called NSFNet. Intermediate networks of regional ARPAnet sites were formed to hook into this backbone, and commercial and nonprofit network service providers were formed to handle the operations.[51] Over time, backbones by other Federal agencies and organizations were formed and interlinked with NSFNet. In 1995, commercial Internet service providers took control of the major backbones, and the commercial Internet as we know it today was realized.

This section provides an overview of several fundamental concepts concerning the Internet and provides a general explanation of the nature and role of its network architecture. Specifically, the section contains an overview of Internet functional components and operations, and information on organizations guiding management and development of the Internet.

3.1 Internet Terminology

Appendix C is a glossary of terms used in this document to describe Internet infrastructure, software, and administration.

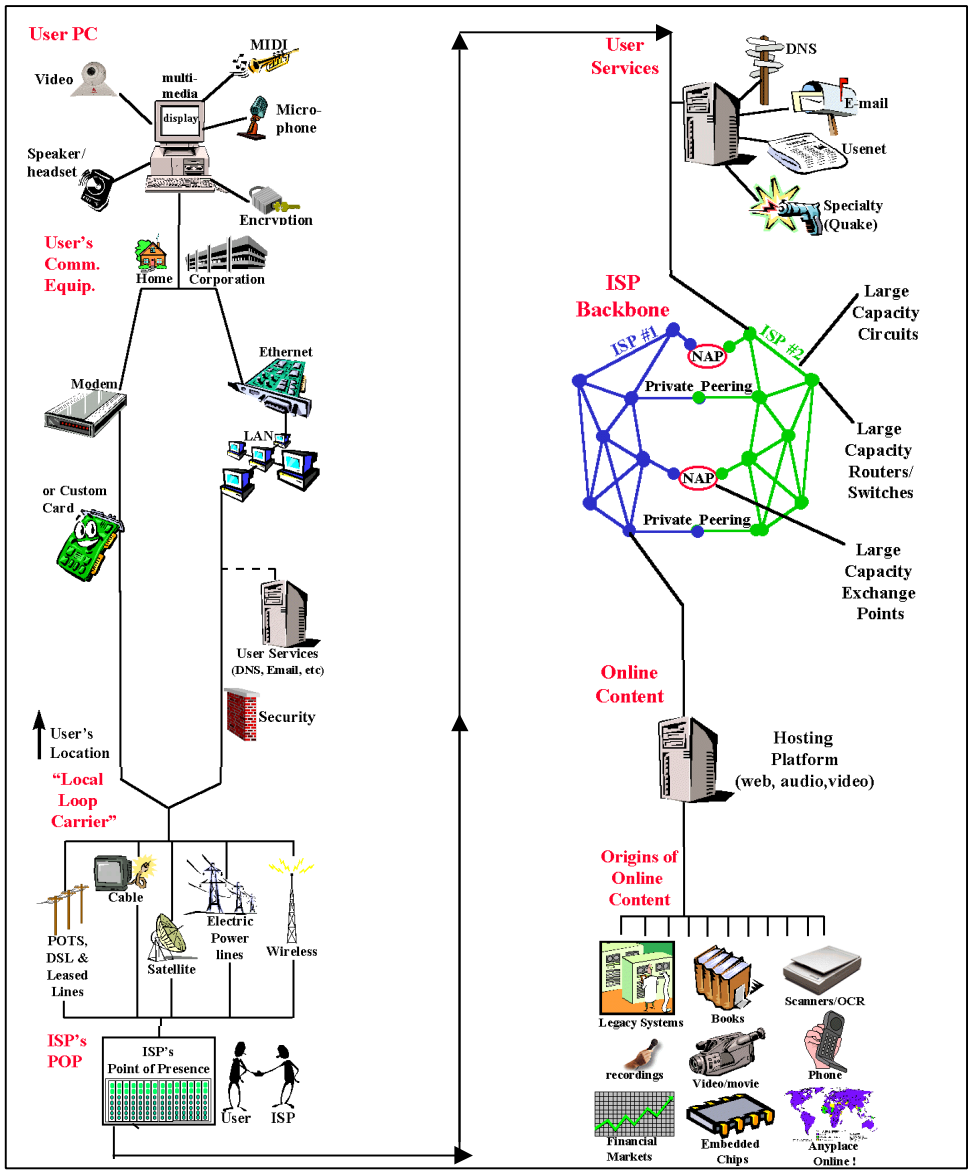
3.2 Internet Functional Components

The Internet is constantly evolving to meet the demands of new users and new services. Its support infrastructure has evolved from mainframes and large minicomputers using dedicated transmission lines to low-cost routers and dial-up access from modems on PCs. Additionally, a growing support industry is providing Internet services, software, and content. Figure 2 illustrates how the Internet functions from the end user to online content.

[50] http://www.techweb.com/encyclopedia/defineterm?term=ARPANET
[51] *Ibid.*

As shown below, the user's PC connects to a local loop carrier (e.g., Bell Atlantic) via communications equipment (e.g., a modem). The local loop then connects the user to an Internet service provider's (ISP) point of presence, which represents the edge of the ISP's network. From there, a user is connected to the services offered by the ISP, such as e-mail. Additionally, the ISP provides connectivity to other ISP networks via backbone networks. Through their connection to the Internet, users link to host sites that provide data from a variety of sources.

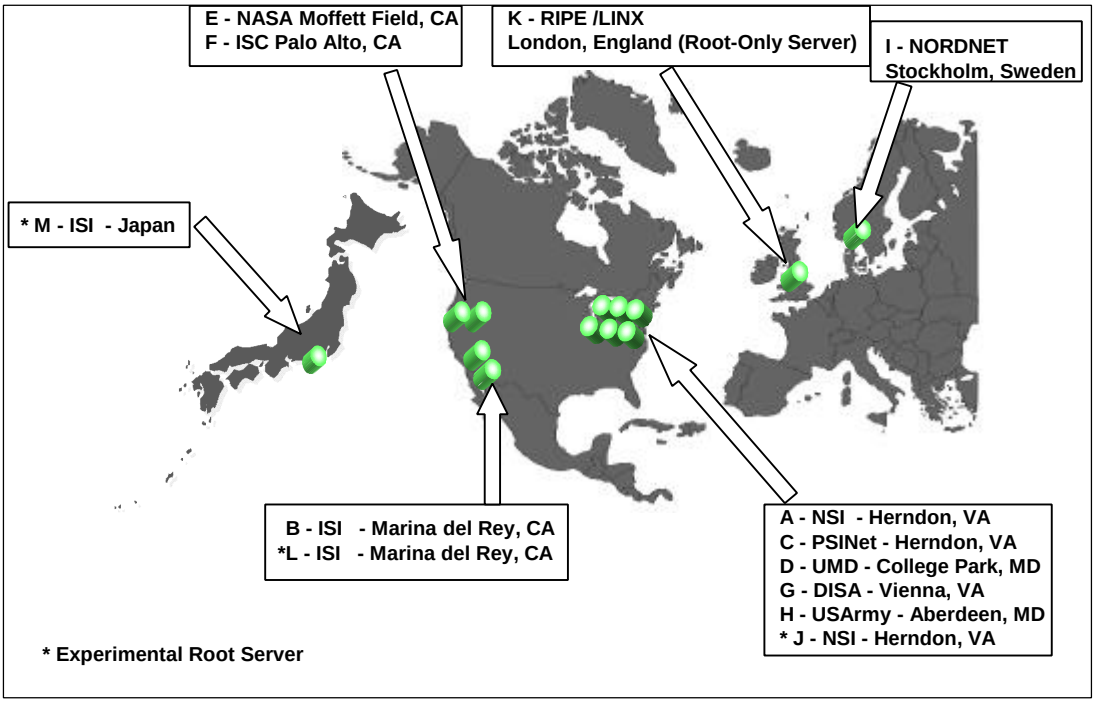
Figure 2
Internet Overview



Source: Internet: The Big Picture, http://navigators.com/internet_architecture.html

A critical element of the Internet is the domain name system (DNS) which, in part, consists of a series of root servers. The main "A" root server, which contains all the primary domain names, is currently maintained by Network Solutions, Inc., Herndon, VA. This data is also replicated on several servers nationwide and abroad. Figure 3 illustrates worldwide locations of the Internet's root servers.

Figure 3
Worldwide Root Server Locations



Source: The New Commercial Internet: Policy Initiatives to Promote Stability, NSI, March 1998.

DNS software translates user-friendly domain names (e.g., www.ncs.gov) to IP addresses (e.g., 123.4.5.67) of the destination computers. (Queries for this translation initially occur at the root servers.) Every computer attached to the Internet has a unique IP address. Without the IP address, routers would not be able to direct packets of information to the correct network node. The following subsection discusses the operational infrastructure of the Internet in greater detail, concentrating on the various tiers of ISPs.

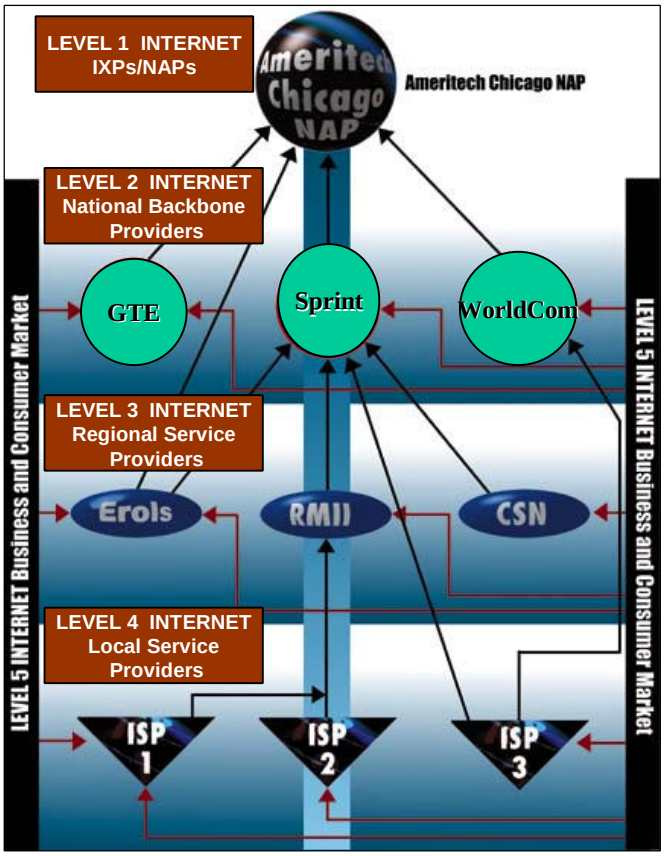
3.3 Internet Infrastructure Operational Overview

The Internet is composed of IXPs and national, regional, and local ISPs serving end users and organizations. This infrastructure can be divided into five levels:

- **Level 1: Interexchange Points (IXP)** (also known as Network Access Points [NAP] or Metropolitan Area Exchanges [MAE]; the terms are used interchangeably). IXPs represent the highest tier in the Internet infrastructure. They provide a common interconnection location for ISPs.
- **Level 2: National Backbone Providers (NBP)**. The second tier and the first category of ISPs. An NBP owns or leases its own backbone network and has a nationwide customer base. MCIWorldCom is an example of an NBP.
- **Level 3: Regional Service Providers (RSP)**. RSPs also own or lease their own backbone networks, but each serves only a single region. Erols is an example of an RSP.
- **Level 4: Local Service Providers (LSP)**. LSPs are smaller companies that typically purchase service from higher tier providers and resell it to customers.
- **Level 5: End Users and Organizations**. This tier consists of the business and consumer market that connects to the Internet via the above organizations.

All these components are tied together through various interconnection agreements. Figure 4 illustrates the relationships among the tiers.

Figure 4
Internet Infrastructure Tiers



Source: Boardwatch Magazine

Although each tier has distinct characteristics, many providers operate in two or more tiers. In addition, the infrastructure is a mix of hierarchical (local service provider to regional service provider) and flat associations (ISP to ISP). For clarity, Figure 4 does not show every possible combination of interconnections between the various ISPs and the interexchange points. However, all the various types of interconnections are represented. The first four architecture tiers are described below.

3.3.1 Interexchange Points

Although becoming less important because of peering arrangements among Internet service providers, IXPs still provide an essential interconnecting function for the Internet. IXP facilities generally have high-speed network architectures capable of interconnecting various wide area network (WAN) technologies. ISPs connect to the IXP through either a large-capacity router or an asynchronous transfer mode (ATM) switch. Once connected, each ISP must negotiate interconnection agreements with other ISPs connected at that IXP. After an agreement is

established, a route server within the IXP network broadcasts each party's routing and addressing information to each ISP's router. Incoming packets are routed to the high-speed network where the route server indicates the possible routes available to the packet. Figure 5 illustrates the location for selected major IXPs.

Figure 5
Major IXP Locations

Source: Boardwatch Magazine

IXPs are privately owned and administered by interexchange carriers (IEC), incumbent local exchange carriers (ILEC), competitive local exchange carriers (CLEC), or ISPs. Currently, four main IXPs or NAPs, are located in New Jersey, Chicago, Los Angeles, and Washington, DC. In addition, MFS operates MAEs in large urban areas nationwide. MAEs serve the same function as IXPs but generally provide service to a smaller geographic area. MAEs typically consist of a fiber-optic data ring around the city where companies and offices can inexpensively connect to a citywide network. Finally, there are two Federal Internet Exchange (FIX) points: FIX-East at the University of Maryland in College Park, Maryland, and FIX-West at the NASA Ames Research Center at Moffett Field in Mountain View, California. FIXs interconnect Military Network (MILNET), National Aeronautics and Space Administration (NASA) Science Net, and other Federal networks.

Large IECs, ILECs, and CLECs can provide network management for their IXPs from their PN network operations centers. Most IXP operators ensure reliability of service and provide maintenance for collocated equipment.

If an ISP has only a single dedicated connection to an IXP, this connection becomes the greatest vulnerability for this ISP. As a standard practice, NBPs and RSPs either have redundant connections to a single IXP, or they are connected to multiple IXPs. In addition, ISPs typically use different carriers for redundant connections, minimizing their dependency on a particular carrier's network.

3.3.2 National Backbone Providers

NBPs typically have a presence at all the major IXPs and have interconnection agreements with other major NBPs at these IXPs to carry each other's traffic. Most NBPs have a network infrastructure consisting of routers and switches. The routers are typically owned by the NBP, and most large NBPs have their own switching networks with point-to-point leased lines from various IECs.

Table 2 lists the top Internet backbone companies with market share based on percentage of ISPs connected to each company's network.

Table 2
Top Internet Backbone Companies

Provider	Description	Market Share (%)
Cable & Wireless (Internet assets formerly owned by MCI Communications)	Composed of 22 domestic nodes; 15,000 interconnection ports; more than 40 ongoing peering agreements; routers; switches; modems; e-mail servers; and other equipment dedicated to its support.	31
Sprint	Consists of more than 500 domestic points of presence over a SONET ring architecture. Provides dialup and direct access to business and residential customers.	22
MCI WorldCom	MCIWorldCom has acquired assets from UUNET, MFS, ANS Communications and CompuServe to become an Internet leader. Customers include America Online and the Microsoft Network.	20
GTE	Offers service to 5,000 business customers and 500,000 dial-up residential users	4

Source: Business Week, July 20, 1998, p. 60.

NBPs rarely sell directly to small consumers (e.g., small businesses and residential customers) because of the added "customer handholding" required by the less experienced users. Instead, NBPs sell their services to large businesses and other resellers such as RSPs and LSPs.

However, some NBPs, such as PSINet, do not allow customers to resell their network services.

3.3.3 Regional Service Providers

RSPs rely on LECs and IECs for transport. To transfer traffic over the Internet, RSPs usually have interconnection agreements with NBPs, and connect directly to the NBP or to an IXP where traffic is transferred to the NBP network. RSPs are attractive to residential and small business customers because they can offer more "hands-on" assistance to less knowledgeable users. Regional Bell Operating Companies (e.g., Bell Atlantic) that offer Internet service fall into this category.

3.3.4 Local Service Providers

Some LSPs have their own network infrastructures and rely on LECs for transport. However, many LSPs do not have their own infrastructures. Instead, they purchase service from NBPs and RSPs and resell this service to residential and small business customers. These LSPs usually operate out of a single site with a modem bank for customer access and a T1 connection to the NBP or RSP network. Typically, unlimited access is provided monthly for a flat-rate fee or a combination of flat-rate and usage-based pricing. LSPs specialize by providing value-added services, such as Web page hosting and development, security management, and electronic commerce consulting.

3.4 Interconnections

The policies for data exchange between ISPs are defined by the parties involved. Agreements typically specify how traffic is carried and transferred, and how billing is handled. There are two basic types of exchange policies:

- **Peering.** A peering agreement between ISPs allows each party to access the other's customers. Peering usually occurs between providers that are roughly equal in size. Peering agreements apply at a common location, giving each ISP access to the other's customers. A peering agreement obligates a provider to advertise all of its customers' routes to all other participating ISPs and to accept customer routes advertised by these other providers. Smaller ISPs typically have peering agreements only at IXPs. Larger ISPs (NBPs) typically peer at IXPs and have private peering agreements at many other facilities where other large ISPs are collocated.

- **Transit.** If an ISP is not accepted as a peer by another (e.g., not of equal size), the rejected company must become a customer to send data across the larger ISP's network. A transit agreement between providers allows each party to use the other's backbone network to reach the rest of the Internet. This type of agreement is typical in ISP-reseller arrangements.

3.5 Organizations Guiding Management and Development of Internet Architecture

Several organizations currently play a significant role in Internet management, infrastructure, and operations. An overview of some of the most important organizations and their responsibilities is provided below. Note that the administrative structure of the Internet is currently in the process of being reorganized. This process will be discussed further in Section 4.0, Internet Vulnerabilities and Failure Implications.

3.5.1 Internet Assigned Numbers Authority

Every computer connected to the Internet has a unique IP address. Internet Assigned Numbers Authority (IANA) coordinates the allocation of blocks of these numerical IP addresses to regional IP registries (American Registry for Internet Numbers in North America, Researux IP Europeans in Europe, and Asia Pacific Network Information Center in the Asia/Pacific region) under contract with the Defense Advanced Research Projects Agency. Larger ISPs then apply to these registries for blocks of IP addresses, which are then reassigned to smaller ISPs and end users. IANA functions will be assumed by the new nonprofit private corporation being established to administer DNS services for the Internet.

3.5.2 National Science Foundation (NSF)

The National Science Foundation (NSF) is the agency responsible for coordinating and funding the management of the non-military infrastructure of the Internet.

3.5.3 Network Solutions, Inc. (NSI)

In 1992 NSF entered into a cooperative agreement with Network Solutions, Inc. (NSI) to manage the domain name system, register domain names for top-level domains (TLD), and maintain a directory linking domain names with the IP numbers of domain name servers.[52] NSI also operates the "A" root server, which maintains the authoritative root database and replicates this information to the other 12 root servers located throughout the world on a daily basis.

3.5.4 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is an international community of network designers, operators, and researchers that address issues related to Internet protocols, the evolution of Internet architecture, and the efficient operation of the Internet. Although the IETF focuses on the advancement of Internet technology and services through the development of standards that specify the technical parameters of Internet protocol suites (e.g., IPv4, IPv6), IANA serves as the central coordinator for the assignment of unique parameter values for Internet protocols and maintains a registry of the assigned values. The IETF consists of several working groups that

[52] Management of Internet Names and Addresses, U.S. Dept. of Commerce, Docket No. 980212036-8146-02.

provide technical analysis and solutions on various Internet-related topics including routing, transport and security. The Internet Engineering Steering Group (IESG) provides overall direction to the working groups.

The OMNCS participates in the IETF and the Asynchronous Transfer Mode (ATM) Forum working groups that develop specifications for carrying Internet protocols on high-speed ATM networks.

3.5.5 Internet Architecture Board (IAB)

The Internet Architecture Board (IAB) is a volunteer organization that provides guidance, broad direction, and adjudication to the IETF in defining the overall architecture of the Internet. It appoints the IETF Chair and all other IESG candidates.

3.5.6 Internet Society

An international membership organization dedicated to extending and enhancing the Internet. It supports Internet bodies such as the IETF and works with governments, organizations, and the public to promote Internet research, information, education, and standards.[53] It also helps developing nations design their Internet infrastructure.

3.5.7 International Telecommunication Union (ITU)

The International Telecommunication Union (ITU), headquartered in Geneva, Switzerland, is an international organization within which governments and the private sector coordinate global telecommunications networks and services. Study Group 16, the multimedia group of the Telecommunications Standardization Sector of the ITU, has begun work on a new standard for voice gateways to interface data networks with conventional telephone systems. The new standard will permit control of gateway devices that pass voice, video, facsimile, and data traffic between conventional telephony networks and packet based data networks such as the Internet.[54]

The OMNCS heads the U.S. delegation to the ITU Standardization Sector (ITU-T) Study Group 4, which develops telecommunications management network recommendations for application to geographically dispersed, nonhomogeneous networks. The OMNCS also heads the U.S. delegation to ITU-T Study Group 7. Study Group 7 is responsible for studies related to data communications networks, including the Internet, and for studies related to application of open system communications, including networking and security.

[53] http://www.techweb.com/encyclopedia/defineterm?term=Internet+Society
[54] http://www.itu.int/newsroom/press/releases/1998/98-33.html

4.0 INTERNET VULNERABILITIES AND FAILURE IMPLICATIONS

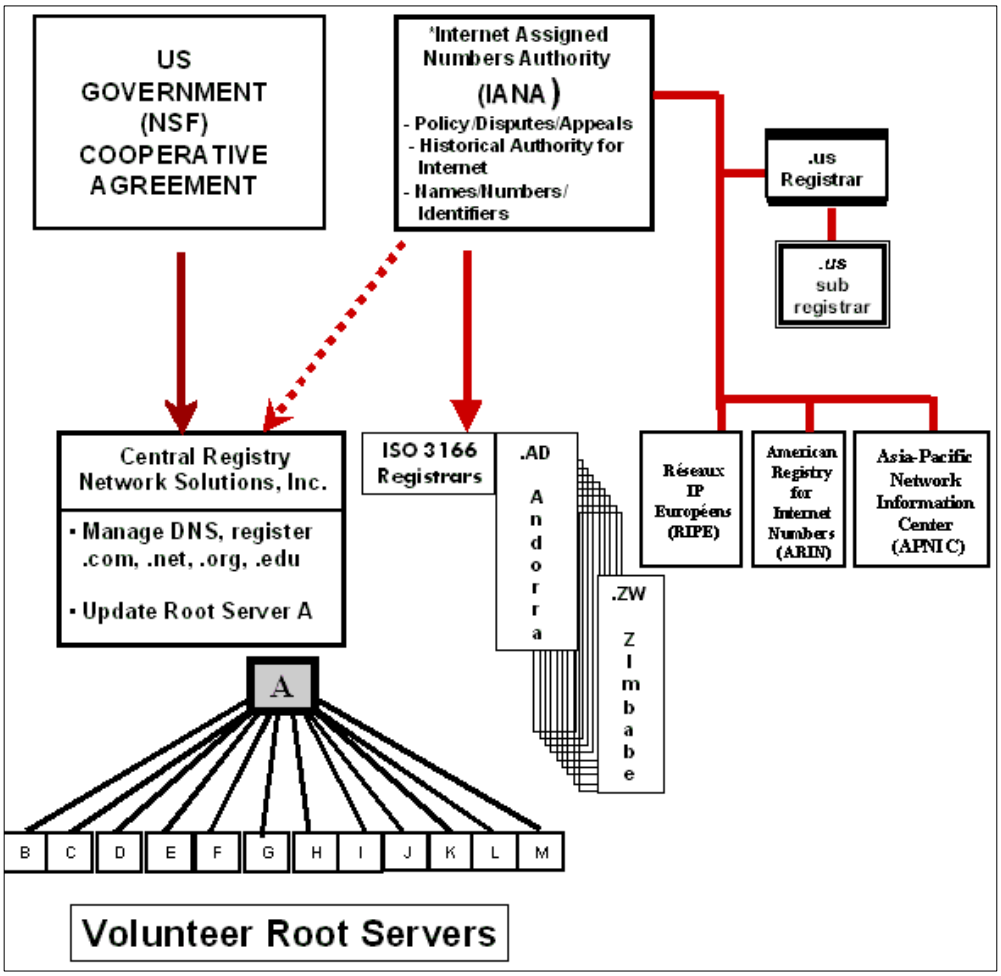
This section provides an overview of the Internet's technical and administrative vulnerabilities and associated failure implications. Although it is widely known that the Internet can be used as a medium through which end-user systems can be attacked, this paper is not intended to address those concerns because it is the responsibility of end users to develop security policies and implement security mechanisms to protect their own systems. Although it acknowledges such concerns, this study is focused on the vulnerabilities of higher level components of the Internet (e.g., Internet management and infrastructure elements) that are beyond the control of individual end-user organizations. The purpose is to identify vulnerabilities in these higher level components that, if exploited, would have far-reaching impact, resulting in sustained interruption or severe degradation of Internet service affecting multiple ISPs and degrading the ability of essential infrastructures to function.

The Internet is composed of several elements that complement each other and must operate and interact efficiently to achieve successful end-to-end communications. This section will focus on the vulnerabilities associated with the Internet's management structure and its key infrastructure components (e.g., Interexchange Points, routers, ISP infrastructure, and software). It will also discuss malicious exploitation of Internet vulnerabilities and the significance of procedural errors. Finally, it will address trends that may affect the state of Internet vulnerabilities.

4.1 Vulnerabilities: Management

Two general aspects of the management of the Internet offer the potential for concern: the distributed, informal nature of some Internet management tasks, and the fact that the management structure of the Internet is being reorganized. Although it is not possible to determine how these general aspects may lead to specific vulnerabilities, the lack of definitive control of critical functions and the uncertainty regarding how the Internet will ultimately be managed are of concern. Therefore, it is important to monitor developments related to these organizations to ensure that overall functionality of the Internet is secure and reliable. Figure 6 outlines the current administration of the Internet.

Figure 6
Internet Administration



Source: The New Commercial Internet: Policy Initiatives to Promote Stability, NSI, March 1998.

Those management functions with which specific vulnerabilities are associated include the central registration of IP parameters and addresses and the domain name system (DNS). These will be discussed below.

4.1.1 IP Parameters and Addresses

The Internet Assigned Number Authority (IANA), an Internet body chartered by the Internet Society and Federal Network Council and funded by DARPA, currently maintains a central registry of Internet protocol parameters. Internet protocols require unique names and numbers in

Internet addresses, domain names, protocol parts and private enterprise numbers.[55] IANA is responsible for assigning new Internetwide IP addresses that identify each host attached to the Internet. The efficiency and reliability of these processes are essential to sustain continued Internet operations. Any disruption in the assignment of IP addresses might result in the inability to establish new hosts.

The Internet Corporation of Assigned Names and Numbers (ICANN), a nonprofit corporation being developed by Internet industry members and associations, will soon assume responsibility for many of the Internet functions currently performed under Government contract by IANA and other entities. These functions include IP address space allocation, protocol parameter assignment, DNS management, and root server system management functions. ICANN will ultimately determine the level of competition for DNS registration (in terms of the number of registry organizations), decide whether to institute new top level domains, and be responsible for the administration of the root server system. The establishment of ICANN will help to formalize the management of important procedural and technical functions necessary for the continued operation of the Internet. Some lawmakers have voiced concerns that the private sector has drafted a consensus plan to reform governance of the DNS under ICANN without proper public input. The House Commerce Committee chairman has stated that a loss of credibility in this process will undermine ICANN's ability to administer the DNS and potentially affect the stability of the Internet itself.[56]

4.1.2 Domain Name System (DNS)

As discussed in Section 3, the DNS is a critical element of the Internet. The DNS is composed of a series of root servers and software that manage the translation of domain names to IP addresses to connect users to Internet locations. Any vulnerability affecting the main root server ("A" server) maintained by NSI[57] has the greatest potential to affect Internet service because it supplies the DNS information to the other 12 servers. If the "A" server experiences a sustained outage or propagates incorrect information, Internet operations might be severely impaired.

Although the Internet could continue to function if one or more of the redundant individual root servers ("B" through "M") went out of service for a short time period, a sustained outage (24 hours or more) among several servers could affect traffic flow and potentially affect user connectivity. More importantly, malicious tampering with the DNS (e.g., cache poisoning, malicious corruption of the servers) could severely impair Internet functionality. Additionally,

[55] http://www.techweb.com/encyclopedia/defineterm?term=INTERNETASSIGNEDNUMBERSAUTHORITY
[56] U.S. Lawmakers Start Internet Name Probe, *TechWeb*, October 16, 1998, http://www.techweb.com/internet/story/reuters/REU19981016S0003
[57] The National Science Foundation (NSF) has a cooperative agreement with InterNIC, an organization that oversees Internet domain name registration. InterNIC is managed by Network Solutions, Inc., which provides domain name registration services in .com, .net, .org, and .edu top level domains. NSI also administers the primary root server for the Internet.

the destruction or inoperability of the DNS could induce a severe disruption of Internet service, if not a complete shutdown of the Internet itself.

Note that the root server system is administered by volunteer organizations. The volunteer nature of this oversight, combined with the absence of uniform security policies and best practices, raises concerns for system security. Although the root server system has not experienced any prolonged outages or significant attacks, the lack of coordinated standards for security and administration of the servers is a concern. This factor takes on added relevance with the current efforts to privatize the DNS through the establishment of ICANN.

4.2 Vulnerabilities: Infrastructure Components

The Internet is an increasingly complex network of infrastructure components with a variety of vulnerabilities, many of which are similar to those of the PSN. For instance, cable cuts and equipment failures may affect Internet performance much like the PSN. In addition, the collocation of Internet-related equipment at PSN facilities offers a linked vulnerability between the two infrastructures. Further, the Internet is a network of networks. Any vulnerability that affects a particular network and its supporting technologies (e.g., ATM, SS7) can affect the public Internet. As with any software-dependent function, the Internet can be adversely affected by software errors and malicious code. In addition, it is subject to procedural errors that can have far-reaching impacts. The Internet's key infrastructure components and their vulnerabilities are described below.

4.2.1 Interexchange Points (IXP)

IXP vulnerabilities can affect the ISPs that rely on them to exchange data with other ISPs. Threats to IXPs can come externally through physical damage and disruption, or internally through configuration errors. IXPs can be disrupted internally from within the Internet; however, they are more susceptible to external forces. Physical destruction or disruption of a major IXP would have a severe impact on the Internet, resulting in network outages and heavy congestion. Although there has never been a case of physical destruction of an IXP, there are a few cases of disruption from other external causes. One such case occurred on July 11, 1997, when a power failure to one of MAE West's three switches caused severe congestion on the West Coast for nearly 3 hours. This problem was compounded by the extraordinarily heavy traffic going to NASA servers to download Web pages for the Mars Pathfinder mission. All ISPs sending traffic into MAE West were affected by the congestion. Although some traffic was able to route through the other two switches, most of the traffic that normally routes through the MAE West was correctly rerouted elsewhere. However, because MAE West normally handles enormous amounts of traffic, these other routers and connections quickly became overloaded.

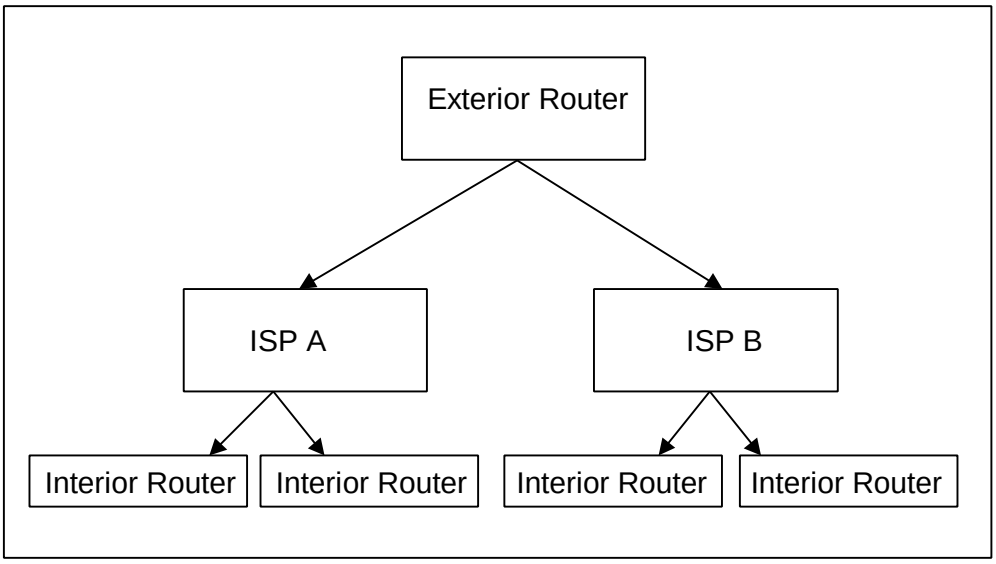
External threats to major IXPs, though rare, can greatly stress the Internet infrastructure. IXP owners protect their assets by utilizing facilities with 24-hour security, backup power, and

various forms of shielding. Except for the NAPs owned by Pacific Bell and Ameritech, most IXPs are collocated at facilities shared by interexchange carriers (IEC) and competitive local exchange carriers (CLEC). However, as more and more assets are collocated within single facilities, they become higher value targets for attack because the potential impact is greater. For example, by housing the assets for many large ISPs and IXPs, one facility provides an interconnection point for nearly 200 ISPs.[58] Destruction or disruption of this facility could have severe repercussions for the worldwide Internet. A facility can also be considered a high-value target because of the number of collocated Internet and telecommunications carrier assets.

4.2.2 Routers

By viewing the network as a compilation of network addresses and all the possible paths between them, Internet routers direct Internet traffic to its proper location(s). Routers read the network address in each packet header and determine how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Most routers owned by ISPs are collocated at facilities housing IXPs or ISP backbone switches. End users typically keep their routers at their own sites. As shown in Figure 7, routers fall into two classifications. Some routers are used to move information within a particular ISP. Routers used for this purpose are called interior routers. Routers that move information between different ISPs are called exterior routers.

Figure 7
Internet Routing Diagram



[58] Internet/PN Interconnectivity and Vulnerability Report, National Communications System, August 1997, p. 3-3.

Vulnerabilities are inherent to the routing infrastructure. Routing tables control the network topology; if there are errors in these tables, packets will be misdirected. The absence of authentication and verification of routing information in network routers could lead to a wide-scale Internet disruption. For example, on April 25, 1997, a small ISP sent incorrect Border Gateway Protocol (BGP) routing information to a major carrier causing a significant amount of traffic to be directed toward a backbone provider (MAI Network Services in McLean, VA). MAI then forwarded incorrect routing tables to Sprint Communications Co. and many other network backbone providers. The incorrect tables sent a high volume of traffic to MAI, turning major backbone providers such as ANS (which carries America Online Inc. traffic), BBN Planet, MCI Communications Corporation, Sprint, and UUnet Technologies Inc. into so-called "black holes" from the point-of-view of incoming traffic. The disruption effectively shut down a major portion of the Internet for at least 20 minutes, and experts estimated that up to 40 percent of Internet users were affected.[59] Although this disruption was caused by human error, fault also rests with the routers. MAI's routers did not detect the erroneous data because of a technical flaw.[60] This example illustrates the far-reaching effect a simple error can have on Internet service.

4.2.3 ISP Infrastructure

Many end users, including larger organizations, connect to the Internet through regional or local ISPs and, consequently, can be affected by vulnerabilities in ISP network infrastructure, operations, and maintenance procedures. An America Online, Inc. (AOL) network failure in August 1996 illustrates the vulnerable nature of ISPs. The problem occurred when Advanced Network and Services, Inc., AOL's backbone provider, updated routing tables in its backbone network as AOL was installing new switches in its LAN in Virginia. Because the AOL system was down during the ANS update, the AOL equipment did not receive the updated routing tables. When AOL brought its system back online, its routing tables were no longer valid and it was unable to reconnect to its backbone provider.[61] This caused an AOL outage that lasted 19 hours and affected 6 million subscribers. In addition, smaller ISPs may have single connections to the Internet backbone, which if disrupted can isolate their subscribers from online access. Users who depend on a single organization for Internet access can be vulnerable. To reduce the risk, many larger organizations may have redundant connections to ISPs or may choose to link directly into the Internet. However, such preventive measures may be too expensive for smaller organizations, including local emergency response organizations.

[59] http://www.zdnet.com/intweek/daily/9704251a.html
[60] *Ibid.*
[61] http://www.teledotcom.com/1096/headend/tdc1096headend_net.html

4.2.4 Software

The Internet, like all networked systems, relies on software to function. As discussed previously, the DNS software is a critical component. Additionally, there are other software-related issues that could affect the Internet's functionality. These topics are discussed further below.

4.2.4.1 Berkeley Internet Domain Name (BIND)

The Berkeley Internet Name Domain (BIND) is the UNIX software implementation of DNS that runs on the root servers of the Internet. (Note: All of the root servers and most other DNS servers attached to the Internet are UNIX-based machines.) BIND eliminates the need for a "host table" that would list all the hosts connected to the Internet and their addresses. It enables local administrators to assign their own host names and addresses and install them in a local database, which automatically distributes them to other systems as needed. (DNS is an example of a distributed database.) BIND consists of two elements: the name server, which performs name-to-address conversions, and a resolver, which queries another name server for information not cached on the original server. If a local server cannot provide the information, the process will continue until an "authoritative" name server can provide the address conversion. The databases of authoritative name servers contain the name-to-address mapping for the group of hosts they administer. If the authoritative servers cannot be reached (because of the lack of cached addressing), the request will be forwarded ultimately to the root servers, which contain the Internet addresses of the authoritative name servers for every domain.

This complex system of name servers uses the common BIND software. Therefore, the operation of the Internet could be severely affected if the software is corrupted. Additionally, the BIND software sends a complete copy of the DNS database, not just updates to the database, to root servers requesting a copy. Consequently, a corrupted file can affect all of the DNS information, not just the updates. This was illustrated by an incident that occurred at Network Solutions, Inc. (NSI) in July 1997. Each day, NSI updates the DNS database to reflect domain name additions and deletions. In this instance, the database became corrupted upon regeneration, eliminating more than 1 million companies in the .com and .net domains.[62] The corrupted database was then released to the network. The result included returned e-mails and an inability to access numerous Web sites.

Additionally, as with any software, development and maintenance procedures are critical aspects that can affect BIND security and reliability. The development, testing, and distribution processes of BIND are not as vigorous and structured as those typically employed for software that supports the PSN. This raises concern that a corrupted version of a new release of the BIND software could inadvertently, or maliciously, be distributed to all DNS servers. Disparate

[62] Internet Glitch Reveals System's Pervasiveness, Vulnerability, http://www.cs.columbia.edu/~hgs/internet/071897dns.html

implementation of BIND-related security patches among users can further complicate the problem.

4.2.4.2 Other Software Issues

Often, software vulnerabilities can be exacerbated by human factors. For example, although the NSI incident was initially a software problem, it was exacerbated by human error. Internal error-checking software detected the problem, but the employee responsible for monitoring the process ignored a warning before releasing the database. Internet software applications are susceptible to not only human error but also human malice. The lack of centralized administration of the Internet, combined with the lack of security regarding individual and corporate connections to the Internet, can allow hackers to implant malicious code.

Note that software components of the Internet may be affected by the Y2K problem. This could occur as a result of individual components malfunctioning because some Y2K problem was overlooked, or because the Y2K remediation efforts of various components might be incompatible.

4.3 Malicious Exploitation of Internet Vulnerabilities

Today's news headlines frequently describe hacker attacks against various computer networks, including military networks. Computer hackers often target organizations for their attacks. These attacks may have different objectives: to surreptitiously gather information; to inflict simple vandalism (e.g., modifying the home page of the victim); or to deny service to legitimate users.

Attacks intended to simply gain unauthorized access to information may not be detected and the victims cannot resolve the problem until they become aware of it. Acts of vandalism, such as attacks that modify home pages, are more readily detected, provided the modification is blatant, rather than subtle. For example, if an intruder replaced the photograph of a Government official with a photograph of a well-known cartoon character, it would be readily apparent; however, if the intruder changed one digit in the agency's 800 number, it might be some time before this change were detected. Although information-gathering and vandalism attacks could affect an organization's ability to carry out Internet-dependent operations, such attacks are localized in scope, and would not likely result in a severe disruption or degradation of Internet service. Furthermore, end users are responsible for implementing security policies and mechanisms to protect their information and Web sites.

Denial-of-service attacks are the most disruptive, but at least they quickly come to the attention of victims, who can take steps to resolve the problem. Such attacks can come in a variety of forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They

may also disrupt physical components of the network or manipulate data in transit, including Encrypted data.[63]

One hacker technique exploits vulnerabilities from which end-users cannot protect their systems is cache poisoning – tricking name servers into going to the wrong servers to resolve names. As evidenced by various incidents, this technique diverts Internet traffic from one site to another. In July 1997, AlterNIC, a rival domain name registry of the official Internet registrar, InterNIC, redirected users from the InterNIC site (www.internic.net) to its own site (www.alternic.net) after they typed in InterNIC's URL. In October 1998, America Online, Inc. experienced a similar diversion. Someone impersonating an AOL official sent e-mail to InterNIC requesting that the domain name address for AOL be changed to Autonet.net. This caused thousands of incoming e-mails to go to the wrong place and prevented many people from visiting AOL's Web site.[64] AOL had chosen low-level security for such changes that allowed automatic implementation of changes with no review by InterNIC personnel. More secure options are available from InterNIC involving either a password or encryption in the request for a change to an address. To prevent such occurrences, DARPA is creating a cryptographic authentication system for the Internet's domain name address system, which will function as a secure digital ID for Web addresses. The new system would work much like digital certificates, enabling the Internet's routing points to verify the origin of any given Web page. Although this may reduce the probability of hackers corrupting Web page caches or rerouting domain traffic altogether, it will not prevent individual attacks on specific Web pages.

4.4 Procedural Errors

As with any endeavor, procedural errors, while unintentional, can nonetheless significantly affect Internet operations. With respect to the prevalence of procedural errors in the telecommunications industry, the FCC's Network Reliability Council (NRC), now known as the Network Reliability and Interoperability Council (NRIC), issued a report in 1996 that suggests the magnitude of this problem. This report analyzed wireline telecommunications outages and found that procedural error contributed to nearly 25 percent of switch failures and caused more outages than did hardware or software design failures.[65] Although Internet outages have not been studied as rigorously, evidence shows that procedural errors are equally troublesome in this venue. The previously mentioned MAI Network Services incident illustrates the impact such an error can have on something as critical as Internet routing. On April 25, 1997, MAI Network Services propagated bad routing information to Sprint, announcing that the best route for all

[63] http://www.cert.org/pub/encyc-article/tocencyc.html#Denial
[64] "Fake Message Sends AOL E-Mail Astray," *Washington Post*, October 17, 1998, p. G1.
[65] "Network Reliability: The Path Forward," Compendium of Papers presented by the Network Reliability Council of the Federal Communications Commission, April 1996. (Performance Metrics Team Final Report, Sections 5.3.1 and 5.3.2, page 28.)

packets was through MAI's network.[66] Sprint sent this information to MAE East, whereupon it was propagated to many smaller ISPs that use Sprint's backbone. Soon after the bad routes were advertised, heavy traffic began to converge at MAI's routers, immediately overloading its network and forcing MAI to disconnect itself from the Internet. However, because most ISP routers were still routing traffic through MAI, many ISPs nationwide experienced temporary outages. Because all this traffic went through MAE East and Sprint's District of Columbia network to reach MAI, this infrastructure became overwhelmed and heavily congested. Although some safeguards exist to prevent such an occurrence, this disruption illustrates the susceptibility of the Internet to human error.

4.5 Natural Hazards

The telecommunications industry has sustained reliable service in part by designing facilities to withstand anticipated natural hazards and developing disaster recovery plans and procedures to restore service following such natural hazards. For example, although it is not possible to design a totally earthquake-proof building, telecommunications companies take special precautions such as bolting equipment down so that a minor tremor will not affect it. Because ISPs are more recent entrants into the communications arena and have been regarded more as a convenient, rather than essential, service, their facilities may not be as robust as those of the telecommunications carriers, and they may have less extensive disaster recovery plans. As incumbent telecommunications providers offer Internet service, and as individuals with experience in the telecommunications industry migrate into the Internet arena, the ability of ISPs to improve the protection of their facilities from natural hazards should increase. Furthermore, as Internet service becomes increasingly important to users and the business becomes increasingly competitive, ISPs may value robustness more highly and take appropriate measures to protect their facilities from natural hazards.

4.6 Trends

Most Internet users have heard of the Morris Worm, also referred to as the Internet Worm, which occurred in 1988. This instance of malicious code replicated itself from one host to another, affecting approximately 4,000 computers (about 5 percent of those attached to the Internet at that time). It caused a massive, although short lived, disruption of services.[67] Since the worm did not delete or alter existing computer files or install Trojan horses, the damage was restricted to computer downtime. Nevertheless the direct and indirect costs of the Morris Worm have been estimated at over $98 million.[68] This event led to the creation of the Computer Emergency Response Team (CERT®) Coordination Center at Carnegie Mellon University's (CMU) Software

[66] Stutz, Michael, "Net Outage: The Oops Heard 'Round the World'," *Wired Magazine*, http://www.wired.com/news/technology/story/3442.html, April 25, 1997.
[67] http://www.bus.orst.edu/faculty/brownc/lectures/virus/virus.htm#Worm
[68] Magruder, Scott; Lewis, Stanley X., Jr. (1991) "The Economic Costs of Computer Viruses," *Arkansas Business and Economic Review*, 24(4) 11-14.

Engineering Institute (SEI). CERT® has provided a critical service to Internet users, offering advice on recovering from and protecting against such attacks. Since the Morris Worm occurred, UNIX-based networks have been made more secure, and the Internet community has become better prepared to ward off another such attack. However, the growing number of computers attached to the Internet, some on networks with insufficient security capabilities, is a catalyst for similar occurrences in the future.

Because user convenience and security are often opposing factions, the temptation to overlook security holes in favor of ease-of-use often leaves the door open for disruptive events.[69] Further, as the March 1998 denial-of-service attack on Microsoft Windows NT and Windows operating systems demonstrated, end users who fail to keep current with security bulletins and do not take the time to implement fixes may be exposed to unnecessary disruptions. If the NS/EP community comes to depend on the Internet for NS/EP operations, it will be critical to implement security features to protect against all types of malicious code (e.g., viruses, Trojan horses, and worms) that can be promulgated via the Internet. Furthermore, if the Internet becomes a critical infrastructure for NS/EP, appropriate response and contingency plans related to such attacks must be developed by industry and Government (perhaps in coordination with CERT® or ICANN) to ensure continued operations.

Using digital technologies such as ATM and IP, carriers are proposing to build packet-switch-based networks that may eventually supplant traditional circuit-based switching networks. These cost-effective, efficient networks provide customers with heretofore unseen flexibility (e.g., the capability to instantly order phone lines with the click of a computer mouse[70]).

Unfortunately, with the benefits come disadvantages, such as some of the vulnerabilities listed previously in this section. Additionally, the highly competitive nature of the information technology sector encourages companies to implement new technologies quickly, perhaps at the expense of appropriate security features. For example, ATM is incompatible with Internet firewalls at certain transmission speeds.[71] This incompatibility requires users to bypass the firewalls or reduce their transmission rates. Additionally, many ATM switches do not incorporate network access control facilities into their operating systems, which means that unauthorized users could access switches, servers and hosts on an ATM network.[72] Vendors are currently introducing security systems to help mitigate these vulnerabilities.

Despite such risks, telecommunications companies have announced plans to build high-speed data networks to expand their service offerings and increase their market competitiveness. Additionally, new carriers, such as Level3 Communications, are building nationwide IP

[69] http://www1.minn.net/~darbyt/worm/lessons.html
[70] AT&T to Launch High-Speed Service, http://www.internetnews.com/isp~news/1998/09/1001-usa-att.html
[71] "New Firewall Products Coming," InternetWeek, May 19, 1997, http://www.techweb.com/se/directlink.cgi?WIR1997051903
[72] *Ibid.*

networks to offer communications services such as local, long distance, and data transmission. These trends point toward a sweeping transformation of the telecommunications market. They also raise issues regarding the convergence of networks (e.g., IP and circuit-switched). For instance, carriers must ensure that new networks interface reliably with the existing PSN. Traditional carriers will require that VoIP gateways, which convert both call and signaling information between IP networks and the PSN, meet existing telephone company reliability and certification standards. However, IP network quality of service and reliability issues are currently not well defined.

In addition, the *Telecommunications Act of 1996* mandated incumbent carriers to provide to any carrier requesting such access, nondiscriminatory access to network elements on an unbundled basis. This gives new carriers access to the PSN's SS7 network. IP network providers are planning to interface with the SS7 network to offer advanced features similar to those offered by the PSN. This increasingly complex and linked nature of public networks, combined with the integration of IP and PSN network features and technologies, makes it a challenge to ensure that networks remain reliable and secure in support of NS/EP operations.

As the architecture of the public network changes (i.e., as it migrates from circuit switched networks to IP networks), it is important to identify vulnerabilities that may be introduced by the evolving network structure and consider their subsequent impacts on the availability, reliability, and security of NS/EP services.

5.0 INTERNET INITIATIVES AND EVOLVING TECHNOLOGIES

5.1 Introduction

Numerous evolving Internet-related initiatives and technologies may help increase the performance, reliability, security, and availability of the Internet. These initiatives and technologies, along with current industry trends, will have a significant impact on the Internet's network topology and functionality, and consequently on NS/EP dependence on Internet technologies. This section provides an overview of two Internet initiatives, Internet2 and the Next Generation Internet (NGI), which are being established using emerging Internet technologies. This section also provides information on the next generation Internet Protocol (IP), IPv6, and discusses the impact of convergence of the Public Switched Network (PSN) and Internet Protocol (IP) networks and the importance of scaling issues.

5.2 Internet2 and NGI

Internet2 and NGI initiatives are laying the foundation for networks that are more reliable, versatile, and robust than the current Internet. Table 3 compares the two initiatives, and the following sections explain each project in detail.

Table 3
Internet2 and NGI Comparison

Internet2	Next Generation Internet
Funded by research universities and communications and computing companies	Federally funded
Education and research driven	Agency mission driven
Connectivity provided via Gigabit per second points of presence (GigaPoPs), and the vBNS	R&D in advanced networking technologies on a wide-area scalable testbed
Developing a wide range of applications in support of national research objectives, distance learning, etc.	Develop general purpose and agency-specific applications in support of crisis management, health care, etc.

Source: Next Generation Internet Initiative Briefing, National Coordination Office for Computing, Information, and Communications, July 1998.

5.3 Internet2

Internet2, a collaborative R&D effort among academia, industry, and Government, is being pioneered by the University Corporation for Advanced Internet Development (UCAID). The project is already meeting its organizers' primary goal: to build an academic and governmental research-only intranet separate from the public Internet. Members of the Internet2 project

include the Department of Energy, the National Science Foundation (NSF), and 135 universities.[73]

5.3.1 Internet2 Goals

Internet2 is a not-for-profit endeavor to advance the network performance and usefulness of the Internet. Primarily a private industry and academia initiative, the majority of funding for Internet2 comes from research universities and communications and computing companies. The major goals of Internet2 are as follows:

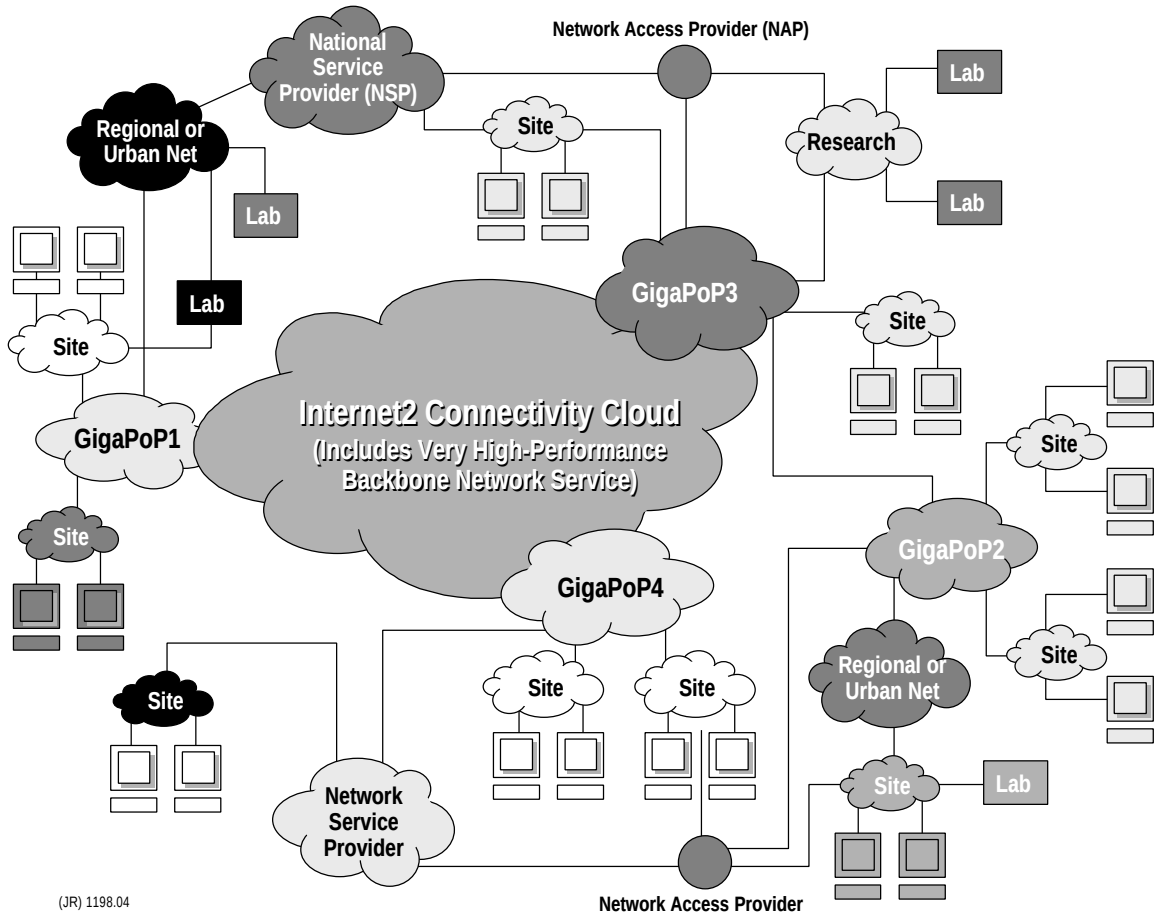
- Demonstrate new applications that can dramatically enhance researchers' ability to collaborate and conduct experiments
- Demonstrate enhanced delivery of education and other services (e.g., health care, environmental monitoring) by taking advantage of "virtual proximity" created by an advanced communications infrastructure
- Facilitate development, deployment, and operation of an affordable communications infrastructure, capable of supporting differentiated Quality of Service (QoS) based on applications requirements of the research and education community
- Coordinate adoption of agreed working standards and common practices among participating institutions to ensure end-to-end quality of service and interoperability
- Catalyze partnerships with governmental and private sector organizations
- Encourage transfer of technology from Internet2 to the rest of the Internet
- Study impact of new infrastructure, services and applications on higher education and the Internet community in general.[74]

5.3.2 Internet2 Architecture

Internet2 developers are working with several established technology companies to develop the project's backbone, which will connect campuses and laboratories. In the future, the network will include state and regional networks encompassed by the NGI initiative project. Figure 8 illustrates the key components of the developing Internet2 architecture.

[73] A complete list of university participants is available on the Internet2 Web site at the URL: http://www.internet2.edu/html/participants.html.
[74] http://www.internet2.edu/html/mission_and_goals.html

Figure 8
Internet2 Architecture



Source: IEEE Spectrum Magazine, January 1998

As shown in Figure 8, Internet2 connectivity will be provided by NSF's very high-performance Backbone Network Service (vBNS). The vBNS, established in 1995 as a 5-year cooperative project, links six NSF supercomputer centers, including the Cornell Theory Center and the University of Illinois National Center for Supercomputing Applications.[75] Initially, it was implemented to design and support gigabit-per-second (Gbps) testbeds, in which R&D in advanced networking technologies could be conducted.

The vBNS will provide the networking foundation for Internet2 by connecting the high speed switching points, called Gigabit Points of Presence (GigaPoPs). The GigaPoPs are interface

[75] "The Internet," IEEE Spectrum, January 1998, p. 39.

points for member sites, network access providers, network service providers (NSP), and regional and urban networks. A GigaPoP on the Internet2 project is the point at which a region's connectivity is aggregated. It allows universities to coordinate their links to the Internet2 network. The NAPs will serve as interconnection points between local and regional network entities to forward traffic using a more direct route and minimizing backbone traffic.

Internet2 is built on a new connectivity architecture that offers significantly higher bandwidth compared to today's capabilities. The Internet2 GigaPoPs have enough routing and switching capacity for high-bandwidth multimedia applications (e.g., streaming audio and video) and for other collaborative research tools required by top university laboratories. Internet2's advanced network infrastructure will support advanced R&D efforts for new categories of applications.

5.3.3 Internet2 and NS/EP

Internet2 is well positioned to provide the collaborative and robust R&D environment necessary among industry, academia, and Government to advance the state-of-the-art of Internet technology. It may also provide a technology framework for enhanced Internet usefulness and performance. The ultimate benefit from Internet2 will be realized if its proposed capabilities, products and services can be integrated into the rest of the Internet. Additionally, these capabilities may prove useful to NS/EP operations and services.

For instance, one of the goals of Internet2 is to enhance delivery of services by taking advantage of "virtual proximity" created by an advanced communications infrastructure.[76] The broadband throughput enabled by Internet2 could facilitate telemedicine and emergency response activities (e.g., damage assessment). Also, another goal of Internet2 is to develop an infrastructure capable of supporting differentiated Quality of Service (QoS).[77] QoS is the ability to define a level of performance in a data communications system.[78] For example, ATM networks specify modes of service that ensure optimum performance for traffic such as real-time voice and video. QoS has become a major issue because voice and video are increasingly used over IP-based data networks.[79] If the public Internet could offer the ability to guarantee a particular amount of bandwidth or maximum amount of latency, the NS/EP community may come to depend on the public Internet more. However, agencies that support NS/EP missions must attain a high level of confidence in Internet and IP network reliability and availability before using these technologies for mission critical operations.

[76] http://www.internet2.edu/html/mission_and_goals.html
[77] *Ibid.*
[78] http://www.techweb.com/encyclopedia/defineterm?term=QoS
[79] *Ibid.*

5.4 Next Generation Internet

In the 21st century, the Internet will provide a powerful and versatile environment for business, education, culture, and entertainment. The NGI initiative, together with the investment sectors (e.g., commercial and industrial business academic infrastructures, Government agency information technology [IT] programs and Government agency R&D programs) will create a foundation for more powerful networks.[80] The Federal Government has committed $100 million per year over the next 3 years to support the NGI initiative.[81] The President has stated that NGI research will –

> "…lead to a new generation of Internet capabilities that will provide connections that are not only much faster, but also more reliable, secure, and high-quality. The next generation of the Internet will facilitate a range of unprecedented new services - such as the ability to support tele-surgery and other medical services - which require extremely high levels of reliability and protection."[82]

Specifically, the NGI initiative is a Federally funded, multiagency R&D program that will accomplish the following:

- Develop new and more capable networking technologies to support Federal agency missions
- Create a foundation for more versatile networks in the 21st century
- Form partnerships with academia and industry that will keep the United States at the cutting edge of information and communications technologies
- Enable the introduction of new networking services that will benefit businesses, schools, and homes.[83]

Government agencies participating in the NGI initiative include the Defense Advanced Research Projects Agency (DARPA), the National Institute of Standards and Technology (NIST), and the National Science Foundation (NSF).

[80] The NGI initiative assessment provided by Grant Miller of the National Coordination Office for Computing, Information, and Communications (NCOCIC) to the NSTAC Network Group on July 14, 1998.
[81] http://www.techweb.com/wire/news/aug/0825sequel2.html.
[82] White House Press Release, October 28, 1998.
[83] http://www.ngi.gov/overview/fast_facts.html

5.4.1 NGI Goals

The NGI initiative has 3 goals that comprise the foundation of the program:

- Conduct R&D in advanced end-to-end networking technologies
- Establish and operate two testbeds
- Conduct R&D in revolutionary applications.

The first, and overarching, goal is to promote experimentation with the next generation of network technologies. This effort will be accomplished by conducting R&D in advanced end-to-end networking technologies focusing on the following:

- Reliability
- Robustness
- Security
- Quality of service/differentiation of service (including multicast and video)
- Network management (including allocation and sharing of bandwidth).[84]

These issues are of great importance to the NS/EP community. As discussed in the Internet2 section, reliability of the future Internet and IP networks is essential to facilitate increased use of the technologies within the NS/EP community. Differentiation of service and network management capabilities may also enable PSN-based NS/EP services such as GETS, to be applied to the NGI. This will be discussed further in Section 6.0.

The second goal of the NGI initiative is to develop next generation network testbeds to connect universities and Federal research institutions at high-speed data transmission rates sufficient to demonstrate new technologies and support future research. The mission will consist of establishing and maintaining two testbeds, called the "100x" and "1000x." The "100x" testbed will connect at least 100 sites, including universities, federal research institutions, and other research partners, at speeds 100 times faster end-to-end than today's Internet. The testbed will be built on Federal networks including NSF's very high performance Backbone Network Service (vBNS) and DOD's Defense Research and Education Network (DREN).[85] The "1000x" testbed will connect about 10 sites with end-to-end performance at least 1,000 times faster than today's Internet. The Federal networks on which this testbed will be built include the multiagency Washington, DC, area Advanced Technology Demonstration network (ATDnet) and DARPA's Advanced Communication Technology Satellite (ACTS) ATM Internetwork (AAI).[86]

The third goal of the NGI is to demonstrate new applications that meet important national goals and missions. These applications will demonstrate the value of advanced networking and test

[84] http://www.ngi.gov/overview/about.html
[85] *Idid.*
[86] *Ibid.*

advanced networking services and technologies. The key objective is to conduct R&D in applications that include the following:

- Collaboration technologies
- Digital libraries
- Distributed computing
- Privacy and security
- Remote operation and simulation.[87]

The NGI initiative should further the state-of-the-art associated with Internet technology, strengthen U.S. technological leadership, and potentially provide significant economic benefits. Additionally, the NGI is being designed for transition to the private sector so that maximum operational benefits can be achieved.

5.4.2 NGI Architecture

To support large-scale development of advanced applications, the NGI testbeds must provide a stable environment, on which developers can build, and offer a flexible network that can be modified and tested frequently. These objectives should be met by the proposed NGI network fabric, which includes expanding and interconnecting existing Federal research networks into a large "leading edge but stable" network of networks for about 100 Federal research sites and national laboratories.[88] It will be a logically separate but physically connected network that can be configured at will to form "virtual networks" to test specific technologies and projects.[89] In essence, NGI will initially be a distributed laboratory consisting of ultra high-speed switching and transmission technologies that enable end-to-end network connectivity from 100 Megabits per second to more than 1 Gbps.[90] This demonstration network fabric will be large enough to provide full system, proof-of-concept testbeds for hardware, software, protocols, and network management that will eventually be migrated to the commercial Internet.[91] The actual network architecture of the commercial NGI will be determined by these NGI R&D testbeds.

5.4.3 NGI and NS/EP

Much like the original Internet, which began as a funded Government project, NGI will also grow into a commercial enterprise that is available to the public. Federal, State, and local organizations may determine that the technologies and applications developed as a result of this

[87] *Ibid.*
[88] Next Generation Internet Initiative Draft Implementation Plan, http://www.ccic.gov/ngi/implementation-Jul97/g2_hp_conn.html, July 1997.
[89] *Ibid.*
[90] NGI Initiative Concept Paper, http://www.ccic.gov/ngi/concept-Jul97/action_2.html, July 1997.
[91] Next Generation Internet Initiative Draft Implementation Plan, http://www.ccic.gov/ngi/implementation-Jul97/g2_hp_conn.html, July 1997.

initiative (and Internet2) could enhance their ability to perform their NS/EP functions. Therefore, the NS/EP community should participate in the development of the NGI. By taking part in policy, architecture, R&D, and protocol discussions related to the NGI, the NS/EP community can help ensure the NGI is suitable for NS/EP operations and services. In particular, such issues as priority service, security, and reliability should be examined. Because the NGI represents, in part, the future of telecommunications, the NS/EP community must consider how it can support mission critical operations in the future.

5.5 Internet Protocol Version 6

IPv6 is the next generation Internet Protocol. It is currently undergoing standardization within the Internet Engineering Task Force (IETF) to succeed the current version, IPv4. IPv6 is designed to operate in high performance networks (e.g., Gigabit Ethernet, ATM) as well as lower bandwidth networks (e.g., wireless).[92] The specifications for the core components of IPv6 have been issued as proposed standards by the IETF, and all major vendors (host and router) are developing and testing IPv6 implementations. IPv6 promises the following protocol enhancements:

- **Expanded Addressing Capabilities.** IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. A new type of address, called an "anycast address," is defined, which is used to send a packet to any one of a group of nodes.

- **Header Format Simplification.** To provide more efficient packet handling and reduce the bandwidth cost of the IPv6 header, some IPv4 header fields have been dropped or moved to optional extension headers.

- **Improved Support for Extensions and Options.** Changes in the way IP header options are encoded allow for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

- **QoS Capability.** A new capability is added to label packets belonging to particular traffic "flows" for which the sender requests special handing, such as non-default quality of service or "real-time" service.

- **Authentication and Privacy Capabilities**. IPv6 defines extensions to support authentication, data integrity, and (optional) data confidentiality.[93]

[92] http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html#CH1
[93] http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html#CH1

The IPv6 standards also outline transition capabilities, which allow users to protect their investment in networking applications written to IPv4 specifications. The most important of these capabilities is the ability to encapsulate IPv6 addresses within IPv4 addresses so that they can still be transported by software and hardware (particularly routers), which are based on 32-bit architectures.

Support for IPv6 in commercial products (e.g., routers and hosts) is gradually becoming available. Commercial IPv6 implementations are now mature enough to support an experimental IPv6 service offering on the vBNS. In its initial offering, the vBNS intends to deploy native, rather than tunneled, IPv6 on the vBNS backbone.[94]

5.5.1 IPv6 and NS/EP

When IPv6 is implemented throughout the Internet, it should provide significant performance and security enhancements (to include IPSec as outlined in Section 2.5.1), that should improve the overall usefulness of the Internet to consumers, industry, and Government. Additionally, IPv6 will enable a priority designation to be applied to traffic sent from a particular end-user location. This and other QoS offerings such as nondefault and real-time services may prove useful to the NS/EP community. These features could encourage broadband use of the Internet, such as using real-time voice and video applications to support emergency response activities. However, IPv6 capabilities are available to all network users and do not facilitate end-to-end priority treatment for NS/EP applications in IP networks similar to Government Emergency Telecommunications Service (GETS). The lack of this capability may discourage more extensive use of public IP networks, including the Internet, within the NS/EP community.

5.6 Convergence of PSN and IP Functionality

The migration of voice traffic from conventional circuit-switched networks to packet-switched networks has begun in earnest. "We're rapidly migrating from being a voice network that also carries data into a data network that also carries voice," as stated by a Bell Atlantic Corporation chief executive.[95] This convergence is of particular importance to the NS/EP community. Current NS/EP services such as GETS and Telecommunications Service Priority (TSP) are based on the PSN architecture. Also, emergency response activities by the Federal Emergency Management Agency (FEMA) and state and local emergency management agencies are based, in large part, on use of the PSN. A large-scale shift in network structure from circuit-switched to packet-switched through IP could have a wide-ranging impact on the NS/EP community. Therefore, it is important for the NS/EP community to understand how and when this convergence may take place in order to effectively prepare for the changes that lie ahead.

[94] Four IPv6 capable routers are being installed on the vBNS in Hayward, CA, Downer's Grove, IL, Perryman, MD, and Reston, VA (http://www.vbns.net/IPv6/IPv6overview.html).
[95] Bell Atlantic Corporation chief executive Ivan Seidenberg at the Supercomm '98 trade show.

As the Internet evolves, PSN and IP networks will converge, and eventually more applications will likely run primarily over IP networks. The IP revolution is not merely about VoIP networks; rather, it is about how a wide variety of applications, including voice and video, will be transported efficiently and seamlessly over these networks. The impetus for the migration to IP networks is the direct result of much of the intelligence in the IP environment being positioned outside of the network and into devices, such as personal computers, servers, and digital set-top boxes. Innovation in the applications arena takes place on the periphery and is no longer dependent upon the more deliberate, centralized processes of the traditional telecommunications industry. This innovation, combined with the efficiency of developing and maintaining IP networks and the widespread use of the Internet, is generating more IP-based traffic.

In fact, the dramatic growth of IP traffic on telecommunications networks foreshadows the coming PSN-IP convergence. The volume of IP traffic is now growing so rapidly on global networks that IP traffic is likely to surpass circuit-switched traffic in volume within the next 5 years.[96] IP traffic through the major U.S. Internet access points has increased at a steady 7 percent monthly rate throughout most of the decade compared to a growth rate of 5 percent or less per year on most circuit-switched networks.[97] Additionally, although only two-tenths of 1 percent of domestic voice traffic was carried over IP networks in 1998, some analysts predict that this may increase to 18 percent by 2002.[98]

The proliferation of IP telephony gateway servers further illustrates the growing convergence of PSN and IP networks. These gateways are emerging as the main interface between the Internet and the PSN and are facilitating the introduction of VoIP. The gateway servers are equipped with voice-processing cards and enable users to communicate via standard telephones. A number of manufacturers are introducing new products to support and capitalize on this burgeoning product market segment.

Lastly, PSN-IP network convergence is driving a significant change to existing architectures. This is already evident across several aspects of traditional telecommunications networks. Carriers are using the latest fiber optic technologies to expand long-haul capacity. The local loop provides a different set of challenges. Many circuit-switched carriers have been forced to upgrade central office equipment to meet the increased demands caused by dial-up Internet access customers. These upgrades can help to support more broadband applications, which will be encouraged by IP networks.

There are, however, issues that work against the efficient convergence of the PSN and IP networks. For instance, new entrants into the telecommunications services industry must define and implement quality-of-service guarantees on IP networks to effectively enable transfer of

[96] Global Telecoms Business, http://www.globaltelecomsbusiness.com/clfiles/gemini, July 1998.
[97] *Ibid.*
[98] "SS7-Stepping Stone to the Future," *Internet Telephony*, September 1998, p. 70.

traffic from the PSN. Customer care and billing will also be a major issue for IP networks. Some industry analysts believe that IP network carriers will adopt metered billing, much like the incumbent telecommunications companies. Others believe billing systems are far too complex and expensive to maintain and point out that today's flat-rate Internet structure has many advantages. In any event, these capabilities are linked with the ability of ISPs and IP carriers to interconnect with the intelligent network of the PSN.

5.6.1 Signaling System 7 Network and IP Networks

The PSN's Signaling System 7 (SS7) technology offers service providers an intelligent network (IN) structure to deliver enhanced services, including NS/EP services such as 911 calls, GETS alternate carrier routing (ACR), and Federal Telecommunications Service (FTS) 2000 calling card features. This IN capability has no counterpart on the Internet. Both the telecommunications and Internet industries share the need to link the SS7 network to the Internet's system of addresses in order to offer services over both networks.[99] To this end, two groups have initiated standards research to facilitate the transfer of traffic between the networks. The IETF has begun work on a standard specification called the "Internet protocol device control," which will provide a common method of passing information between IP and telephony networks.[100] Additionally, the Internet Intelligent Network, a consortium of information technology companies, is outlining the architecture to support next-generation services. The first phase of this initiative is to design a gateway interface that will allow remote access servers from different vendors to communicate using SS7; and the second phase will be to create a signal control point capable of routing calls over IP and telephony networks.[101] These initiatives highlight the importance of building on existing capabilities of the PSN to offer new services with IP telephony. By interfacing with the PSN and the SS7 network, IP carriers can construct IP telephony access devices, which offer features such as fast call set-up times, one-stage dialing, and the use of legacy billing and settlement services.[102]

The convergence of these two networks via the IN will not be a quick and easy process. It has taken traditional telephone companies more than 10 years and billions of dollars to install the infrastructure needed to support IN services. In this regard the Internet infrastructure lags far behind the PSN. However, IP services, especially IP telephony, are attracting investors and a growing number of users. This investment wave provides impetus for hardware and software vendors to work diligently to resolve convergence issues for IP and telephony carriers. Subsequently, as carriers begin offering enhanced services over IP networks and as VoIP matures, many agencies and organizations will investigate the use of these applications. With this in mind, it will be important for the NS/EP community to monitor the accelerating pace of convergence of IP and telephony networks for potential impacts on NS/EP services and

[99] "Advance to Go," *tele.com*, November 1998, p. 64.
[100] *Ibid.*
[101] *Ibid.*
[102] "SS7-Stepping Stone to the Future," *Internet Telephony*, September 1998, p. 71.

operations. The process of linking ISPs with the SS7 network also requires monitoring for potential affects on the security and reliability of the PSN. This process is essential because the PSN is currently an integral component of NS/EP operations and will be for the immediate future.

5.7 Scaling Issues

The ability of the Internet and dedicated IP networks to effectively scale to meet user demands is a major concern as these networks continue to undergo dramatic and unparalleled growth. As the next millennium approaches, the Internet and dedicated IP networks will be increasingly relied on to support business operations, electronic commerce (EC), and other consumer needs.

Network equipment providers are keenly aware of the importance of designing networking equipment to support network growth without reconfiguring or replacing major equipment components. The suppliers who address scalability in an effective and economical manner will be better positioned to exploit marketplace opportunities. Scalability of equipment is one of the prime evaluation factors that network designers use to determine the optimum choice for a particular product application. In addition, network backbone service providers fully understand the importance of being able to provide increased bandwidth capacity when needed to support user demands. As Asynchronous Transfer Mode (ATM) and Synchronous Optical Network (SONET) backbones are implemented throughout the Internet and dedicated IP networks, the ability of IP networks to scale in support of increased user demands and bandwidth-intensive multimedia applications will be enhanced greatly.

The Internet R&D initiatives (Internet2 and NGI) are anticipated to significantly advance current Internet technology. One of the main developmental areas of these Internet initiatives is the scalability of networking elements to provide incremental bandwidth on a cost-effective and high performance, high reliability basis. Robust scalability in networking components and networks is essential, if the Internet and IP networks are to achieve their short- and long-term cost and performance goals. Scalability of IP networks is also of interest to the NS/EP community. As mission-critical dependence on IP networks increases, especially for broadband applications such as real-time voice and video, it will be imperative to maintain reliability and security of these networks. Therefore, it is important for the NS/EP community to participate in Internet R&D initiatives to ensure that evolving IP technologies can support NS/EP services and operations.

5.8 Summary

These Internet initiatives, technologies, and industry trends will have an important affect on the NS/EP community's future dependence on the Internet. To date, the NS/EP community has limited its use of the Internet to nonmission critical activities. Increased dependence is ultimately dependent on the successful implementation of emerging standards, broadband technologies, and intelligent network capabilities. As the Internet's reliability, availability, and

quality of service capabilities increase, the NS/EP community will be more likely to migrate portions of their mission-critical operations to the Internet and take advantage of operational and cost efficiencies. Additionally, as the concept of the Internet changes (e.g., NGI) and as IP networks become more prevalent, the NS/EP community may eventually have no choice but to use these networks for mission-critical operations. Therefore, it is essential for the NS/EP community to consider NS/EP operations, services, and procedures within the context of PSN-IP network convergence. The NS/EP community should be involved in the planning processes affecting network convergence to ensure that NS/EP is considered. Such participation may serve to ensure the continued effectiveness of the NS/EP community, and the ability of each agency and organization to fulfill its NS/EP mission and responsibilities in the fluid public network environment.

6.0 NS/EP IMPLICATIONS

Although the NS/EP community's dependence on TCP/IP networks, both dedicated and the public Internet, continues to grow, today's dependence is generally limited to dedicated TCP/IP networks. The NS/EP community uses the public Internet primarily for routine functions such as e-mail and information sharing applications. The NS/EP community may also depend on the public Internet indirectly because its private sector trading partners use the public Internet to conduct their normal business operations. For example, if the public Internet were unavailable or severely impaired, some private sector trading partners might be unable to respond fully and immediately to NS/EP crisis situations. Further, as Government users become more familiar with the capabilities of the public Internet, they may begin to consider using it directly to support NS/EP operations. Consequently, it is important to explore the implications of using the Internet to support NS/EP operations.

6.1 Dedicated TCP/IP Networks

A dedicated TCP/IP network is used only by specified entities, as opposed to the public Internet that can be used by all. Many federal departments and agencies depend to some degree on dedicated TCP/IP networks, and it is likely that dependence on such networks will continue to grow. DOD runs and relies on two of the largest dedicated TCP/IP networks: NIPRNET (Nonclassified (but sensitive) Internet protocol Routing NETwork] and SIPRNET [Secret Internet Protocol Routing NETwork]. The architecture of these networks mirrors that of the public Internet and uses the same general types of components (e.g., root servers and routers). Product and design vulnerabilities inherent in the public Internet can also affect dedicated networks, albeit on a smaller scale. Therefore, it is important for the NS/EP community to understand potential vulnerabilities in these networks and to take technical and procedural measures to mitigate them to assure continued operations.

6.2 Public Internet

Unlike dedicated TCP/IP networks that facilitate restricted access to authorized users, the public Internet has virtually no access restrictions—almost *anyone* can use it, almost *anytime,* from almost *anywhere*. In addition, the public Internet is physically, architecturally, and technologically diverse. This diversity translates into robustness—aside from the DNS, the Internet does not have a single point of failure or a sole vulnerability that could be exploited to disrupt the entire Internet. The Internet's robustness and ubiquitous accessibility have enticed the NS/EP community and the private sector to use it for routine business operations. However, the Internet's diversity makes it difficult to control and protect, and its accessibility can be exploited for malicious objectives. To the extent that the NS/EP community uses the public Internet, either directly or indirectly, those operations could be affected by Internet vulnerabilities. Therefore, it is important to examine whether these vulnerabilities could have

direct or indirect implications for NS/EP operations before proposing any future dependence on the public Internet.

6.2.1 Direct Implications

NS/EP communications require a high degree of reliability and security for its mission-critical systems. Because the public Internet does not currently offer the level of reliability and security required for NS/EP communications, it is not used to support critical systems and NS/EP operations. For instance, FEMA does not use the Internet to support its emergency communications requirements. The Internet does not meet FEMA's requirements for availability, security, and robustness. Government use is limited to routine functions such as e-mail and Web pages to provide general information to other departments and agencies and to the public at large. At present, important direct NS/EP use of the public Internet is most likely limited to those occasions during which these routine functions are used during times of crisis or emergency. For example, FEMA's Internet home page provides all-hazard disaster preparedness, mitigation, and recovery information. FEMA's home page is not used for emergency operations, but it does provide the status of weather warnings, storms, and seismic events and information regarding such topics as preparing for emergencies such as hurricanes and floods. Although this is not the *only* source of such information, it is certainly a useful source to which citizens can turn for updates on the status of disasters and guidance on emergency preparedness. In the future, as the general population becomes increasingly "Internet-inclined," this may become the preferred source for such information.

Information gathered for this report suggests that a severe disruption of Internet service would not directly affect the mission-critical operations of the NS/EP community because the Internet does not currently support such operations. However, because some implementations of dedicated TCP/IP networks rely on the public Internet for their functionality such as transport and connectivity, there is a potential that such dedicated networks could be affected by service disruptions in the public Internet.

6.2.1.1 Capabilities Comparison

For NS/EP dependence on the Internet to increase, the Internet must provide the levels of reliability, availability, and confidentiality required to support NS/EP operations. Additionally, comparable PSN NS/EP services must also be available. Such services include Government Emergency Telecommunications Service (GETS) and Telecommunications Service Priority (TSP).

GETS provides for the priority access and enhanced routing of NS/EP telephone calls in response to an NS/EP event. GETS traffic receives priority treatment over normal PSN traffic through:

- Controls such as trunk queuing, trunk subgrouping, or trunk reservation

- Exemption from restrictive network management controls that are used to reduce network congestion

- High Probability of Completion Standard (American National Standards Institute [ANSI] T1.631-1993) application to provide NS/EP identification and priority signaling.[103]

GETS also offers alternate carrier routing (ACR), which enables the transfer of GETS traffic from one carrier to another in the event of a network outage.

The TSP System is the regulatory, administrative, and operational framework for the priority provisioning and restoration of any qualified NS/EP telecommunications service. Under the rule of the TSP System, service vendors are authorized and required to provision and restore services with TSP assignments before services without such assignments. The TSP System is used for provisioning or restoration of telecommunications services supporting the following NS/EP missions:

- National Security Leadership
- National Economic Posture and U.S. Population Warning
- Public Health, Safety, and Maintenance of Law and Order
- Public Welfare and Maintenance of National Economic Posture.

Table 4 provides a comparison of the PSN and the current and future Internet in relation to the various NS/EP-related attributes and services.

[103] http://www.ncs.gov/nc-pp/html/new-gets.htm

Table 4
PSN-Internet Capabilities Comparison

	Overall Network Reliability	Overall Network Availability	Priority Restoration	Priority Access/ Transport	Priority Services Reliability	Priority Services Availability	Emergency Response And Coordination
PSN	• Mature reliability • Stable • High tolerance for traffic surge • AIN	• Historically high availability	• TSP	• GETS • GETS ACR • High Probability of Call Completion	• TSP/GETS services *historically* reliable	• TSP/GETS available to all *qualified NS/EP* users	• SHARES • ACN • NTCN • NCC
Current Internet	• Resilient, but not stable • Not designed for high traffic surge • Infrastructure weaknesses (root servers, routers, DNS) • Lack of intelligent network capabilities	• Availability dependent on individual ISPs • Quality of service contracts	• TSP does not apply directly to ISPs • TSP restoration applies to local loop lines owned by telecom carriers and used for access to ISPs	• Access: No method of priority access currently exists • Transport: No method of priority transport currently exits	NA	NA	No proposed applications or services.
Future Internet	• Internet2/NGI is being designed to provide high bandwidth, reliable connections via a high speed backbone (vBNS) and gigaPOPs (points of presence)	• Availability dependent on individual ISPs and telecom carriers • Quality of service contracts	• TSP cannot be used in virtual networks • Reserva-tion Protocol (RSVP) creates virtual circuits	• Access: No proposed method of priority access envisioned • Transport: IPv6 protocol enables priority transport of information from a single end-user location	• IPv6 is a proposed service	• IPv6 will be available to *all* users	No proposed applications or services.

As illustrated in Table 4, today's Internet does not offer the stability, reliability, and availability required to support mission-critical operations for the NS/EP community. Additionally, NS/EP priority services comparable to those available via the PSN are not currently available via the Internet. Because ISPs are considered enhanced service providers, they have not been subject to regulation by the Federal Communications Commission. ISPs are not required to offer TSP services because they are not considered common carriers. (However, if incumbent carriers provide the underlying infrastructure for access to ISPs [e.g., local loop lines], this infrastructure qualifies for TSP restoration.) Also, emergency priority services, similar to GETS, are not available via the extant Internet. If organizations have a dial-up connection to the Internet, they may be subject to congestion on the PSN or at the ISP. Additionally, no method of priority access is being proposed for the future Internet. IPv6, when implemented, will offer priority designation of traffic from a single location and will be available to all Internet users, not just NS/EP users.

6.2.1.2 Market Factors

No economic incentives currently exist for ISPs or IP carriers to offer end-to-end NS/EP priority services over their networks. As previously stated, these carriers are not regulated and cannot be mandated to offer such services. ISPs are offering in-network quality of service contracts for customers, which guarantee certain levels of service. These service guarantees typically focus on intranet services, such as intranet availability guarantees. ISPs cannot guarantee performance levels for the Internet because of its interconnected structure. However, competition among ISPs and IP carriers may generate increased levels of reliability, availability, and confidentiality in their respective networks, and subsequently the Internet, especially as technology and protocol improvements are introduced. Such improvements are necessary to encourage growth of EC, VoIP, and other broadband uses of the Internet among the business community. Whether such improvements will also encourage carriers to offer NS/EP services is unclear. As IP networks proliferate and handle more voice traffic, the FCC may subject ISPs and IP carriers to certain regulations. If this occurs, a legal requirement for these entities to provide certain NS/EP services may be considered.

In summary, there are currently no end-to-end NS/EP services available via the Internet and none are proposed for the immediate future. The PSN architecture includes advanced intelligent network technologies, which are essential to providing end-to-end NS/EP services. Today's Internet does not have comparable technologies, and current Internet protocols themselves cannot support end-to-end NS/EP services. In the future, it is likely that more organizations will depend on IP carriers for voice and other broadband services, and IP carriers will interconnect with the PSN intelligent network. Therefore, it may become increasingly necessary for comparable NS/EP services to be made available via IP networks and the Internet. Unless this occurs, and the future Internet achieves the reliability and availability of the PSN, it is unlikely that the NS/EP community will increase its dependence on the public Internet.

6.2.2 Indirect NS/EP Implications

The extent to which NS/EP operations currently depend on the public Internet indirectly is unknown, but is assumed to be increasing. Because of the Government's desire to improve efficiency by increasing the use of paper-free systems and processes (as indicated in the Defense Reform Initiative, for instance), electronic commerce (EC) between the NS/EP community and its private sector trading partners will continue to increase. Some of these trading partners may depend on the Internet for their basic business operations; if the Internet were severely degraded or unavailable, their ability to support the NS/EP community in times of stress *could* be impaired. The NS/EP community should definitively determine the extent of its indirect dependence on the Internet to ascertain if any NS/EP mission-critical operations could be affected by a severe disruption of Internet service.

6.2.2.1 Other Critical Infrastructure Implications

Based on information gathered for this report, other critical infrastructures such as the telecommunications, electric and gas industries do not currently depend on the Internet for mission-critical operations. Therefore, a severe disruption of Internet service should not currently affect NS/EP operations that depend on these infrastructures.

However, it is clear that market conditions and technology related factors are making the Internet more desirable for transport and connectivity. Further, indications are that some infrastructures are considering changes in their business practices that will make them more dependent on the Internet. For example, some software vendors are considering using the Internet to distribute software patches. An Internet failure could impede implementation of these patches and subsequently affect the infrastructure. Therefore, it remains important to continue monitoring the extent of infrastructure dependence on the Internet. If other critical infrastructures begin to depend on the Internet for mission-critical operations, severe Internet disruptions could significantly impact NS/EP operations.

7.0 CONCLUSIONS AND RECOMMENDATIONS

7.1 Conclusions

The intent of this effort was to accomplish the following tasks:

- Task 1: Examine the extent to which NS/EP operations will depend on the Internet over the next 3 years
- Task 2: Identify vulnerabilities of network control elements associated with the Internet and their ability to cause a severe disruption of Internet service, applying lessons learned from NSTAC's similar studies of the Public Switched Network (PSN)
- Task 3: Examine how Internet reliability, availability, and service priority issues apply to NS/EP operations.

The conclusions derived from each task are presented below.

7.1.1 Task 1: Examine the Extent to Which NS/EP Operations Will Depend on the Internet over the Next 3 Years

The NS/EP community's direct dependence on the public Internet for mission-critical operations is currently modest. Agencies with NS/EP responsibilities are using public Internet sites mostly for outreach, information sharing, and e-mail. Currently, the NS/EP community is more dependent on dedicated TCP/IP networks (also called intranets) for mission-critical NS/EP operations. Dedicated TCP/IP networks offer more security than the public Internet as more network elements are directly controlled by the operating organization. Additionally, operating organizations can implement specific security policies related to their networks and can restrict access to authorized users.

Because of the interconnected nature of the public Internet, however, a disruption or degradation of Internet operations could also affect the operations of dedicated TCP/IP networks/intranets. Although organizations maintain control over more network elements in intranets, any dependence on the public Internet for functionality could affect intranet availability, reliability, integrity, and user confidentiality. For instance, an organization can rely on the public Internet for connectivity between its intranet nodes. Virtual private networks (VPN) specifically rely on this architecture. Additionally, end users may depend on the Internet for remote access to an intranet. Therefore, unless multiple connections exist or alternative means of connecting to an intranet are available, an Internet failure could affect intranet supported capabilities.

The complexity of data networks increases the potential for a public Internet failure to affect NS/EP operations. Further, in some cases, organizations do not fully understand their individual intranet topologies (including connections to the public Internet) and consequently fail to take measures that could help protect their intranets from problems affecting the public Internet. Therefore, it is essential that the NS/EP community thoroughly comprehends the architecture and security capabilities of its mission-critical networks. It may be difficult, if not impossible, to completely protect mission-critical dedicated networks against consequences of exterior network failures or attacks via the connecting public Internet. However, if the NS/EP community understands the potential vulnerabilities of TCP/IP networks, including the public Internet, and keeps abreast of individual network architectures and connections, potential vulnerabilities can be identified and solutions implemented. This becomes increasingly relevant as agencies come to depend more on TCP/IP-based networks, especially the public Internet.

NS/EP dependence on the Internet is likely to grow steadily over the next several years for many reasons:

- The public Internet offers a cost-effective and efficient means of communication.
- Government and industry are rapidly moving toward a paperless, digital society.
- Most Federal departments and agencies now use or have a presence on the public Internet and are promoting its increased use. Some agencies already depend on Internet applications, including remote access and secure Web sites, which if impaired, could affect administrative and coordinating capabilities in support of NS/EP operations.
- Several promising technology enhancements (e.g.,VPNs, Internet Protocol Version [IPv6], Internet Protocol Security [IPSec], and Quality of Service [QoS]) may offer capabilities that could support NS/EP services over the Internet.
- The Next Generation Internet (NGI) and Internet2 initiatives are expected to provide significant enhancements in terms of Internet performance, advanced application support, reliability, and security.

Additionally, critical infrastructures, including medical services, banking and finance, gas and electric industries, and telecommunications, are increasingly using the Internet for various processes, including exchange of business, administrative and research information. Much like the NS/EP community, these infrastructures currently view the Internet as too unreliable and insecure to embrace as a primary means of executing mission-critical activities. However, for the same reasons listed above, this dependence can be expected to increase in the future.

A related issue that merits further analysis is the convergence of IP and PSN networks. This trend may generate additional dependence on IP-based networks in the NS/EP community. As new and existing carriers implement IP-based networks and as incumbent carriers' networks interface and converge with IP networks, the NS/EP community must consider the reliability, availability, and confidentiality implications of NS/EP capabilities in the evolving public network architecture. It would be appropriate for existing joint industry/Government mechanisms to examine these issues. Specifically, by authority of Executive Order 12472, the National Communications System (NCS) is required to ensure that a national telecommunications infrastructure is developed which is responsive to the NS/EP needs of the NS/EP community. Furthermore, Executive Order 12382 – *President's National Security Telecommunications Advisory Committee* – established NSTAC to advise the President on issues affecting NS/EP telecommunications capabilities. Based on the existing responsibilities of the NCS and NSTAC, it would be beneficial for these industry/Government coordinating bodies to ensure NS/EP needs are fulfilled.

7.1.2 Task 2: Identify Vulnerabilities of Network Control Elements Associated with the Internet and their Ability to Cause a Severe Disruption of Internet Service

The Internet is a conglomeration of interexchange points (IXP) and national, regional, and local Internet service providers (ISP) serving end users and organizations. Each level/tier has distinct characteristics, and many providers operate in two or more tiers. In addition, the infrastructure is a mix of hierarchical (local service provider to regional service provider) and flat associations. With this highly diverse architecture and complex interconnection arrangements, consisting of thousands of ISPs using equipment from a variety of vendors, it is unlikely that a major Internet service disruption would be caused by the failure of any single node or transmission facility.

However, several aspects of the management of the Internet and its technology invite potential vulnerabilities: the distributed, informal nature of Internet management, the domain name system (DNS), critical Internet control software and systems, and procedural errors. These vulnerabilities are further discussed below.

Management

Numerous organizations participate in administering Internet operations, including the Internet Assigned Number Authority (IANA), the National Science Foundation (NSF) and its contractor Network Solutions, Inc. (NSI), and the Internet Society. Because current management of critical Internet functions, including oversight of the DNS and root servers, is administered by organizations in a distributed, informal manner, there is a lack of formal guidance, policy, procedure, and accountability related to these functions.

However, with the formation of the Internet Corporation of Assigned Names and Numbers (ICANN), changes to this system are in progress. ICANN will become responsible for many of

the Internet functions now performed under U.S. Government contract by IANA and other entities. These functions include IP address space allocation, protocol parameter assignment, DNS management, and root server system management functions. As it evolves, it is essential that ICANN establishes policies related to the security of these functions, including DNS security, to enhance Internet reliability. Although it is not possible to determine how these general aspects of a distributed management structure may lead to specific vulnerabilities, the current lack of definitive policy, control, and best practices on security together with the uncertainty regarding how the Internet will ultimately be managed, are of concern. The problem is further exacerbated by the overall lack of awareness of NS/EP services, capabilities, and requirements among the entities that provide oversight for Internet management. Therefore, the NS/EP community should increase NS/EP awareness among the various Internet management organizations and proceed cautiously on the use of and dependence on the Internet. Note that the Office of the Manager, NCS (OMNCS), and various NSTAC companies participate in several Internet organizations. Additionally, the OMNCS serves as chair of the Federal Telecommunications Standards Committee. These existing relationships and mechanisms can be leveraged to provide mediums through which OMNCS and NSTAC can work to increase awareness of NS/EP related needs within the Internet community.

Domain Name System

A critical element of the Internet is the DNS, which is composed of 13 root servers (referred to as root servers "A" through "M") and software that manages the translation of domain names to IP addresses to connect users to Internet locations. The main root server ("A") contains all the top and secondary level domain names, and promulgates new domain names to the other 12 root servers. The data housed on the "A" server is also replicated on the other 12 root servers throughout the Unites States and abroad. DNS failures could affect Internet availability and functionality. For instance, if the "A" server experiences a sustained outage (24 hours or more) or propagates incorrect information (incorrect domain names), Internet operations might be severely impaired. Although the Internet could continue to function if one or more of the 12 redundant individual root servers ("B" through "M") were out of service for a short period of time, a sustained outage of several of the root servers could affect traffic flow and potentially affect user connectivity. More importantly, malicious tampering with the DNS (e.g., cache poisoning, malicious corruption of the servers) could severely impair Internet functionality.

In addition, the root server system is voluntarily administered by various organizations worldwide. The volunteer nature of this oversight, together with the absence of security policies and best practices, raises concern for the system's security. Although the root server system has not experienced any prolonged outages or known significant attacks, the lack of coordinated standards for security and administration of the servers is a concern.

Software

Like all networked systems, the Internet relies on software to function as intended. The DNS software, known as Berkeley Internet Name Domain (BIND), is a UNIX software implementation of DNS that runs on the Internet's root servers. BIND eliminates the need for a "host table" that would list all hosts connected to the Internet and their addresses. BIND enables local administrators to assign their own host names and addresses and install them in a local database that automatically distributes them to other systems as needed. Corruption of the local database and its propagation throughout the Internet could severely affect Internet availability and reliability.

As with any software, development and maintenance procedures are critical aspects that can affect BIND security and reliability. The development, testing, and distribution processes of BIND are not as vigorous and structured as those typically employed for software that supports the public switched network (PSN). This raises the concern that a corrupted version of a new release of the BIND software could inadvertently, or maliciously, be distributed to all DNS servers. Disparate implementation of BIND-related security patches among users can further complicate the problem.

Software components of the Internet may also be affected by the Y2K problem. This could occur as a result of individual components malfunctioning because some Y2K problem was overlooked, or because the Y2K remediation efforts of various components might be incompatible.

Procedural Errors

Procedural errors and other unintentional actions can significantly affect Internet operations. Although Internet service outages have not been studied as rigorously as PSN outages, there is some evidence that procedural errors are equally troublesome to the Internet community.

7.1.3 Task 3: Examine How Internet Reliability, Availability, and Service Priority Issues Apply to NS/EP Operations

The NS/EP community is currently dependent on dedicated TCP/IP networks for mission-critical operations. At present, the reliability and availability of the public Internet is considered inadequate for mission-critical functions. These factors have resulted in a lack of demand within the NS/EP community for end-to-end NS/EP-related Internet services to support critical NS/EP operations.

Today, there are no Internet technologies or applications that facilitate the same type of end-to-end NS/EP- related services available in the PSN (i.e., priority access, routing, and transport). Therefore, if organizations have a dial-up connection to the Internet, they may be subject to

congestion on the PSN or at the ISP. Additionally, no method of priority access is being proposed for the future Internet (e.g., level of availability and performance). Additionally, although certain ISPs currently offer in-network quality of service (QoS[104]) standards, there are no end-to-end QoS offerings available via the public Internet. Additionally, end-to-end priority service routing is not yet commercially available for any type of Internet traffic. It is anticipated that if IPv6 is implemented, it will enable all public Internet users to request priority for specific data traffic. However, the concept of priority traffic in relation to NS/EP becomes less relevant if all users can request it. Therefore, for IPv6 to support NS/EP operations, it would have to be further refined to provide a unique end-to-end routing feature for NS/EP traffic. When end-to-end QoS, end-to-end priority routing for NS/EP traffic, and adequate security measures are available for implementation on the Internet, the use of the Internet for mission-critical functions should increase.

Currently, there are no economic incentives for ISPs to develop NS/EP service enhancements for deployment on their networks. Furthermore, ISPs are not regulated and cannot be mandated to offer such services. However, competition among ISPs and IP network (facility-based) carriers may generate increased levels of reliability and availability in their respective networks, and subsequently the public Internet. Such improvements are necessary to encourage growth of electronic commerce (EC), Voice over Internet Protocol (VoIP), and other broadband uses of the Internet. Whether these improvements will encourage carriers to offer NS/EP services is unclear.

In summary, end-to-end NS/EP services cannot currently be offered via the public Internet. A number of factors (e.g., lack of NS/EP demand, market factors, and lack of regulatory mandates) make it unlikely that the same type of NS/EP services available in the PSN will be available over the Internet for the foreseeable future. Therefore, it would benefit the NS/EP community to increase NS/EP awareness in the NGI and Internet2 initiatives, and continue to encourage the initiatives to examine NS/EP priority service features for the next generation of Internet technologies and applications. Additionally, by authority of Executive Order 12472, the NCS is required to ensure that a national telecommunications infrastructure is developed which is capable of satisfying priority telecommunications requirements under all circumstances. Therefore, it would be appropriate for the NCS to ensure consideration of NS/EP priority services among Internet technology vendors, service providers, and standards bodies.

7.2 Recommendations

The following recommendations are proposed to help increase awareness and understanding of Internet dependencies, technologies, and vulnerabilities in the NS/EP community and to encourage NS/EP awareness among Internet organizations and initiatives.

[104] QoS is the ability to define a level of performance in a data communications system (http://www.techweb.com/encyclopedia/defineterm?term=QoS).

7.2.1 NSTAC Recommendations to the President

- Recommend that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, direct the establishment of a permanent program to address NS/EP issues related to the Internet. The program should have the following objectives:

  - Work with the NS/EP community to increase understanding of evolving Internet dependencies by—

    a. Evaluating the extent of their current and future direct and indirect dependence on the public Internet for NS/EP mission-critical operations

    b. Developing a thorough understanding of their physical intranet architectures and connections to the public Internet in order to identify and protect against potential vulnerabilities

    c. Developing plans and programs to implement long-term goals related to NS/EP dependence on the public Internet

    d. Defining Internet security and reliability requirements needed to support NS/EP operations.

    Although current NS/EP community dependence on the public Internet is modest, dependence on TCP/IP intranets is more extensive. As agencies and organizations consider and adopt additional applications that increase their dependence on the Internet and intranets, it will become increasingly important to assess the extent of this dependence and to determine potential consequences resulting from Internet disruptions. The NS/EP community will need to be more aware of the physical topology of individual networks to understand how dependence on the Internet may affect network operations. It is also important that the NS/EP community determine Internet reliability and availability requirements needed to support NS/EP services and operations and subsequently develop plans and programs necessary to implement long-term goals for increased dependence on the Internet. Because Executive Order 12472 provides the NCS with the authority and responsibility for addressing NS/EP telecommunications infrastructure issues, the Office of the Manager, NCS would be the appropriate body to coordinate these activities.

- Work with key Internet organizations and standards bodies to increase awareness of NS/EP requirements by—

  a. Continuing to interact with organizations and initiatives driving Internet administrative, operational, and technical direction, (e.g., Internet Corporation for Assigned Names and Numbers [ICANN], Internet Engineering Task Force [IETF], and the Next Generation Internet [NGI]) to assure consideration of NS/EP needs, services, and operations.

  b. Ensuring that the Federal Telecommunications Standards Committee considers NS/EP requirements for Internet reliability and availability.

  It is essential that organizations assisting with administration of the Internet and those responsible for implementation of Internet standards and technology be made aware of the NS/EP community's needs as related to the Internet. Therefore, it is important that a working relationship with these Internet bodies is fostered to assure consideration of NS/EP needs and services. The Office of the Manager, NCS has working relationships with several Internet-related organizations such as the IETF, and serves as chair of the Federal Telecommunications Standards Committee. Therefore, the OMNCS would be the appropriate body to coordinate these activities.

- Interact with the appropriate Internet organizations and initiatives (e.g., ICANN, IETF, and NGI) to investigate, develop, and employ NS/EP-specific Internet priority services, such as end-to-end priority routing and transport.

  NS/EP priority services, similar to those available via the PSN, may be necessary via the Internet if the NS/EP community's dependence on Internet technology and applications increases. Therefore, regular interaction with Internet organizations and initiatives is necessary to assure that NS/EP needs are considered and that NS/EP Internet priority services are investigated and implemented. The Office of the Manager, NCS, by authority of Executive Order 12472, is the principal advocate for NS/EP services for the PSN (e.g., Government Emergency Telecommunications Service). Therefore, the OMNCS would be the appropriate body to promote the development and implementation of NS/EP-specific Internet priority services.

  - Examine the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services (e.g., Government Emergency Telecommunications Service and Telecommunications Service Priority).

    As new and existing carriers implement IP-based networks, and as IP networks interface with the PSN's SS7 network, it is important to consider reliability and availability of the evolving public network architecture as it relates to NS/EP service capabilities.

- Recommend that the President direct the appropriate Government departments and agencies to make use of existing industry/Government partnership mechanisms to increase awareness of NS/EP requirements within key Internet organizations and standards bodies.

  It is essential that organizations assisting with administration of the Internet and those responsible for implementation of Internet standards and technology be made aware of the NS/EP community's needs as related to the Internet. Therefore, it is important to use existing industry/Government mechanisms such as the NSTAC to complement the Government's activities of fostering a working relationship with Internet bodies to assure consideration of NS/EP needs and services.

7.2.2 NSTAC Direction to the IES

The NSTAC directs the Industry Executive Subcommittee (IES) to examine the potential impact of IP network-PSN convergence on PSN-specific NS/EP priority services (e.g., Government Emergency Telecommunications Service and Telecommunications Service Priority).

As new and existing carriers implement IP-based networks, and as IP networks interface with the PSN's SS7 network, it is important to consider reliability and availability of the evolving public network architecture as it relates to NS/EP service capabilities. Given NSTAC's responsibility for advising the President on NS/EP telecommunications issues, this study would be consistent with NSTAC's established mission.

APPENDIX A

REPORT CONTRIBUTORS

REPORT CONTRIBUTORS

ACTIVE PARTICIPANTS

Nortel Networks	Dr. Jack Edwards, NG Chair
GTE	Mr. Jim Bean, NG Vice-Chair
SAIC	Mr. Hank Kluepfel, NG Vice-Chair
U S WEST	Mr. Jon Lofstedt, NG Vice-Chair
Lockheed Martin	Dr. Chris Feudo, Task Chair
MCI WorldCom	Mr. Don Frick, Task Vice-Chair
AT&T	Mr. Gordy Bendick
Boeing	Mr. Robert Steele
CSC	Mr. Guy Copeland
ITT	Mr. Peter Steensma
NTA	Mr. Bob Burns
Raytheon	Mr. John Grimes
Sprint	Dr. Sushil Munshi
USTA	Dr. Vern Junkmann

OTHER CONTRIBUTORS

Bay Networks	Bob Gaughan
Telcordia Technologies, Inc.	John Lutin
CERT®	Jeff Carpenter
Cisco	Steve Sneddon
	Stephen Wolf
COSPO	Lawrence Carnegie
DOC	Roger Baker
	Paul London
DISA	Tony Montemarano
GSA	Thomas Burke
GTE/BBN	J.F. Mergen
ICSA Labs	Donald Krysakowski
Intelink	Jack Torok
NCOCIC	Kay Howell
	Grant Miller
NSI	Don Telage
	Scott Williamson
OMNCS	Bernie Farrell
	James Kerr
	Art Schoenwetter
MCI WorldCom	Dale Drew
	Charles Lee
Sandia	Bob Hutchinson
	Margie Tatro
UMD	Rodney Peterson
	Karl Reuss
	Don Riley
	Gerry Sneeringer
UUNET	Mike O'Dell

APPENDIX B

REFERENCES

REFERENCES

Magazine/Newspaper/Press Release Articles

"Advance to Go," *tele.com*, November 1998.

"DOD's Hamre Spells Out Web Rules," *Federal Computer Week*, September 28, 1998.

"DOD Reels in Content on Web Sites," *Federal Computer Week*, September 21, 1998.

"DOE Tests Tool to Speed Priority Internet Traffic," *Federal Computer Week*, April 20, 1998.

"Energy Aims Sights on ATM," *Government Computer News*, January 12, 1998.

"Fake Message Sends AOL E-mail Astray," *Washington Post*, October 17, 1998.

"Feds Eye VPN to Lower Remote Access Costs," *Federal Computer Week*, January 19, 1998.

"GSA's Thompson Urges Feds to Use the Internet for EC," *Government Computer News*, June 30, 1997.

GSA News Release, World Wide Web, http://post.fts2k.gsa.gov/cinema/.

"Hurricane Watchers Clog Weather Web Sites," *New York Times* Web Site, http://www.nytimes.com/library/tec…08/cyber/articles/27hurricane.html, August 26, 1998.

"Navy Urges Use of the Net for Most Data Comm," *Government Computer News*, March 16, 1998.

"Net Outage: The Oops Heard 'Round the World," *Wired Magazine*, April 25, 1997.

"New Firewall Products Coming," *InternetWeek*, May 19, 1997.

"SS7-Steeping Stone to the Future," *Internet Telephony*, September 1998.

Statement by the President, White House Press Release, October 28, 1998.

"The Internet," *IEEE Spectrum*, January 1998.

The Economic Costs of Computer Viruses, Scott Magruder and Stanley X. Lewis, Jr., Arkansas Business & Economic Review, 1991.

"The Whole Wired World," *Federal Computer Week*, March 30, 1998.

"U.S. Lawmakers Start Internet Name Probe," *TechWeb*, October 16, 1998.

"Voice Over IP," *Telecommunications*, March 1998.

National Security Telecommunications Advisory Committee (NSTAC) Documents

Financial Services Risk Assessment Report, December 1997.

NSTAC Network Group (NG) Briefings

Open Source Information System, Community Open Source Program Office, December 8, 1998.

Current Interdependencies and Vulnerabilities of the Internet and PSN, James Kerr, OMNCS, February 10, 1998.

DOD Intranets, Tony Montemarano, DISA, May 12, 1998.

Effects of An Internet Intrusion on the PSN, John Lutin, Telcordia Technologies, Inc. (formerly Bellcore), December 3, 1998.

Future Internet Architecture and Governance, Don Telage, NSI, May 12, 1998.

Internet Architecture and Vulnerabilities, Mike O'Dell, UUNET, February 10, 1998.

Internet Security Issues and Service Disruptions, Jeff Carpenter, CERT®, March 10, 1998.

Internet Vulnerabilities That Could Cause Severe Disruption of Internet Service, Scott Williamson, NSI, July 14, 1998.

Issues Associated With Securing the Internet Without Affecting Performance, Bob Hutchinson, Sandia, August 11, 1998.

MCI Security and Protective Measures, Dale Drew, MCI WorldCom, March 10, 1998.

Network Security, J.F. Mergen, GTE/BBN, November 10, 1998.

Next Generation Internet and Internet2, Kay Howell and Grant Miller, National Coordination Office for Computing, Information, and Communications (NCOCIC), July 14, 1998.

Overview of DOC Internet and EC Programs, Roger Baker and Paul London, DOC, October 8, 1998.

Overview of GSA Internet and EC Programs, Thomas Burke, GSA, October 8, 1998.

Overview of IPSec Certification, Donald Krysakowski, ICSA Labs, August 11, 1998.

Overview of NS/EP Reliance on Private and Public TCP/IP Networks, Bernie Farrell, OMNCS, March 18, 1998.

Overview of the Future Internet Including the Internet2 and the NGI, Charles Lee, MCI WorldCom, August 11, 1998.

Overview of the Intelink Program, Jack Torok, Intelink Program Office, July 14, 1998.

Overview of the UMD Root Server Installation and Operation, Rodney Peterson, Karl Reuss, Don Riley, and Gerry Sneeringer, UMD, September 1, 1998.

Router Vulnerabilities, Steve Sneddon, CISCO, April 21, 1998.

The Energy Industry's Current and Potential Future Reliance on the Internet, Margie Tatro, Sandia, August 11, 1998.

VoIP and PSN/IP Convergence, Bob Gaughan, Bay Networks, October 8, 1998.

Office of the Manager, National Communications System (OMNCS) – Sponsored Documents

Assessment of PSN Component's Critical Roles and Interdependencies in Call Processing, September 1997.

Internet/PN Interconnectivity and Vulnerability Report, August 1997.

Other

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations, GAO/AIMD-98-145, May 1998.

Defense Reform Initiative Report, November 1997.

FERC Order No. 889, http://www.ferc.fed.us/news/rules/data/rm95-9-00k.txt.

Management of Internet Names and Addresses, U.S. Department of Commerce, Docket No. 980212036-8146-02.

Network Reliability: The Path Forward, Compendium of papers presented by the Network Reliability Council of the Federal Communications Commission (Performance Metrics Team Final Report), April 1996.

Next Generation Internet Initiative Draft Implementation Plan, http://www.ccic.gov/ngi/implemenmtation-jul97/g2_hp_conn.html, July 1997.

NG*I Initiative Concept Paper,* http://www.ccic.gov/ngi/concept-jul97/action_2.html, July 1997.

Report to the President's Commission on Critical Infrastructure Protection, Carnegie Mellon University/SEI-97-SR-003, CERT® Coordination Center, January 1997.

Security Architecture for IP, Internet Draft, IETF Network Working Group, July 1998.

Trust in Cyberspace, Computer Science and Telecommunications Board, National Resource Council, September 29, 1998.

APPENDIX C

GLOSSARY

GLOSSARY

The list of terms included in this appendix is by no means exhaustive. For additional information on telecommunications/Internet-related terminology, refer to the following online glossaries:

- The Federal Communications Commission Web site glossary http://www.fcc.gov/Consumers/glossary.html
- The Technology Network encyclopedia at http://www.techweb.com/encyclopedia.
- Internet.com's PC Webopeadia at http://webopedia.internet.com.
- http://www.netdictionary.com

Availability

The assurance that a given resource will be usable during a given time period.

Backbone

In the Internet, the part of a network that transports major traffic. It employs the highest speed transmission paths in the network and may also run the longest distance. Smaller networks (ISP networks) are attached to the backbone.

Domain Name

An Internet domain name is an organization's unique name combined with a top-level domain (TLD) name. For example, ncs.gov is the domain name of the NCS.

Domain Name System

Software that enables users to identify the addresses for computers on the Internet by cross-referencing the domain name with the IP address. The domain name system (DNS) server maintains a database of domain names (host names) and their corresponding IP addresses. In this hypothetical example, if www.mycompany.com were presented to a DNS server, the IP

address 204.0.8.51 would be returned. DNS has replaced the manual task of updating HOSTS files (a text file that lists host names and their corresponding IP addresses).[1]

Firewall

A system designed to prevent unauthorized access to or from a private network, which can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.[2]

Internet Protocol

Internet Protocol (IP) specifies the format and the addressing scheme of packets, also called datagrams. Most networks combine IP with a higher level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is similar to the postal system. It permits users to address a package and drop it in the system. Although IP provides the routing mechanism for information, it does not provide a direct link between the sender and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that messages can be sent back and forth for a period of time. The current version of IP is IPv4. A new version, called IPv6 or IPng, is under development.[3] IP works at the Network layer (OSI layer 3).

IP Address (Internet Protocol Address)

The physical address of a computer attached to a TCP/IP network. Every client must have a unique IP address. IP addresses are written as four sets of numbers separated by periods; for example, 202.192.81.1.

Internet Service Provider

An organization that provides access to the Internet. Small Internet Service Providers (ISP) provide service via modem and ISDN whereas larger ones also offer private line hookups (T1, fractional T1, etc.). ISPs have a point of presence (PoP) at LEC facilities

Reliability

The assurance that a given system will perform its mission adequately under expected operating conditions.

[1] http://www.techweb.com/encyclopedia/defineterm?term=DNS
[2] http://webopedia.internet.com/TERM/f/firewall.html

Root Server

A domain name system server. Network Solutions, Inc., Herndon, VA, currently maintains the primary or "A" root server. It contains all the primary domain names that are registered, and it is continuously updated. The data is replicated on several secondary root servers nationwide and abroad.

Router

A device that routes data packets from one local area network (LAN) or wide area network (WAN) to another. Routers see the network as network addresses and all the possible paths between them. They read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at the network layer (OSI layer 3).[4]

Top Level Domain

The highest level domain category in the Internet naming system (e.g., .com, .org, .gov and .net).

Transmission Control Protocol (TCP)

Part of the TCP/IP communications protocol, which is used on the Internet. TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same sequence in which they were sent.[5] TCP works at Transport layer (OSI layer 4).

[3] http://webopedia.internet.com/TERM/I/IP.html
[4] http://www.techweb.com/encyclopedia/defineterm?term=router
[5] http://webopedia.internet.com/TERM/T/TCP.html

APPENDIX D

ACRONYM LIST

ACRONYM LIST

AAI	ACTS ATM Internetwork
ACTS	Advanced Communication Technology Satellite
ACN	Alerting Coordination Network
ACR	Alternate Carrier Routing
ANSI	American National Standards Institute
ANX	Automotive Network Exchange
AOL	America Online
ARPA	Advanced Research Project Agency
ATDNet	Advanced Technology Demonstration Network
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
CERT®	Computer Emergency Response Team
CINEMA	Commerce, Internet and E-mail Access Services
CIO	Chief Information Officer
CLEC	Competitive Local Exchange Carrier
CMU	Carnegie Mellon University
COSPO	Community Open Source Program Office
DARPA	Defense Advanced Research Projects Agency
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNS	Domain Name System
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DREN	Defense Research and Education Network
E-mail	Electronic Mail
EC	Electronic Commerce
EDI	Electronic Data Interchange
ERLink	Emergency Response Link
ESF	Emergency Support Function
FBIS	Foreign Broadcast Information Service
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission

FIX	Federal Internet Exchange
FRP	Federal Response Plan
FTS2000	Federal Telecommunications Service 2000
GAO	Government Accounting Office
Gbps	Gigabit-per-Second
GETS	Government Emergency Telecommunications Service
GigaPoPs	Gigabit Points of Presence
GSA	General Services Administration
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation of Assigned Names and Numbers
IEC	Interexchange Carrier
IES	Industry Executive Subcommittee
IETF	Internet Engineering Task Force
IESG	Internet Engineering Steering Group
ILEC	Incumbent Local Exchange Carrier
IN	Intelligent Network
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Standardization Sector
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IXP	Inter-exchange Point
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LEC	Local Exchange Carrier
LSP	Local Service Provider
MAE	Metropolitan Area Exchange
MILNET	Military Network
NAP	Network Access Point
NASA	National Aeronautics Space Administration
NBP	National Backbone Provider
NCC	National Coordinating Center for Telecommunications

NCOCIC	National Coordination Office for Computing, Information, and Communications
NCS	National Communications System
NG	Network Group
NGI	Next Generation Internet
NIPRNET	Nonclassified [but sensitive] Internet Protocol Routing NETwork
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission; Network Reliability Council
NRIC	Network Reliability and Interoperability Council
NSA	National Security Agency
NS/EP	Network Security and Emergency Preparedness
NSF	National Science Foundation
NSI	Network Solutions, Inc.
NSP	Network Service Provider
NSTAC	National Security Telecommunications Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTCN	National Telecommunications Coordinating Network
OASIS	Open Access Same-time Information System
OMNCS	Office of the Manager, National Communications System
OSIS	Open Source Information System
OPT	Office of Priority Telecommunications
PC	Personal Computer
PN	Public Network
POC	Point of Contact
POP	Point of Presence
PPTP	Point-to-Point Tunneling Protocol
PSN	Public Switched Network
QoS	Quality of Service
RSP	Regional Service Provider
R&D	Research & Development
SEI	Software Engineering Institute
SHARES	SHAred RESources High Frequency Radio Program
SIPRNET	Secret Internet Protocol Routing NETwork
SONET	Synchronous Optical Network
SSL	Secure Socket Layer
SS7	Signaling System 7

TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domain
TS/SCI	Top Secret/Sensitive Compartmented Information
TSP	Telecommunications Service Priority
UCAID	University Corporation for Advanced Internet Development
URL	Uniform Resource Locator
U.S.	United States
vBNS	Very High Performance Backbone Network Service
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WWW	World Wide Web
Y2K	Year 2000