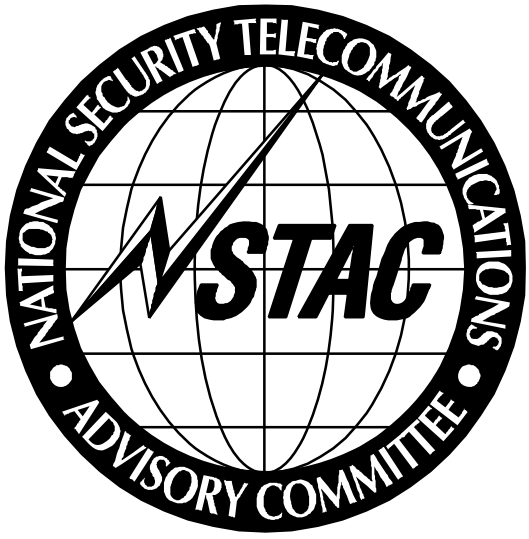
THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE



NETWORK GROUP
WIDESPREAD OUTAGE SUBGROUP
REPORT

Report on the Likelihood of a Widespread Telecommunications Outage

December 1997

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, requested that Mr. Charles Lee, Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), provide NSTAC's forward-looking views on the possibility of a widespread service outage in the public telephone network. The Widespread Outage Subgroup was established in July 1997 to address Dr. Gibbons' letter.

A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would impact the availability and integrity of telecommunications service for at least a significant portion of a business day.

U.S. telecommunications service providers have historically offered robustness, availability and quality unparalleled by other public services. Although the public network (PN) track record is superlative, natural and technological threats could adversely affect telecommunications service. These threats could also disrupt other critical infrastructures, such as electric power, on which the PN is highly dependent for sustained operation. While the PN's supporting technologies provide an expanding array of services and features, and facilitate robustness, these same supporting technologies can introduce exploitable vulnerabilities with adverse effects on service availability and reliability. Considering these threats and vulnerabilities, the potential concern for a widespread network outage is reasonable. Given the limited precedent for telecommunications outages of this magnitude, NSTAC members' prior experiences with smaller-scale outages lead them to believe there is a *low probability* of a widespread, sustained outage of public telephone service. The potential societal impacts of such an outage are high enough to warrant consideration.

The Widespread Outage Subgroup offers the following cost-effective recommendations for the NSTAC and the President to decrease the overall probability of a widespread outage. These measures will further facilitate the readiness of the PN for a more open, interconnected, and uncertain global information infrastructure.

- **Improve Inter-Carrier Coordination for Widespread Outage Recovery**
  Current industry plans and coordination procedures for responding to a widespread telecommunications outage are company oriented. The President should direct the appropriate Federal departments and/or agencies to work with industry to improve inter-carrier coordination plans and procedures. To support this mechanism, communications capabilities are required between Government and the telecommunications industry to respond to and recover from a possible widespread outage affecting National Security Emergency Preparedness (NSEP) services.

- **Remove Legal and Regulatory Obstacles to Widespread Outage Recovery.**

It is not clear who has the authority to resolve legal and regulatory impediments to the rapid and orderly restoration of service during a widespread outage. The President should encourage the Federal Communications Commission (FCC) to maintain a Defense Commissioner at all times to help industry and Government overcome these impediments and to clarify the Defense Commissioner's authority to address NSEP telecommunications regulatory concerns. The President should also encourage the FCC to ensure Local Number Portability (LNP) national standards and requirements, including NSEP, are agreed on and adhered to before implementing LNP on a widespread basis. Sufficient time to complete reliability, interoperability, and security testing of new services and products should be allowed prior to implementing regulatory mandates.

- **Advance the State-of-the-Art for Software Integrity and Interoperability to Reduce the Probability of a Widespread Outage.**
  All U.S. infrastructures, including the PN, continue to be increasingly reliant on software-controlled information systems. Security analysis of software products is not universally practiced by major equipment manufacturers. It is possible, because of the complexity of the large systems involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to protracted denial of service. The President should task the appropriate Federal departments and agencies to work with industry to advance the state-of-the-art for software integrity. The NSTAC should work to increase awareness within the telecommunications industry of the importance of software security and the use of best business practices for managing complex automated systems.

- **Expand Research and Development (R&D) Efforts to Address Telecommunications Technology Vulnerabilities.**
  The President should direct the expansion of government R&D efforts to address the most significant vulnerabilities of new and evolving telecommunications technologies and services. As a first step, existing R&D efforts should be examined and coordinated to determine any necessary increases. Industry should be urged to participate in these efforts. As a specific case, the President should encourage the FCC to examine and assist with the implementation of the Network Reliability and Interoperability Council (NRIC) recommendations as they relate to potential widespread outage vulnerabilities attributed to physical network design and new supporting technologies.

- **Foster Education and Awareness.**
  The NSTAC, as part of its outreach efforts, should offer the NSIE model to the Network Interconnection/Interoperability Forum (NIIF) for consideration and potential use by network operations managers. The NSTAC should encourage the use of this model to help foster effective plans, procedures, and inter-carrier relationships in the increasingly competitive telecommunications environment.

1.0 INTRODUCTION

1.1 Background

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, wrote to Mr. Charles Lee, Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), seeking the NSTAC's forward-looking views on the possibility of a widespread, sustained interruption of the public telephone network. In response, the NSTAC's Network Group and Operations Support Group established the Widespread Outage Subgroup (WOS) to answer Dr. Gibbons' inquiry. This report provides NSTAC's views on the validity of this concern, considering the rapid changes foreseen in the industry structure, regulation, and technologies of the public telecommunications network and other critical infrastructures.

1.2 Scope

This report focuses on the current public telecommunications network and recognizes traditional threats and vulnerabilities, such as equipment malfunctions, natural hazards, sabotage, and physical design. It also addresses potential concerns as the network evolves through new technologies and regulatory mandates, as well as the growing threat from information system intrusions which could trigger systemic network failures.

The specific issues addressed are drawn directly from Dr. Gibbons' letter, including: (1) the likelihood of a widespread outage; (2) possible causes of outages; (3) coordination mechanisms required for recovery of network operations; and (4) the ability of service providers to keep the President apprised of recovery activities and status.

1.3 Widespread Outage Definition

A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day.

2.0 OBJECTIVE

This report answers the following questions:

- To what extent is a widespread, sustained interruption of public telephone service-because of common equipment, software, single point of failure, sabotage, or any other factor-a realistic concern?
- What plan does the industry have for inter-carrier coordination to facilitate recovery of the network from a widespread outage?

- Are existing communication and coordination mechanisms among service providers sufficient for the efficient diagnosis of the problem, identification of technical solutions, and restoration of service from an outage of this type?

- Are there legal or regulatory obstacles that would hinder recovery from such an outage?

- What interface between the telecommunications service providers and the Government would allow the President to be sure that restoration priorities meet the national interest? How would the service providers keep the President apprised of the progress of restoration efforts in the event of an outage affecting multiple companies?

In responding to Dr. Gibbons' questions, this report acknowledges both the current and future states of the public network (PN).[1] It further discusses the potential impact of new technologies and regulatory mandates on robustness and reliability.

3.0 FINDINGS

United States (U.S.) telecommunications service providers have historically offered unparalleled service robustness, availability, and quality. The June 1997 Network Reliability Steering Committee report acknowledged that the PN has maintained a 99.9 percent operational availability while the network has experienced significant growth and technological change. Although the PN's track record is superlative, known threats do adversely affect telecommunications service. Natural disasters such as earthquakes and hurricanes have disrupted elements of the PN, but overall the industry has been successful in mitigating the service impact. Outages in other critical infrastructures, such as electric power,[2] also stress the PN's reliability. While the PN's evolving technologies provide an expanding array of services and features and facilitate robustness, these same technologies can introduce vulnerabilities which, if exploited, could adversely affect service availability and reliability. The rapid implementation of changes to the network fostered by the Telecommunications Act of 1996 (e.g., Local Number Portability, interconnection, unbundling, infrastructure sharing, and collocation) have the potential to introduce further vulnerabilities into the PN. Considering these factors, it is prudent to consider the possibility of an unprecedented and widespread telecommunications outage.

---

1 "The PN includes any switching system or voice, data or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks)" NSIE Risk Assessment, December 1995.

2 On July 2, 1996, a massive power blackout swept across the western United States. One telecommunications carrier reported that 87 of its 1,475 switches used backup generators or batteries to remain in service. Technicians were sent to switches where batteries were being used and in some cases secondary generators were sent to central offices where heat-caused battery exhaustion threatened to shut down the system. Switches on backup power served about 70,000 customers, yet the network remained "fully operational" throughout the power interruption.

3.1 To what extent is a widespread, sustained interruption of public telephone service-because of common equipment, software, single point of failure, sabotage, or any other factor-a realistic concern?

Given the limited precedent for telecommunications outages of this magnitude, NSTAC members' prior experiences with smaller-scale outages lead them to believe that there is a low probability of a widespread, sustained outage of service. However, the potential impact on society of such an outage is high enough to warrant consideration. As an example, the Common Channel Signaling (CCS) disruptions experienced in 1991[3] by some of the NSTAC member companies provided a strong impetus for subsequent improvements to network standards, software, and hardware.

Several additional examples of contributing factors are described in the following subsections.

3.1.1 Software

Within the modern PN, all of the nodes within each network, as well as those within interconnecting networks, are controlled by software furnished by the node equipment manufacturers or their vendors. This software, as with all computer software, is vulnerable to design flaws, implementation errors, and other problems that could cause it to fail or not function as desired, despite its designers' best efforts. Software patches are frequently released to add minor feature enhancements, as well as to correct previous errors. While testing is performed to ensure the software operates as designed and intended, it is not feasible to test for and against every conceivable network condition. Finding and mitigating software mistakes is often a difficult and imperfect process. Detecting subtle but *intentional* and destructive software alterations could be much more problematic. Destructive code, if propagated through large portions of the PN (for example, in a commonly-used equipment node, database, or protocol), could cause widespread turmoil when activated.

Security analysis of software products, including patches, minor version updates, and full new releases, is not universally practiced by many manufacturers. Adequate tools to verify the anti-tampering integrity of the product are not widely used or, in some cases, may not be available. Most software testing is performed to ensure the program features interact and operate as intended. It is possible, because of the complexity of the large systems often involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to a protracted denial of service. For example, the urgent need to update software-dependent systems, nodes, and databases to accommodate Year 2000 or Local Number Portability (LNP) functionality could create an environment where software introduced into the network fabric may result in unintentionally anomalous network behavior.

---

[3] In June and July 1991, network outages occurred in several parts of the United States that were attributed to software errors in the control elements of the SS7 network. Network switching outages and call processing delays were experienced in Los Angeles, CA , San Francisco, CA , Pittsburgh, PA, and parts of Maryland, Virginia, West Virginia and the District of Columbia.

3.1.2 SONET Operations Control

The incorporation of Synchronous Optical Network (SONET) as the transport medium of choice for trunks, data communications lines, asynchronous transfer mode (ATM) and common channel signaling (CCS) links (also known as Signaling System 7) makes it among the most crucial of PN components. Despite its importance to the health of SONET-based networks, SONET's address resolution functions support almost no security measures that could prevent an intruder from subverting it. An attack on the control protocols within portions of a SONET network could degrade operations, with a resulting loss of control of the SONET network elements and transport capabilities.

3.1.3 CCS (SS7) Gateway Screening

Public networks are dependent on CCS, a packet-switched data network employing Signaling System 7 (SS7) protocols, to set up and terminate calls as well as transmit advanced feature data such as Caller ID. A second application of SS7 is its use as a rapid transport network for fraud protection and billing authorization within wireless and wireline networks. Because of publicly-available detailed information about SS7 protocols, an adversary could potentially exploit the CCS packet data network by independently generating SS7 messages and injecting them into the PN signaling links.

SS7 is one of many network capabilities subject to unbundling and widespread interconnection as part of the regulatory scheme implementing the Telecommunications Act of 1996. In addition, a number of commercially-available devices and tools have SS7 message generation capabilities. The pro-competitive impetus to open SS7 networks up to traffic other than that generated by the service provider operating those networks, coupled with the proliferation of third parties who desire to access it, reflects the SS7 network's importance. Loss of, or damage to, the SS7 network almost inevitably precipitates a corresponding degradation or interruption of service to the PN. SS7 network and software security is therefore a requirement of substantial significance to reliability.

Gateway screening is one of a very limited set of SS7 security tools currently available to all network service providers and is implemented at the interface between service providers' networks. Presently, there is no industry-wide understanding of how gateway screening should be extended into the new competitive network environment. Without "standardized" screening, large quantities of malicious or erroneous messages could lead to a widespread degradation.

Many network subsystems, such as operations support systems (OSS), which are used by incumbent carriers for operations, maintenance and billing, were not designed for third-party access. This may be particularly problematic considering the number of potential new service providers that will need access to incumbent networks and subsystems, including the CCS network and OSSs. Many of these new providers are not familiar with security considerations and practices and could present risks to overall network reliability. There is currently no overall unified scrutiny of the interconnected CCS networks for real-time management and control to guard against intrusions and unauthorized users.

3.1.4 Physical Design

The U.S. public networks have been designed to preclude single points of failure above the local switching level. This has been accomplished through substantial investments in both physical and logical diversity. As examples, signal transfer points (STP) of SS7 systems are commonly deployed in mated pairs that are physically and electronically redundant as well as geographically diverse. Long-haul transmission links between switches are increasingly designed to be resilient and self-healing (e.g., SONET rings). Networks are utilizing dynamically-controlled routing, with non-hierarchical network architectures capable of routing traffic around damaged or congested portions of the network in real time. These factors, coupled with the diversity of carriers that exist in the United States, contribute to a high level of PN reliability and robustness. It is therefore highly unlikely that a single point network failure would result in a widespread outage of service. This conclusion is supported by the continuing success of carriers providing reliable service even while experiencing the impact of traditional threats such as natural disasters, cable cuts, and power failures.

Economic tradeoffs, enabled by technological advances, continue to cause some carriers to consolidate and collocate both facilities and network operations functions. While somewhat decreasing the physical diversity of the PN, it has enabled the rapid introduction of advanced network management technologies into consolidated control centers. It will be important for carriers, service providers and vendors to continue to employ "best practices" for reliability and security as new technologies are deployed, networks continue to expand, and new providers connect to the network.

3.1.5 Sabotage

The act of sabotage can take many different forms. Two primary forms of sabotage are damage (physical or electronic) or interference with normal operation. Both of these acts result in disruption of service. To cause a widespread outage, these disruptions would have to occur at a number of facilities, affect multiple carriers, and be successfully coordinated to have a significant and measurable impact. Sabotage can be instigated by either insiders (e.g., employees, contractors), outsiders (e.g., hackers, criminals, nation-states), or-more likely-both. Multiple acts of sabotage may use different attack methods and have different goals, which would increase the confusion and diminish service providers' ability to effectively restore network services. The massive coordination and long-range planning required to execute such an attack, while eluding law enforcement and intelligence agencies, coupled with the physical and logical diversity of the PN, implies a low probability of success.

In summary, the likelihood of a widespread, sustained outage of service resulting from sabotage is remote.

3.1.6 Introduction of New Technologies or Services

New technologies, by their nature, are often more complex and sometimes create unintended consequences and unexpected interactions among subsystems. Because new

technologies cannot be tested for and against every conceivable set of events or network conditions, unforeseen vulnerabilities may be introduced into the network.

Rapid introduction of changes mandated by the Telecommunications Act of 1996 (e.g., Local Number Portability, seamless interconnection, unbundling, infrastructure sharing, and collocation) could potentially introduce unforeseen vulnerabilities into the PN. The Telecommunications Act requires existing carriers to allow new carriers to interconnect with existing networks "at any technically feasible point."[4] The lack of standards and interfaces to support multiple carrier use of OSS's increases the likelihood of potential conflicts and mistakes. Additionally, security and privacy concerns must be addressed as these standards and interfaces are developed. Conflicts and mistakes, or overt malicious actions, increase the probability of a significant outage. The Network Reliability and Interoperability Council's (NRIC) report to the FCC, published in July 1997, provides additional guidance and recommendations to be considered in developing such standards.

Increasing connectivity of OSS and PN control mechanisms to the Internet remains an item of NSTAC concern. As described in "*An Assessment of the Risk to the Security of Public Networks*" in December 1995:

> "Connections to the Internet are increasing, and while many service providers have exercised due care in isolating critical network systems and components from more open-enterprise data networks and the Internet, there may still be potentially exploitable connectivity, such as through a restrictive router or firewall. An error in the design, configuration, or implementation of such a protective barrier could lead to compromise of critical systems from anywhere in the world."[5]

Conversely, the Internet is highly dependent on PN-based switching and transport networks for long-haul transmission of traffic. A disruption or outage in the PN will likewise interfere with Internet traffic.

3.2 What plan does the industry have for inter-carrier coordination to facilitate recovery of the network from a widespread outage?

There are two categories of widespread outages. The first type is caused by the impact of traditional hazards, threats, and vulnerabilities. The other is characterized by a systemic and widespread network failure.

3.2.1 Traditional Hazards, Threats, and Vulnerabilities

---

4 Telecommunications Act of 1996 (47 U.S.C. Section 251c(2)(B)).

5 *An Assessment of the Risk to the Security of Public Networks*, Network Security Information Exchange (NSIE), December 1995.

Existing carriers have disaster recovery plans and a proven track record of quickly recovering from traditional outages. Included in many of these recovery plans are bilateral and multilateral mutual aid agreements, designed to address multicarrier network problems. These agreements focus on resource sharing, such as supplies, portable equipment, motor vehicles, personnel, and may also dictate arrangements for temporary routing of traffic and services over another carrier's spare facilities. In addition to formal agreements, informal arrangements exist throughout the industry for inter-carrier and carrier-vendor communication and cooperation during emergencies. The vast majority of telecommunications disruptions that require a multi-carrier/vendor response effort are addressed through industry cooperation. Instead of precisely defining the scope of network sharing or resource lending arrangements, the industry approaches each incident with a customer-focused "can do" approach that has a long history of success. Informal arrangements offer additional flexibility in dealing with emergencies because each telecommunication outage situation is unique. These informal arrangements leverage relationships between network managers already established within the industry through day-to-day interaction and operations.

3.2.2 Systemic and Widespread Network Failure

The industry has had limited experience with a systemic, widespread network outage. Currently, there is no industry-wide plan to facilitate inter-carrier coordination for recovering from a widespread outage of this nature. While an industry-wide plan has not yet been developed, companies have prepared internal plans and processes for maintaining the integrity of their own networks. These plans and processes include specifics for diagnosing problems, identifying solutions, and ensuring service can be restored as rapidly and orderly as possible.

3.3 Are existing communication and coordination mechanisms among service providers sufficient for the efficient diagnosis of the problem, identification of technical solutions, and restoration of service from an outage of this type?

Although some agreements, communication systems, and coordinating mechanisms do exist between and among carriers, it is questionable whether they would be a sufficient response to a severe widespread service outage. In the event of an outage affecting multiple carriers, individual carriers will first concentrate on restoring service in their own systems before reestablishing connections with other carriers. To assist in service restoration, most of the larger telecommunications companies have alternate communications capabilities between critical centers in their networks. These alternatives include private line networks, high frequency (HF) radio, and satellite telephone systems.

Reconnection with other networks would only be initiated after individual carriers are confident of the health of their own network and those to which they are connecting. It is during this phase that a means of communication and coordination between and among critical centers is indispensable. Several communications capabilities exist outside the PN for inter-carrier coordination of service restoration. The Backup Emergency Alerting Management System (BEAMS) is a switched private line network operated by the National Telecommunications Alliance (NTA) connecting selected telecommunications carriers, equipment and switch vendors,

and the National Communications System (NCS). The National Telecommunications Coordinating Network (NTCN), a multimedia network administered by the NCS's National Coordinating Center for Telecommunications (NCC), provides emergency communications among critical Federal Government and industry operations centers. Although some of the major U.S. carriers are connected via BEAMS and/or NTCN, both networks would require expansion to meet an emerging need for inter-carrier coordination of restoration from a widespread telecommunications outage.

Several industry fora have taken strides to alleviate potential coordination problems in the event of a catastrophic outage. For example, the Network Interconnection/Interoperability Forum (NIIF) of the Alliance for Telecommunications Industry Solutions (ATIS) developed emergency traffic management guidelines for network management personnel at local and interexchange carriers. The guidelines provide alternatives for dealing with network emergencies, including network congestion, switch or network failures, and SS7 failures. In addition, the NIIF maintains contact directories for use in emergencies. These directories are targeted toward incident type and include contact and reporting numbers for network management centers, for use in the event of catastrophic SS7 failures, media simulated mass calling events, and other service troubles. The NIIF and other committees within ATIS address industry-wide issues concerning telecommunications interconnection and interoperability, network reliability analyses, and implementation and deployment of new technologies, including Synchronous Optical Network (SONET) and Advanced Intelligent Network (AIN) services.

A successful coordinating mechanism requires a high level of mutual trust and information sharing. An example of such a mechanism is the Network Security Information Exchange (NSIE)[6], whose goal is to share information and experiences among telecommunications network security managers. The NSIE has established trusted relationships among and between the government and industry members. Trust among industry and government participants facilitates responses to routine and emergency security incidents.

Much of the telecommunications industry's success in recovering from outages is attributed to long-standing inter-carrier relationships existing among incumbent network managers that arise from day-to-day interaction and operations. In the increasingly competitive telecommunications market, this level of cooperation and trust may be difficult to sustain. Although not a perfect model, the NSIE example could be offered to industry network operations managers. Through the auspices of the NIIF, industry might benefit from an NSIE-like body to share their inter-carrier operations concerns in the increasingly diverse and competitive environment.

---

[6] The Network Security Information Exchange (NSIE) is a forum for industry and Government members to share and coordinate information security knowledge that will assist in preventing, detecting, and/or investigating public network penetrations. The NSIE identifies issues involving penetration or manipulation of software and databases affecting NSEP telecommunications, and exchanges views on threats, incidents, and vulnerabilities affecting the PN. The current NSIE membership includes 9 Government organizations from the law enforcement, national defense, and intelligence communities, and 19 NSTAC member companies representing the telecommunications, information systems, and financial industries.

3.4 Are there legal or regulatory obstacles that would hinder recovery from such an outage?

NSTAC members have identified several legal and regulatory barriers to the rapid and orderly restoration of service during a widespread outage. For example, the ability of a local exchange carrier to provide emergency inter-Local Access Transport Area (LATA) communications to state or Federal agencies may prove to be critical to their ability to protect the interests of public safety and national security.[7] In addition, it may also be necessary for a carrier to utilize the resources of its affiliates to make necessary physical repairs to the network that could be perceived to involve manufacturing of telecommunications hardware.[8] Finally, domestic carriers may often need to call on the assistance of international carriers to recover from a significant outage. While many companies are not prohibited from providing in-region inter-LATA and manufacturing services, Sections 271 and 273 of the Telecommunications Act require that Regional Bell Operating Companies (RBOC) satisfy a number of requirements and receive Federal Communications Commission (FCC) approval to offer these services. No RBOC currently has approval to perform these services, and until such approval is requested and obtained, this obstacle remains and could potentially hinder recovery from a future widespread outage. Additionally, other regulatory safeguards imposed on other companies and RBOCs alike could likewise affect the ability of carriers to fully use their corporate resources to respond effectively to a widespread outage (e.g., restrictions imposed on the financial, marketing, and operational interactions of dominant and non-dominant carriers, and FCC requirements for carriers to keep their regulated and unregulated businesses completely separated).

The Telecommunications Act of 1996 transfers many telecommunications policy enforcement responsibilities from a single Federal judicial official to the FCC and, to a lesser extent, the Department of Justice (DOJ). This transfer of authority raises questions about the appropriate official(s) or organization(s) telecommunications companies should approach for swift and consistent guidance in an emergency. It also is unclear whether the FCC has the authority to grant temporary waivers of applicable sections of the Telecommunications Act during a widespread outage recovery effort, even when the waiver is in the public interest. Currently, existing regulations regarding the National Security and Emergency Preparedness (NS/EP) responsibilities of various Federal officials and organizations, as described below, do not place a

---

[7] In 1991, BellSouth experienced a 1-year delay in receiving a Modification of Final Judgment (MFJ) exception. Hurricane Hugo caused disruption to the State of South Carolina's private line network. As a result, the BellSouth Corporation asked the Department of Justice (DOJ) to support a petition seeking an exemption from part of the MFJ in order to provide emergency inter-LATA communications for the State of South Carolina. After a year delay, and following an extensive public comment and review period, the DOJ endorsed the petition. For reference, a copy of the request, dated 18 March, 1991, from Mr. Ted Lightle, Director, Division of Information Resource Management, State of South Carolina, to Ms. Constance K. Robinson, Esq., Acting Chief, Communications and Finance Section, Antitrust Division, U.S. DOJ, is attached in Appendix C.

[8] In 1991, Bell Atlantic Corporation requested Bellcore's assistance to restore part of the PSN serving the mid-Atlantic region, including Washington D.C. and the Federal Aviation Administration's air traffic control system at Newark International Airport. As a Regional Bell Operating Company (RBOC) affiliate, however, Bellcore was concerned that physical repairs made to the network might be viewed as "manufacturing" and thus violate the then existing MFJ provisions prohibiting the manufacturing of telecommunications equipment by the RBOCs or their affiliates.

single Federal official in charge of deciding whether to enforce or waive compliance with applicable laws or regulations.

3.4.1 Federal Communications Commission

Executive Order (E.O.) 12472 requires the FCC to perform functions during national non-wartime emergencies, including the investigation of violations of pertinent law and regulations and the initiation of appropriate enforcement actions.[9] The FCC's rules accordingly assign the FCC Defense Commissioner the specific duties of assuring continuity of the Commission's NS/EP functions and of approving NS/EP plans and programs (including the provision of service by common carriers and the investigation and enforcement of violations of Federal law).[10] These regulations task the Defense Commissioner to uphold carriers' compliance with applicable law. The rules are unclear, however, as to whether they extend to the Defense Commissioner or the entire Commission (with or without consultation with the DOJ) the power to forbear from enforcing relevant provisions of the Telecommunications Act during a crisis. Even if the rules did place one official in charge, that one Commissioner may not have the authority to override the Telecommunications Act (i.e., permit something that is specifically prohibited or precluded by the Act) in an emergency such as a widespread outage.

3.4.2 The President

Section 706(e) of the Communications Act of 1934, as amended, empowers the President to suspend or amend, during a national emergency, FCC rules applicable to any wire communications facilities. Section 706(g), however, prohibits the President from making any amendment to the FCC's rules that the agency would not itself be authorized by law to make.[11] Because it is questionable whether the FCC Defense Commissioner or the entire Commission by itself could grant to service providers waivers from complying with relevant portions of the Telecommunications Act, it follows that the President's power to do so is also questionable.

3.4.3 The National Security Council (NSC) and Office of Science and Technology Policy (OSTP)

Section 2(c)(1)(a) of E.O. 12472 instructs the NSC to coordinate the development of policy, plans, programs, and standards within the Federal Government for the use of the Nation's telecommunications resources during non-wartime conditions. Section 2(b)(2) charges the Director, OSTP, to provide appropriate guidance and assistance to the President and other Federal organizations responsible for the provision, management, or allocation of telecommunications resources during such conditions. Section 2(b)(3) further assigns the Director, OSTP, with establishing and chairing a Joint Telecommunications Resources Board

---

9 Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984.

10 Federal Communications Commission rules, "Defense and Emergency Preparedness Functions," 47 C.F.R. 0.181-0.186.

11 Section 706 of the Communications Act of 1934 (47 U.S.C. 606), "War Emergency Powers of President."

(JTRB) to assist the Director in exercising non-wartime telecommunications functions.[12] Although the NSC and the JTRB might help craft future policy initiatives to address the industry's legal concerns prior to the occurrence of a widespread outage, it is unclear whether either group would play a significant role during an actual recovery effort.

3.5 What interface between the telecommunications service providers and the Government would allow the President to be sure that restoration priorities meet the national interest? How would the service providers keep the President apprised of the progress of restoration efforts in the event of an outage affecting multiple companies?

For many years, the telecommunications industry has provided the NCC with relevant information pertaining to major outages. More recently it has also provided the FCC with reports of outages that conform to the FCC's specific requirements. Because the NCC's mission is to monitor NSEP telecommunications, and experience has shown that industry willingly provides relevant outage information to the NCC, then the NCC is positioned to collect widespread outage information for the President. To support this function, the Office of the Manager, National Communications System (OMNCS), has a video teleconferencing system that is used to communicate directly with the Executive Office of the President. The NCC Vision Subgroup is addressing the issue of sharing intrusion and network outage information among industry and government.

4.0 CONCLUSIONS/RECOMMENDATIONS

While the PN is robust and highly reliable, it is also built on a complex, interconnected set of heterogeneous technology platforms. The PN can be disrupted by natural calamities, electric power outages, or assaulted by hostile forces. In addition, rapid legislative, regulatory and market changes could potentially introduce unforeseen vulnerability into the PN. Although the probability of a widespread sustained outage is low, the high potential societal cost of such an outage requires that the concern be addressed. Industry and government can take cost-effective measures to reduce the overall risk of a widespread outage and enable an orderly restoration of service if such an outage occurs.

Other Industry Executive Subcommittee groups, including the Intrusion Detection Subgroup, Information Infrastructure Group, Legislative and Regulatory Group, and the NCC Vision Subgroup, are examining several of the issues addressed in this report that would improve

---

[12] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984. The JTRB's membership consists of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence; the Assistant Secretary, Communications and Information, of the Department of Commerce; the Commissioner, Federal Telecommunications Service, of the General Services Administration; the Associate Director, Operations Support, of the Federal Emergency Management Agency; the Defense Commissioner of the FCC; and the Manager, NCS.

the overall ability of the United States to respond to a widespread telecommunications outage. We recommend that their conclusions be examined in light of our findings.

Pursuant to the concerns expressed in Dr. Gibbons' letter, the Widespread Outage Subgroup offers the following recommendations:

4.1 RECOMMENDATIONS

4.1.1 Improve Inter-Carrier Coordination for Widespread Outage Recovery

Current industry plans and coordination procedures for responding to a widespread telecommunications outage are company-oriented. Inter-carrier coordination plans and procedures for responding to a widespread telecommunications outage require upgrading to meet new and emerging threats.

The President should direct the appropriate Federal departments and/or agencies to-

- Cooperate with industry to build a mechanism to upgrade current industry
  - Recovery plans
  - Coordinating mechanisms, and
  - Emergency communications capabilities.
- Ensure adequate communications capabilities are available between Government and the telecommunications industry, as well as with other critical infrastructures, to respond to and recover from a possible widespread outage affecting NS/EP services.

4.1.2 Remove Legal and Regulatory Obstacles to Widespread Outage Recovery

There are potential legal and regulatory impediments to the rapid and orderly restoration of service during a widespread outage. It is not clear who has the authority to resolve these impediments. The relative specificity of the rules governing the FCC Defense Commissioner's responsibilities suggests that this individual could help industry and Government overcome these impediments.

The President should encourage the FCC to-

- Appoint and maintain a Defense Commissioner
- Clarify the Defense Commissioner's authority to-

- Address NSEP telecommunications regulatory concerns in Commission activities, rulemaking, and particularly during emergency situations

- Establish a process for the expeditious resolution of NSEP issues and other impediments affecting industry recovery from a widespread telecommunications service outage.

Competitive market and legislative mandates often create a rush to introduce new products and services before they are fully evaluated in the laboratory and under live network conditions (e.g., Local Number Portability [LNP]). Before schedules are mandated through FCC regulations, reliability, interoperability, and security concerns need to be carefully considered to guard against premature implementation of "unseasoned" technologies that may contribute to the possibility of a widespread outage. An additional concern is the impact of industry restructuring on NSEP communications, especially considering the entry of new carriers under the Telecommunications Act.

The President should also encourage the FCC to-

- Minimize the possibility of a widespread outage by ensuring LNP national standards and requirements, including NSEP, are agreed on and adhered to before implementing LNP on a widespread basis

- Allow sufficient time to complete reliability, interoperability, and security testing of new services and products prior to implementing regulatory mandates.

4.1.3 Advance the State-of-the-Art for Software Integrity and Interoperability to Reduce the Probability of a Widespread Outage.

All U.S. infrastructures, including the PN, continue to be increasingly reliant on software-controlled information systems. Security analysis of software products is not universally practiced by major equipment manufacturers. It is possible, because of the complexity of the large systems involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to protracted denial of service.

The President should-

- Task the appropriate Federal departments and agencies to work with industry to lead the advance of the state-of-the-art for software integrity through intense research, development, and operational investigations.

The NSTAC should-

- Increase awareness within the telecommunications industry of the importance of software security and the use of best business practices for managing complex automated systems.

4.1.4 Expand Research and Development (R&D) Efforts to Address Telecommunications Technology Vulnerabilities

New technologies, by their nature, often are more complex, sometimes resulting in unintended consequences and unexpected interactions among subsystems. Because new technologies cannot be tested for and against every conceivable set of events or network conditions, unforeseen vulnerabilities may be introduced into the network.

The President should-

- Direct the expansion of government R&D efforts to address the resolution of the most significant vulnerabilities of new and evolving telecommunications technologies and services. As a first step, identify or coordinate more closely existing R&D efforts in order to determine any necessary increases.

- Encourage industry to assist in these efforts.

- Encourage the FCC to examine and assist with the implementation of the Network Reliability and Interoperability Council (NRIC) recommendations as they relate to potential widespread outage vulnerabilities attributed to physical network design, and new supporting technologies.

4.1.5 Foster Education and Awareness

Trust among telecommunications network managers facilitates the effective response to routine and emergency network incidents. Much of the telecommunications industry's success in recovering from outages is attributed to long-standing inter-carrier relationships among network managers arising from day-to-day interaction and operations. Achieving and maintaining this level of trust becomes more difficult in an increasingly competitive environment.

The NSTAC should, as part of its outreach efforts-

- Offer the NSIE model to the Network Interconnection/Interoperability Forum (NIIF) for consideration and potential use by network operations managers

- Encourage the use of this model to help foster effective plans, procedures and inter-carrier relationships in the increasingly competitive telecommunications environment.

ANNEX A

References

REFERENCES

- *Potential Legal and Regulatory Obstacles to Widespread Outage Recovery,* Draft Report of the Legislative and Regulatory Group (LRG) of The President's National Security Telecommunications Advisory Committee (NSTAC), September 30, 1997.

- *Network Interoperability: The Key to Competition*, Network Reliability and Interoperability Council (NRIC) of the Federal Communications Commission (FCC), July 1997.

- *Electric Power Information Assurance Risk Assessment Report*, Information Assurance Task Force (IATF) of The President's NSTAC, March 1997.

- *Analysis of Power Related Network Outages*, Alliance for Telecommunications Industry Solutions, Network Reliability Steering Committee, August 29, 1996.

- *An Assessment of the Risk to the Security of Public Networks*, Network Security Information Exchange (NSIE), December 1995.

- *Final Report of the Common Channel Signaling Task Force*, The President's NSTAC, January 1994.

- *Network Reliability: A Report to the Nation*, Network Reliability Council of the FCC, June 1993.

- FCC Common Carrier Bureau Report on Network Outages, July 1991

- *Growing Vulnerability of the Public Switched Networks*, National Research Council, 1989.

ANNEX B

Acronyms

ACRONYMS

AIN	Advanced Intelligent Network
ATIS	Alliance for Telecommunications Industry Solutions
BEAMS	Backup Emergency Alerting Management System
CCS	Common Channel Signaling
DOJ	Department of Justice
EO	Executive Order
HF	High Frequency
JTRB	Joint Telecommunications Resources Board
LATA	Local Access Transport Area
LNP	Local Number Portability
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NIIF	National Interconnection/Interoperability Forum
NRIC	Network Reliability and Interoperability Council
NSEP	National Security Emergency Preparedness
NSIE	Network Security Information Exchange
NSTAC	President's National Security Telecommunications Advisory Committee
NTA	National Telecommunications Alliance
NTCN	National Telecommunications Coordinating Network
OMNCS	Office of the Manager, National Communications System
OSS	Operations Support System
OSTP	Office of Science and Technology Policy
PN	Public Network
R&D	Research and Development
SONET	Synchronous Optical Network
SS7	Signaling System 7
STP	Signal Transfer Point
U.S.	United States
WOS	Widespread Outage Subgroup

ANNEX C

Widespread Outage Subgroup Members

Widespread Outage Subgroup Members

NTA	Mr. Bob Burns, Chair
AT&T	Mr. Dave Bush
Bellcore	Mr. Carl Ripa
GTE	Ms. Ernie Gormsen
MCI	Mr. Mike McPadden
OMNCS	Mr. Bernie Farrell
SAIC	Mr. Hank Kluepfel
USTA	Dr. Vern Junkmann
US West	Mr. Jon Lofstedt

ANNEX D

Letters

LETTERS

1) April 24, 1997, letter from Dr. John H. Gibbons, Assistant to the President for Science and Technology, to Mr. Charles R. Lee, Chairman, National Security Telecommunications Advisory Committee (NSTAC), Chairman and Chief Executive Officer, GTE Corporation.

2) March 18, 1991, letter from Mr. Ted L. Lightle, Director, Division of Information Resource Management, State of South Carolina, to Ms. Constance K. Robinson, Esq., Chief, Communications and Finance Section, Antitrust Division, U.S. Department of Justice.

3) August 24, 1992, letter from Mr. Richard L. Rosen, Esq., Acting Chief, Communications and Finance Section, Antitrust Division, U.S. Department of Justice, to Mr. Michael J. Schwartz, Esq., General Attorney, BellSouth Corporation.