

Critical Infrastructure Protection in the National Capital Region

**Risk-Based Foundations for Resilience and
Sustainability**

**Final Report, Volume 7:
Telecommunications Sector**

September 2005

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

This Page Intentionally Blank

Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume 7: Telecommunications Sector

Submitted in fulfillment of:

Department of Homeland Security Urban Areas Security Initiative (UASI) Grant 03-TU-03; and
Department Justice Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199

September 2005

PJ Aduskevicz, Lee Zeichner, and Benjamin Stafford

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University



– **Notice** –

This research was conducted as part of the National Capital Region Critical Infrastructure Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator.

It was sponsored by the U.S. Department of Homeland Security's Urban Area Security Initiative grant #03-TU-03, and by the U.S. Department of Justice Community Oriented Policing Services Program grant #2003CKWX0199, under the direction of the Senior Policy Group of the National Capital Region.

The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security, the Department of Justice, or the Senior Policy Group of the National Capital Region.

Copyright © 2005 by George Mason University

Published in 2006 by George Mason University

Table of Contents

Executive Summary	1
1. Sector Background	4
1.1 Sector Profile.....	4
1.1.1 General.....	4
1.1.2 Definition.....	7
1.1.3 Features.....	7
1.2 Regional Sector Characteristics.....	8
1.2.1 Service Areas.....	8
1.2.2 Companies, Employees, Customers.....	8
1.2.3 Capacity, Supply, Demand.....	8
1.3 Review of Authorities.....	8
1.3.1 Statutes.....	8
1.3.2 Regulations.....	9
1.3.3 Roles and Responsibilities.....	9
1.4 Mapping of Interdependencies.....	12
1.4.1 Upstream Sectors.....	13
1.4.2 Downstream Sectors.....	14
1.4.3 Sidestream Sectors.....	15
1.4.4 Other Dependencies.....	16
2. State of Security Assessment	17
2.1 Assessment of Status and application of CIVA/RM in sector.....	17
2.1.1 Awareness of CIP and CIVA/RM.....	17
2.2 Availability of Appropriate Tools.....	18
2.2.1 Vulnerability Assessments.....	18
2.2.2 Compliance-oriented policies and procedures.....	19
2.2.3 Risk management.....	20
2.3 Extent of application of appropriate tools through resource allocation.....	20
2.4 Extent of implementation of CIP measures.....	21
2.5 Extent of evaluation of CIP effectiveness.....	22
3. Risk Reduction Programs and Processes	22
3.1 Risk Reduction Project/Investment Recommendations.....	22
3.1.1 Tactical Steps for Immediate Benefit on the Ground.....	23
3.1.2 Strategic Steps for Long-Term Benefit on the Ground.....	23
3.2 Risk Reduction Process Improvements.....	23
3.2.1 Recommendations for enhancements.....	23
3.2.2 Recommendations for enhancements in risk management.....	24
3.3 Specific recommendations for governance at sector-level.....	24
3.3.1 Incentives.....	24
3.3.2 Organization and Management (e.g. accreditation, enforcement).....	25
3.4 Specific recommendations addressing dependencies.....	25
3.4.1 Intra-sectoral.....	25
3.4.2 Inter-sectoral.....	25
3.4.3 Regional.....	26
3.5 Measuring Effectiveness.....	27
3.6 Managing Continuous Improvement.....	27
4. Conclusion	28

4.1	Challenges.....	28
4.2	Areas for Future Investigation.....	28
	Appendix A: Methodology for Data Gathering and Analysis Literature Review for Sector.....	29
	Appendix B: Focus Group Questions.....	31
	Appendix C: Focus Group Members/NCC Membership.....	33
	Appendix D: Discussion of the Internet.....	35
	Appendix E: NRIC Physical, and Cyber Best Practices and Disaster Recovery.....	40
	Appendix F: Proactive Telecomm Industry Initiatives.....	44
	Appendix G: Acronyms.....	51
	Appendix H: Glossary.....	52
	Appendix I: Bibliography.....	54
	Appendix J: Alliance for Telecommunications Industry Solutions	56
	Appendix K: Endnotes.....	57

List of Figures

Figure 1: Mapping Relationships.....	12
Figure 2: Internet Network Levels Diagram.....	16

List of Tables

Table 1: Upstream Sectors.....	13
Table 2: Continuum of Vulnerability Assessment and Risk Management Model.....	19

Telecom Sector Report

Executive Summary

I. Sector Overview

The telecommunications industry has changed significantly since 1984 and the divestiture of the Bell System. It has changed from predominately equipment and voice services to a converged set of services with new service providers continually entering the market. Two key policy events shaped the last twenty years: The court ordered breakup of AT&T ; and the Telecommunications Act of 1996 aimed to deregulate the industry so any communications business could compete in any market against any other. Many new wireless service providers, cable, satellite and Internet providers have emerged since. (Appendix C has a list of key providers in the National Capital Region (NCR) that are also members of the National Coordinating Center for Telecommunications (NCC).) The NCC has representatives of all the critical telecommunications firms for nationwide service and within the capital region. These representatives handle special requests and issues of regional and national importance; they are designated spokespersons for their corporations on key issues; and, they have the ability to reach senior leaders of their firms in a crisis or emergency.

The industry expanded in the 1990s in connection with the growth spurt of the economy. Consequently, large investments were made in new fiber facilities, which in turn helped upgrade/modernize the transport layer of the infrastructure. Features to provide enhanced reliability and resiliency, and new technology allowing for new services, such as Voice over Internet Protocol (VoIP) were added. The NCR infrastructure has experienced these same changes.

Risk Assessment and Business Continuity

The telecommunications industry utilizes applied risk management and business continuity principles as part of its daily business structure. Incident management is a continuous business operation/process for service providers. For example, there is always the threat of a backhoe digging up a cable. Protection, mitigation, and response and recovery are processes utilized daily, and rigorous root cause analysis is routinely completed. For Critical Infrastructure Protection (CIP) since 9/11, service providers have overlaid the terrorist threat mode analysis to their established procedures to deal with vulnerabilities.

Interdependencies/Dependencies

Telecommunications and information systems are critical elements of our nation's infrastructure; many other sectors including transportation, finance and banking, and electric utilities rely heavily on this infrastructure to carry out important functions. In turn, telecommunications relies heavily upon power, water, transportation, finance and banking, to maintain its mission critical services. Recognition of telecommunications as "critical infrastructure" dates back several administrations illustrated in August 1963 when by a Presidential Memoranda, *John F. Kennedy established the National Communications System (NCS)*. Further, the establishment of the National Coordinating Center (NCC) in January 1984, as a result of divestiture, is further recognition that telecommunications is a critical infrastructure.

Overarching Findings

The data gathering and the focus group meeting, represented by communications service providers, industry associations, and government, found evidence of:

- Active involvement by industry and government in critical infrastructure programs. The government has sponsored or is currently sponsoring forums for private industry and the government to work through common issues involving CIP. Examples include National Security Telecommunications Advisory Council (NSTAC), Network Reliability and Interoperability Council (NRIC), National Coordination Center (NCC). Private Industry has also invested resources on its own to review and develop new standards and business processes as mentioned above. Examples include Alliance for Telecommunications Industry Solutions (ATIS), Internet Engineering Task Force (IETF), International Organization of Standardization (ISO), European Telecommunications Standards Institute (ETSI), and International Telecommunications Union (ITU).
- Risk management/business continuity is important to this industry because stable reliable infrastructure is a key attribute to successful business for the communications sector. These processes were established and incorporated into business plans and operations long before 9/11. Certainly, the aftermath of September 11th increased activities and assessments in risk management/business continuity models overlaying terrorist threat modes. Service providers at the focus group meeting represented risk management/business continuity principles as a process inherent to their respective businesses.
- The NCR will have and has had unique activities, such as Presidential inaugurations that require the assistance of the communications sector. Moreover, the NCR is the seat of the national government, headquarters of national defense, and home to numerous international institutions. The NCS/NCC for critical communications activities as well as special events should be a focal point for telecommunications needs for the NCR. The coordinating center can be a vehicle for specific needs during an event or preplanning required for an event: hence, the NCR could benefit from the ongoing vulnerability and risk assessment activities conducted at the NCC along with participation of private industry.

Recommendations and Future Work

- Continue to officially recognize the NCC/NCS/Telecom Information Sharing and Analysis Center (Telecom ISAC) as the source of contact for the communications sector; and, recommend that more non-traditional communications players, such as cable and Internet Service Providers (ISP), participate in the center for better synergy.
- Create a single Point of Contact (POC) for perimeter control process and, once established, maintain the process; eliminate the need to change the process during an incident or function.
- Develop a methodology to have one source for requests to the telecommunications sector in connection with recommendations coming out of studies, evaluations, and tabletops: not 50 states, multiple counties and cities, including the NCR, rather, have a single source to funnel requests.
- Have Federal Emergency Management Agency (FEMA) abide by the National Response Plan – which designates the Federal Emergency Communications Coordinator (FECC) as the single POC for the sector during an event.
- Increase the NCR’s awareness and education of the services the NCS and NCC perform for the government and the communications sector; have a senior representative from the Department of Homeland Security’s (DHS) Office of the National Capital Region

Coordination participate with and/or utilize the NCS/NCC as the single point of contact for any communications issues within the NCR region.

- Have the federal government, when working with the communications service providers, provide feedback and threat information that is useful to the sector for response and mitigation.
- Incorporate the communications sector, through the NCS/NCC, as full participants with the government sector, especially for the National Special Security Events (NSSE) process.
- Conduct a study to determine ways to finance security improvement/risk mitigation and provide recommendations.
- Conduct tabletop exercises – interdependencies with other sectors. Expense reimbursement funding for sector participation in the exercise should be part of the process design to ensure success.

Acknowledgements

This report was prepared by the faculty and staff of the Critical Infrastructure Protection Program (CIPP) at George Mason University's School of Law, P.J. Aduskevicz, PJ Aduskevicz Enterprise LLC, Lee Zeichner, President, Zeichner Risk Analytics and Ben Stafford, Sector Coordinator, Zeichner Risk Analytics/George Mason University. The authors would like to thank the National Communications Systems National Coordinating Center members for supporting the George Mason University National Capital Region Critical Infrastructure Protection project. Their contributions of time, resources and expertise were invaluable.

The authors would also like to thank the National Capital Region's Senior Policy Group for funding this project.

1. Sector Background

1.1. Sector Profile

1.1.1 General

The telecommunications sector includes companies engaged in providing telecommunications or network services and providers of the equipment and software employed in the telecommunications infrastructure. Companies provide telecommunications services to a customer base ranging in size from a few hundred to several million. Some of these companies are engaged in the full spectrum of telecommunications services while others may specialize in any one or more telecommunications services, including local distribution, local and long-distance telephony, customer-facing Internet Service Providers (ISP), Internet Providers (IP) backbones, cellular wireless (telephony, text messaging, paging and Internet access), satellite (telephony and data), free-space optical, radio, and other information transmission services. In addition to the service providers and vendors, the sector also includes telecom professionals, Standards Development Organizations (SDO), trade organizations, and entities involved in conformity assessment.

Telecommunications has changed significantly since 1984 and the divestiture of the Bell System. It has evolved from predominately equipment and voice services to a converged set of services with new service providers continually entering the markets.

Two key policy events shaped the last twenty years. The court-ordered break up of AT&T and the Telecommunications Act of 1996 aimed to deregulate the industry. As a result, many new wireless, cable, satellite and Internet providers have emerged.

The industry continued to expand in the 1990s in connection with the growth spurt of the economy. Thus, investments were made in new fiber facilities, which helped upgrade/modernize the transport layer of the infrastructure. Further, automatic routing (one feature as a result of the upgrades) could alleviate impact to an affected area, if a failure existed, and has also helped to mitigate risk for technology segments/equipment deemed as critical in the infrastructure.

Telecommunications and information systems are critical elements of our nation's infrastructure, and many other sectors including transportation, finance and banking, and electricity rely on this infrastructure to carry out their business functions. In turn, telecommunications relies heavily upon power, water, transportation, and finance and banking to maintain its mission critical services. Recognition of telecommunications as "critical infrastructure" dates back several administrations.

In recognition of the critical functions of telecommunications, the National Coordinating Center for Telecommunications (NCC) was created at divestiture for National Security and Emergency Preparedness (NS/EP). (Additional information on the NCC can be found in Appendix C.) The center has been in service for the government and the communications sector for more than 20 years. In addition, the NCC Telecom Information Sharing and Analysis Center (ISAC) is an industry/government partnership that provides around-the-clock threat analysis, warning, and incident coordination for industry participants. When the National Security Telecommunications Advisory Committee (NSTAC) was established in 1982 by Executive Order 12382 by President Reagan, it laid the foundation for the NCC when it made its first recommendation that a national coordinating mechanism for emergency telecommunications be formed. Today, the reach of the NCC Telecommunications ISAC includes 30 member companies and 3 member associations: 1) the Cellular Telecommunications and Internet Association (CTIA), 2) the Telecommunications

Industry Association (TIA), and 3) the United States Telecom Association (USTA). Through member companies and member associations, the reach of the Telecom ISAC within the United States includes:

- Approximately 95% of wire-line telecommunications service providers, by serving areas and subscribers.
- More than 60% of wire-line telecommunications vendors, by sales volume.
- Approximately 95% of wireless telecommunications service providers, by serving areas and subscribers.
- More than 90% of the wireless telecommunications vendors (equipment/software suppliers) by sales volume.
- More than 42% of the consumer Internet Service Providers (the companies that provide services such as data and voice) subscribers.
- Approximately 90% of the Internet Service Providers backbone networks.
- Six of the top 10 system integrators in the US Federal Information Technology (IT) market.
- 15% of Domain Name Service root and global Top Level Domain operators.

Internationally, the International Organization for Standardization (ISO) Security Advisory Group (AG) on Security gives each of its representatives a voice to ensure that advances made in homeland security to date are not only preserved, but also become part of the foundation of international security. This not only ensures that businesses will remain competitive in the market, it also gives the international community a foundation of existing consensus standards to build on, especially for some of the most critical security technologies.

Risk Assessment and Business Continuity

The telecommunications industry utilizes applied risk management and business continuity principles as part of its daily business structure. Incident management is a continuous business operation/process for service providers. For example, there is always the threat of a backhoe digging up a cable. Therefore, protection, mitigation, and response and recovery are processes utilized daily, and rigorous root cause analysis is completed on a routine basis. For Critical Infrastructure Protection (CIP) in our world since 9/11, service providers have overlaid the terrorist threat mode analysis to their established procedures to deal with vulnerabilities.

Interdependencies/Dependencies

Telecommunications and information systems are critical elements of our nation's infrastructure and many other sectors including transportation, finance and banking, and electric utilities rely heavily on this infrastructure to carry out important functions. In turn, telecommunications relies heavily upon power, water, transportation, and finance and banking, to maintain its mission critical services. Recognition of telecommunications as "critical infrastructure" dates back several administrations. *John F. Kennedy established the National Communications System (NCS) by a Presidential Memoranda on August 21, 1963. This mandate included linking, improving, and extending the communications facilities and components of various federal agencies, focusing on interconnectivity and survivability.* Accordingly, the establishment of the NCC in January 1984, as a result of divestiture, is further recognition that telecommunications is a critical infrastructure. Further, work completed by the NSTAC and NRIC reinforce this concept of communications having the status of a critical infrastructure; the telecommunications industry through NSTAC has been engaged in many issues involving dependencies. NSTAC has

convened task groups to address issues with the banking and finance sector, and are currently addressing issues with the power sector.

Service providers are often dependent upon services of others in the telecommunications sector or in other sectors. For instance, they have the option of leasing sections of a circuit from other service providers, where their network does not have the required footprint. An example is a circuit comprised of three different service providers designed to establish a complete end-to-end circuit for a customer; this circuit would have different Regional Bell Operating Companies (RBOC) on each end, and then a long distance provider in the middle (these types of relationships are governed by legal contracts). Another example of dependencies are the cellular antennae frequently mounted on water towers, power poles and other commercial structures owned and operated by other sectors. Clearly, providers realize the strong correlation and relationships among other sectors.

Industry and Government Work Activities in Critical Infrastructure Protection

Both the private telecommunications industry and the federal and state governments have sponsored activities to promote the reliability and resiliency within the communication sector. Many of these activities are not new activities as a result 9/11, but continuations of existing committees and forums. Examples include:

- The Federal Communications Commission (FCC) has sponsored the NRIC for more than a decade. NRIC is a partnership between the FCC and private industry to improve/maintain the network performance with respect to reliability, security, etc. To date, seven councils have been chartered with deliverables in various focus areas including network reliability, physical and cyber security, and emergency services. The products of the council are best practices that provide guidance to the industry.
- The NCS/NCC, another partnership between industry and government, has provided many programs to ensure telecommunications in times of national security and emergency preparedness. Programs include Government Emergency Telecommunications Service (GETS), Telecommunications Service Priority (TSP) Program, and Wireless Priority Service (WPS) coordinating functions.
- NSTAC provides the president with insight from private industry on issues related to implementing national security and emergency preparedness communications policy. Participants include top executives from the communications and information technology sectors, finance and aerospace.

Industry, through the standards process and forums, has also focused on critical infrastructure.

- The Alliance for Telecommunications Industry Solutions (ATIS) sponsors many committees focused on security, reliability, architecture and prioritization of standards work.
- The Internet Engineering Task Force (IETF) has similar programs and technical work completed and in progress targeting security, resiliency, etc.

Many more examples exist within the industry. Service providers, equipment and software vendors voluntarily implement the applicable practice or standard to their products or services depending on their situational requirements, risk management plans, and so forth. Further, these service providers and vendors use critical infrastructure processes on network architecture and services nationwide, including in the National Capital Region (NCR).

1.1.2 Definition

Telecommunications include “Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems. [National Telecommunication and Information Administration (NTIA)]; or “Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.”¹

1.1.3 Features

Composition of the telecommunications sector evolves continually due to technology advances, business and competitive pressures, and changes in the regulatory environment. Despite its dynamic nature, the sector has consistently provided robust and reliable communications and processes to meet the needs of businesses and government. In the new threat environment, the sector faces significant challenges to protect its vast and dispersed critical assets, both cyber and physical. Because the government and critical infrastructure industries rely heavily on the public telecommunications infrastructure for vital communications services, the sector’s risk mitigation initiatives are particularly important.

The telecommunications sector provides voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks. The collective public network provides switched circuits for telephone, data, and leased point-to-point services, and to other services as well. This sector consists of physical facilities, including switches, access tandems, and other equipment whose components are connected with fiber and copper cable. Importantly, these structures are the backbone of the infrastructure, with cellular, microwave, and satellite technologies providing extended gateways to the wire-line network for mobile users. In addition, supporting the underlying networks are operations, administration, maintenance, and provisioning systems, which provide the vital management and administrative functions: billing, accounting, configuration, and security management.

Advances in data network technology and the increasing demand for data services have spawned the rapid proliferation of the Internet infrastructure. The Internet consists of a global network of packet switched networks that use a common suite of protocols: Internet Service Providers (ISPs) provide end-users with access; larger ISPs use Network Operation Centers (NOC’s) to manage high capacity networks, linking them through Internet peering points or network access points; and smaller ISPs usually lease their long-haul transmission capacity from the larger ISPs and provide regional and local Internet access to end-users via the other service provider’s backbone. Further, Internet access providers interconnect with the PSTN through points of presence, typically a switch or a router, located at a service provider’s offices, and international service and Internet traffic travels underwater via cables that reach the United States at various cable landing points. In addition to the PSTN and the Internet, enterprise networks are also an important component of the telecommunications infrastructure. In particular, enterprise networks are dedicated networks supporting the voice and data needs and operations of large enterprises. These networks use a combination of leased lines or services from service or Internet providers.

1.2. Regional Sector Characteristics

1.2.1 Service Areas

The area of service for providers in the NCR includes local service providers, long distance providers, Internet service providers and wireless service providers. Some provide only local infrastructure and services while others extend internationally.

1.2.2 Companies, Employees, Customers

The sector is dominated by a handful of large firms such as Verizon, AT&T, MCI, Nextel, Sprint, and Cingular, etc.

Roughly 1100 establishments in the NCR fall within the category of communications as defined by the 2-digit Standard Industrial Classification (SIC) code 48.² This category includes all firms related to telephone communications and other message communications, cable and other pay television services, as well as other communications services not elsewhere classified. These establishments are scattered across the region although, some clusters are located along major transportation corridors.

In 2003, 196,890 persons were employed in the Information Technology sector of the NCR:³ 110,729 in Virginia, 59,164 in the Maryland and 26,997 in the District of Columbia. A more detailed breakdown of these figures by sub sector is available through the Bureau of Economic Analysis. The telecommunications sub sector employment in Virginia is 40,138, Maryland is 22,991, and the District of Columbia is 4,638.⁴

1.2.3 Capacity, Supply, Demand

In the NCR, 1617 fiberlit buildings are fairly evenly distributed throughout the region. A further breakdown includes 44 co-location facilities, 76 carrier points-of-presence (POP's), and 209 wired connection centers. Most of these facilities are located along the main transportation lines, many west of the District of Columbia and within the Dulles Corridor.⁵

The region has an abundance of fiber-optic cable: roughly 888 miles of regional fiber and 34,928 miles of long-haul cable. Like many other metropolitan regions, the NCR area has excess capacity.⁶

1.3 Review of Authorities

1.3.1 Statutes

The most significant legislation is the Telecommunications Act of 1996. (Telecommunications Act of 1996, Pub. LA. No. 104-104, 110 Stat. 56 (1996), superseding the Act of 1934). The purpose of the Act is to foster fair competition and innovation in the telecommunications sector. Section 256 *Coordination for Interconnection* “. . . mandates that the FCC put in place procedures to oversee coordinated network planning by telecommunications carriers and service providers and to participate in standard setting for this purpose.” Specific purposes are “. . . to promote nondiscriminatory accessibility by the broadest number of users and vendors of communications products and services to public telecommunications networks, and to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks.”

Legislation had two objectives: to facilitate competition in the sector by removing barriers to entry, and to encourage carriers and service providers to integrate their networks.

1.3.2 Regulations

Federal/State/District

Federal Communications Commission (FCC). The FCC is an independent government agency that regulates domestic and international communications by radio, television, wire, satellite and cable. Communication service providers report service disruptions to the FCC and to the state regulatory bodies. The requirements for the FCC outage reporting rules are contained in Part Four of the FCC rules; each state sets its own requirements. For the National Capital Region, Maryland Public Service Commission, Virginia Public Utilities Commission and Washington DC Public Service Commission, all would play a role and service providers would follow both federal and state required processes, as applicable.

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection

This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

1.3.3 Roles and Responsibilities

Multiple national organizations are involved in helping to secure the sector. The balance between the private sector and the government sector contributes to success. The federal government leads forums such as NRIC, while the industry leads other forums and standards bodies. Both industry and government have worked many of the risk management/vulnerability assessment issues in a cooperative environment. The following are examples of organizations for the communications sector with lead responsibility (for a complete list of all organizations, please refer to appendix F):

(NCS) was established by Executive Order (EO) 12472 as a federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spectrum of emergencies. Under the policy objectives stated in EO 12472 and National Security Decision Directive (NSDD) 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the government during any emergency.

In order to accomplish these responsibilities, the NCS must (among others):

- Increase survivability and interoperability of NS/EP telecommunications
- Provide connectivity augmentation for the public switched network (PSN)
- Develop a NS/EP telecommunications architecture responsive to current and future needs of the federal government
- Develop telecommunications technical and procedural standards
- Perform NS/EP telecommunications network performance analysis
- Develop emergency operations training and exercises
- Develop and manage NS/EP automated systems and capabilities

The organization is comprised of 23 federal departments and agencies, and it interfaces with industry through its involvement with NSTAC, NCC and the NCC's Telecommunications Information Sharing and Analysis Center (ISAC).

NRIC: This council provides recommendations to the FCC and to the communications industry that, if implemented, will under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wire line, satellite, cable, and public data networks. This includes facilitating the reliability, robustness, security, and interoperability of communications networks including emergency communications networks. The scope of this activity also encompasses recommendations that will ensure the security and sustainability of communications networks throughout the United States; ensure the availability of adequate communications capacity during events or periods of exceptional stress due to natural disasters, terrorist attacks or similar occurrences; and facilitate the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of communications services. The council addresses such topics as Emergency Communications Networks, homeland security best practices, best practices for wireless and public data network services, and broadband.⁷ NRIC and other industry forums have over the years developed 801 best practices (refer to Appendix E for additional information).

NCC: The NCC was created at divestiture for National Security and Emergency Preparedness (NS/EP). The center has been in service for the government and the communications sector for more than twenty years. The NCC's capabilities include the Communications Resource Information Sharing (CRIS) initiative, the Government Emergency Telecommunications Service (GETS), the Shared Resources (SHARES) High Frequency (HF) Radio Program and the Telecommunications Service Priority (TSP). The CRIS initiative is a database of assets, services and capabilities of federal government telecommunications systems available to all government agencies to aid in NS/EP efforts. The GETS, SHARES and TSP programs are set up to ensure that appropriate personnel at the local, state and national level can communicate effectively in emergency situations: GETS does this with the provision of a nationwide NS/EP switched voice and voice band data communications service; SHARES, through the consolidation of HF radio resources and the TSP Program, provides priority restoration and provisioning of NS/EP telecommunications services. Last, the Wireless Priority Service (WPS) came about post 9/11 (For additional information on the NCC, refer to Appendix C).

Media Security and Reliability Council: This council gives members of the broadcast and multi-channel video programming distribution (MVPD) industries the opportunity to provide recommendations to the FCC and their industries that, when implemented, will assure optimal reliability, robustness and security of broadcast and MVPD facilities. These recommendations are based on, among other things, homeland defense and security considerations, and take into account all reasonably foreseeable circumstances to: ensure the security and sustainability of broadcast and MVPD facilities throughout the United States; ensure the availability of adequate transmission capability during events or periods of exceptional stress due to natural disasters, man-made attacks or similar occurrences; and to facilitate the rapid restoration of broadcast and MVPD services in the event of widespread or major disruptions. The committee addresses such topics as security, restoration, reliability, as well as other topics.⁸

NSTAC: President Ronald Reagan created the NSTAC by Executive Order 12382 in September 1982. This organization has up to 30 industry chief executives who represent the major communications and network service providers and information technology, finance, and

aerospace companies. Moreover, the NSTAC provides industry-based advice and expertise to the president on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

Three accomplishments best illustrate NSTAC's capabilities to address NS/EP communications issues in today's environment: the establishment of the NCC and its ISAC; the implementation of the government and NSTAC National Security and Information Exchange (NSIE) process; and the examination of the NS/EP implications of Internet technologies and the vulnerabilities of converged networks.¹

NCC's Telecom ISAC: The National Coordinating Center for Telecom and its Telecom Information Sharing and Analysis Center (NCC Telecom ISAC), has an operational responsibility as a joint public sector/private sector body to respond to all hazards that can affect the telecommunications infrastructure in the USA. It is a partnership of industry and government. Currently, there are 32 industry members, including three associations, and 23 federal agencies. In addition, the sector has three sector coordinator organizations that are also members of the NCC Telecom ISAC to extend the reach of the ISAC and to cover other non-operational issues affecting the sector. Those sector coordinator organizations under Presidential Decision Directive 63 (PDD-63)/Homeland Security Presidential Directive 7 (HSPD-7) are the Cellular Telecommunications and Internet Association (CTIA), the Telecommunications Industry Association (TIA), and the United States Telecom Association (USTA). Both the sector coordinators and the NCC Telecom ISAC (including individual members as appropriate) coordinate with other sectors via the ISAC Council, the Partnership for Critical Infrastructure Security (PCIS), or the American National Standards Institute Homeland Security Standards Panel (ANSI HSSP), or all three.

The **Network Reliability Steering Committee (NRSC)** was formed to monitor network reliability utilizing the information contained in major outage reports filed with the FCC. The committee's mission is to analyze the industry's reporting of network outages to identify trends, make recommendations aimed at improving network reliability, and to make the results publicly available, in order to help ensure a continued high level of network reliability. It has been supported by industry for more a decade.

The NRSC has produced reviews of the major outages reported to the FCC since 1991-92. Moreover, it provides guidance to the industry with respect to the state of reliability of the network and offered best practices and procedures to maintain or improve reliability.

In addition, the NRSC has commissioned study groups for particular areas of interest where it has seen rising trends and special requests: The following are a few examples:

- The Power Outage study group
- The Northeast Blackout Power Outages Study Group Report
- The Timing Study Group

For instance, the Northeast Blackout Power Outages Study Group reviewed in detail all the outages reported to the FCC as a result of the blackout in 2003. Each report was reviewed for direct cause, root cause and other contributing factors. The team had four major recommendations. The first two addressed the NRSC data handling procedures, and the other

two addressed best practices. Of the best practices, the NRSC reminded the industry of three pertinent “power” best practices:

1. 6-6-1028 Routine Maintenance/Testing
2. 6-5-0662 Full Load Testing
3. 6-5-0658 Redundant Fuel Systems

The NRSC also developed a new best practice for industry guidance:

Service providers, network operators and property managers with buildings serviced by more than one emergency generator, should design, install, and maintain each generator as a stand-alone unit that is not dependent on the operation of another generator for proper functioning, including fuel source (See appendix J for the link to the NRSC).

1.4 Mapping of Interdependencies

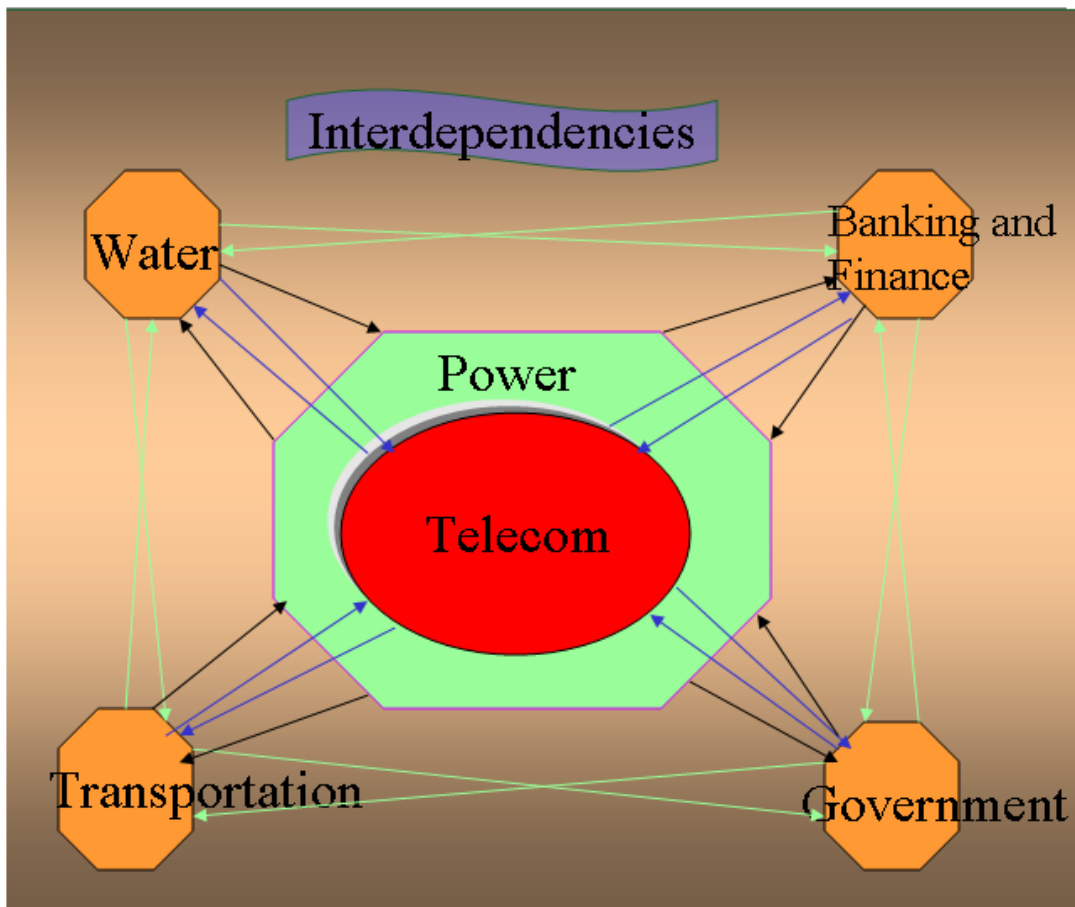


Figure 1: Mapping Relationships

Note: Figure 1 is not meant to imply one sector is more important or more of a key factor than others. Although power is a key element for telecommunications, the graphic simply displays relationships from the telecommunications viewpoint.

Also worth noting is that power is key to the long-term survivability of the communications sector as well as to the other sectors. For instance, service providers plan their networks with back-up power generation based on business continuity principles. This is time sensitive: back-up power can be engineered to last 6-8 hours; other back up power systems can last as long as fuel supply exists. Consequently, in the event of a widespread outage, lasting for extended periods, lack of power to all sectors, including banking and finance, would be a factor.

1.4.1 Upstream sectors

The telecommunications sector depends heavily on energy for operation of its public voice/data network. Many public telecommunications carriers have batteries or back-up generators in place to be activated in the event of a power outage. Lengthy power outages require refueling of the back up generators hence, refueling can be problematic if transportation is disrupted or access into the site location is restricted.

The sector also relies on having access to its infrastructure in the event that there are restoration/repair needs. During Hurricane Isabel, there was evidence that repair efforts were hampered by flooded roads and bridges, and downed trees and poles. Hurricane Katrina, also, made access to affected locations problematic. For example, the flooding in New Orleans and the security issues did not allow responders to complete their assignments with dispatch.

The availability of water is also important to the operation of the communications networks. For instance, cooling is vital for sector operability; electronic equipment requires certain temperature/humidity parameters to run efficiently; power can affect the HVAC systems along with lack of clean water; and availability of cash/funding arrangements can be a factor in widespread outages.

Table 1: Upstream Sectors

Sector	Comments/Potential Effects
Power	<ul style="list-style-type: none"> • Power is required to keep the network equipment operational. • Back-up power is engineered to service provider specifications, however, if long-term power outage occurs and there is no return of commercial power, equipment failures can occur.
Transportation	<ul style="list-style-type: none"> • Transportation is essential to the distribution channel for equipment and supplies. • System maintenance/repair. • If new equipment is required for replacement during an incident/disaster, the vendor/provider of the equipment must have transportation available to deliver the new equipment to the disaster site. • Delivery of fuel for back-up power.

Water	<ul style="list-style-type: none"> • Water is required to keep electronic equipment functioning efficiently. Temperature and humidity parameters are important to long-term viability of the equipment. • Heating, ventilation, air conditioning (HVAC) functions.
Emergency Services	<ul style="list-style-type: none"> • During a disaster, access to the site is fundamental to restoration of service. • Response for fire and other emergencies.
Banking and Finance	<ul style="list-style-type: none"> • Access to cash could be required; cash would be required for gas for technician’s personnel vehicles, company trucks, etc. • Other financial transactions such as funds transfer

1.4.2 Downstream sectors

Telecommunications infrastructure and the services provided in this sector support functions in all other critical infrastructure sectors. Two sectors whose critical functions depend on this infrastructure include banking and finance, and transportation.

Banking and Finance

The financial services sector identifies telecommunications infrastructure as a critical component of the systems it uses to carry out functions related to the sector such as payment, settlement and clearance. This sector, in cooperation with the telecommunications sector, has already adopted a number of “best practices” to help assure resiliency in the communications networks that are used in the sector.

Transportation

Telecommunications and other advanced technologies have become an important element of all types of transportation systems for operations, management and control functions. – transportation systems that use these technologies are called Intelligent Transportation Systems. Concepts such as “smart roads,” would communicate to travel management centers and, in real time, to travelers of instances of congestion and accidents that would affect travel. . In addition, “smart travelers,” where route guidance, ridesharing, and transit information will be available to commuters in kiosks and on-line information systems, reflect how intelligence is located in the transportation system using telecommunications.

The freight industry has become increasingly reliant on telecommunications and computer systems for its day-to-day operations, and terrorists could exploit this situation by carrying out a cyber attack. With that in mind, computers are used to link information systems for carriers, shippers and manufacturers within and across transportation sectors. Further, the Internet is used as a vehicle for communication, and other technologies such as Radio Frequency Identification (RFID) tags, E-sensors, and wireless communications are also used for various purposes. Possible threat scenarios include hacking into an information system to identify and track shipments of dangerous materials, or perhaps a “denial of service attack” or other cyber attack to shut down the command thereby controlling the system; or a cyber attack to tamper with

information on particular shipments (e.g., disguising a shipment to make it appear that it is not hazardous) so that it could more easily be hijacked.

1.4.3 Sidestream sectors – e.g. regulators, competitors, consumers

During a widespread outage, whether physical, cyber or weather related, all users of communications could potentially be affected, although this would depend on the nature of the incident and the risk mitigation planned in the service provider's networks.

The FCC, which is the regulatory body for telecommunications service providers, participates with the NCS/NCC and, in addition, has an outage reporting process in place that requires service providers to notify the commission within certain parameters.

The communications industry sector is dependent on each other and its competitors. For example, local access for a long distance carrier could be provided by a Regional Bell Operating Committee (RBOC), or the reverse. For service to be reliable, all sections/components of the circuit must be active and must meet certain parameters for quality of service. Thus, a wireless service provider might choose to lease backbone service from a long-haul provider. Such arrangements are governed by contractual arrangements between the two service providers.

Similarly, the Internet has these same arrangements. Hence, an ISP may choose to lease backbone or other services provided to complete the network architecture for its customers. The Internet has a wide variety of small, medium and large networks that all interconnect in different degrees (Figure 2) See Appendix D for a detailed discussion on Internet interdependence.

As a result of these interdependencies, consumers, small businesses, etc, should assess their risk and criticality of their processes, and then take action to remediate these risks based on their specific needs. Questions to consider include: Does the consumer feel the need to have a firewall for his home computer? Or, is a back-up generator required (if online communication is deemed by the end user), as a critical function for the household or small business? Normally, large private enterprises utilize risk management principles to address their critical services. Meanwhile, there is a variety of information available to perform risk assessment analytics for end users, as well as small and large businesses.

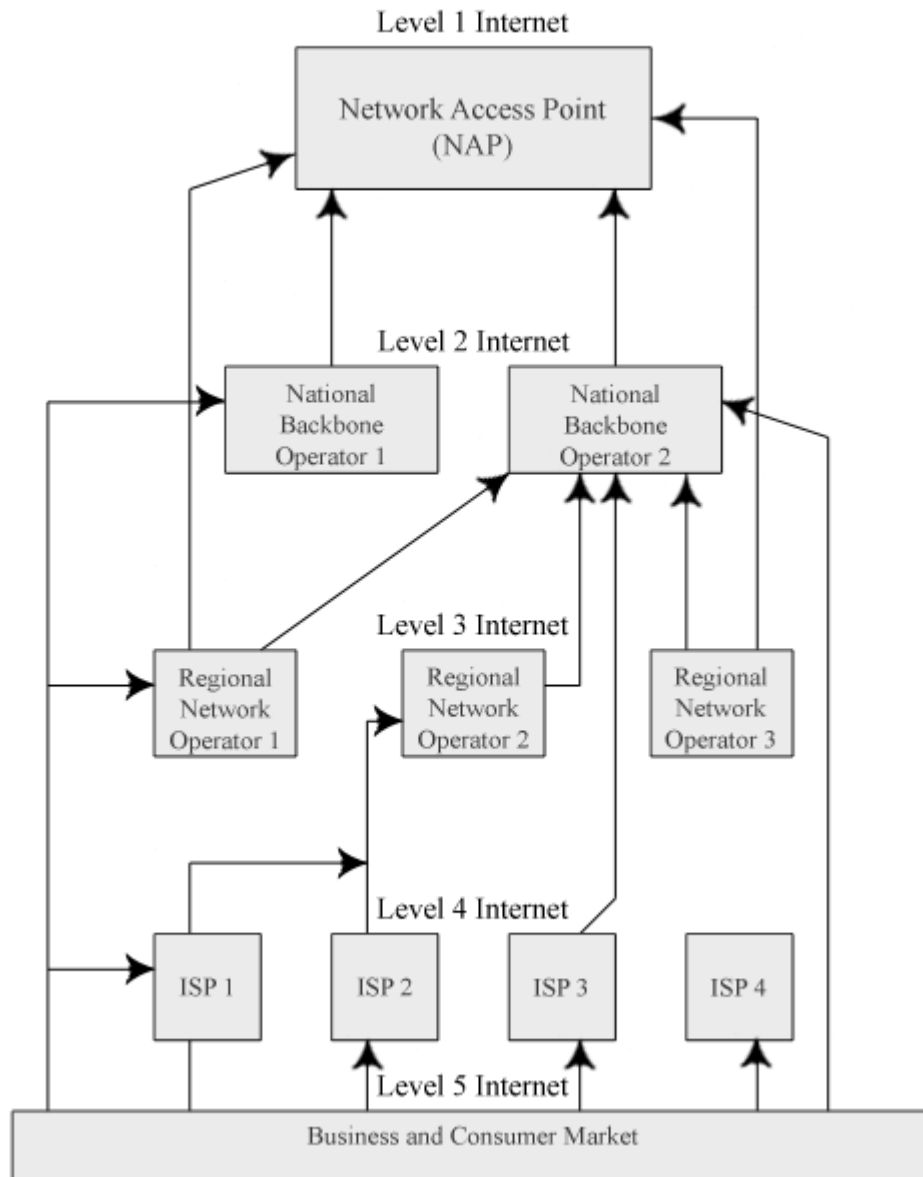


Figure 2. Internet Network Levels Diagram

(Source: Adapted from Boardwatch 1998)

1.4.4 Other Dependencies – e.g. co-locations, rights-of-way

The telecommunications infrastructure has evolved over time. This infrastructure depends on access to land, water, structures, etc. Local authorities, such as municipalities, oversee the permit process for new construction of basic cable infrastructure. Yet, the rules of entry to the Right of Way (ROW), construction of new ROW, or cable ducting can be problematic to the communications sector as network enhancements are planned. For example, local rules can

enforce certain processes such as no access to a geographic area/rights of way/duct work, except during specified times of the year. There was a time when a ROW was dedicated to one utility or sector such as power; now the ROW serves more than one sector.

Another dependency, fiber optic cable, often shares the same right-of-way as roads, pipeline and power lines indicating one example of a correlation between the sectors, although not an interdependency in its strictest sense. Proximity may result in damage to one sector thereby involving the rest of those in the right of way. Fortunately, the Common Ground Alliance (CGA) establishes best practices for all those constituents in the right of ways or adjacent areas.

Besides right of way issues, another common infrastructure issue is accidental cable breaks, which account for a large percentage of cable “dig ups,” according to the NRSC quarterly and annual reports. Many of these cable breaks occur from lack of notice by the excavator to the owner of the facility prior to digging. Accordingly, all states have damage prevention laws requiring notification, and centers in place to receive the calls (known as the One Call System (OCS)). This notification mandate is essential in continuing to improve this issue; The OCS is now within the umbrella of the CGA.

2. State of Security Assessment

2.1 Assessment of Status and application of Critical Infrastructure Vulnerability Assessment/Risk Management (CIVA/RM) in Sector

All service providers, vendors, or other infrastructure providers evaluate the set of practices, standards, business policies, rules, etc. to determine which are applicable to their networks/environments. This assessment is based on each service provider’s/vendor’s environment and criteria for selection. Included in the decision process are such principles as Business Continuity/Risk Management, along with entity-specific criteria. Each service provider/vendor has unique architectures, software, etc., and therefore, a universal mandate or application is not appropriate. Indeed, in a market driven sector, reliable infrastructure is vital to continuity of business. For additional information and examples of some of the tools, procedures, processes, and best practices, refer to appendix E.

The communications industry uses a variety of tools including best practices, standards, business processes, certification processes, external environmental data, and auditing, to name some; service providers and vendors evaluate all the tools available to them.

2.1.1 Awareness of Value of CIP and CIVA/RM

The literature review/data gathering and the focus team, (communications service providers, industry associations, and government were represented), provided evidence of active involvement by industry and government in critical infrastructure protection (CIP) programs. The government has either sponsored or is currently sponsoring forums for private industry and the government to work through some common issues. Examples include the NSTAC, NRIC, and the NCC. In addition, private industry has also invested resources on its own to review and develop new standards, as well as those business processes mentioned above.

On the focus teams, service providers represented risk management/business continuity principles as a process inherent to their respective businesses. These principles are important to this industry because stable and reliable infrastructure is a key attribute to successful business for the communications sector. Therefore, these processes were established and incorporated into business plans and operations long before 9/11. Accordingly, the aftermath of 9/11 increased

activities and assessments related to risk management/business continuity models, thereby overlaying terrorist threat modes into risk assessment/business continuity systems.

Regarding industry standards, telecommunications uses voluntary consensus standards. Internationally, a few examples are the International Telecommunications Union (ITU); International Electrotechnical Committee (IEC); International Organization for Standardization (ISO); Internet Engineering Task Force (IETF); American National Standards Institute (ANSI); and International Electric and Electronic Engineering (IEEE). Nationally, the standards of Telecommunications Industry Association (TIA) and the Alliance for Telecommunications Industry Solutions (ATIS) are the widely used, along with best practices from NRIC. There are also many other standards bodies which are utilized by the industry.

While some government regulations reference standards, the National Technology Transfer and Advancement Act (NTTAA) and Office of Management and Budget Circular A-119 require federal agencies to use voluntary consensus standards whenever practical for both agency mission (for regulation purposes, for example) as well as procurement activities. Further, agencies and NCC Telecom ISAC industry members are encouraged to participate in the standards development process. With regard to federal agencies, such as the Department of Homeland Security (DHS), this US law and policy direct federal agencies to use non-government standards wherever appropriate and feasible, in lieu of developing government-specific standards. Therefore, the government looks to all available standards to meet stated needs, at the international level as well as other levels. Some homeland security standards work, such as that in the biometrics field, which is already being conducted in ISO. On the other hand, there will be areas where a unique national need is identified and where standards development work is concentrated at the national level. Likewise, there will be areas where specific standards will need to be developed by government agencies, particularly where classified information is involved. Wherever feasible, however, the US government will look for one standards solution. Consequently, one of the first activities by American National Standards Institute's (ANSI) Homeland Security Standards Panel was to identify the range of standards in existence or under preparation that might be applicable to US homeland security. These include ISO standards, as well as many others. ANSI is currently developing a comprehensive database of standards for DHS reference. Importantly, NCC Telecom ISAC members, including companies, organizations and agencies, participate in and/or support all the standards groups listed previously.

2.2 Availability of Appropriate Tools

2.2.1 Vulnerability Assessments

As noted in section 2.1 above, service providers, vendors, etc., evaluate the set of practices, standards, business policies, and rules and determine which are applicable to their networks/environments. This is based on each service provider's/vendors environment and criteria for selection. Principles such as business continuity/risk management, along with entity-specific criteria, are part of the decision process. Because each service provider/vendor has unique architectures, software, etc., a universal mandate or application is not appropriate. In a market driven sector, reliable infrastructure is vital to continuity of business.

In order for service providers/vendors to keep abreast of the latest technology, practices, and standards, and developments, they participate in such forums as NRIC, the standards bodies, and the Telecom Information Sharing and Analysis Center.

The following three initiatives demonstrate that the telecom sector has been proactive in developing measures toward security excellence (Refer to Appendix E for additional details).

1. NRIC Best Practices
2. National Security Telecommunications Advisory Committee (NSTAC) Reports
3. Media Security and Reliability Council (MSRC) Adopted Best Practices Recommendations

The tools, best practices, and standards that the telecommunications industry utilizes for risk mitigation can be categorized into four areas of the Continuum of Vulnerability Assessment and Risk Management model: 1) Broad and Qualitative, 2) Detailed Specific, 3) Relative Risk and 4) Absolute Risk. The first two are more operational planning; the last two are more strategically focused. The chart below explains where tools, standards, best practices, and risk programs would be placed in the Vulnerability Assessment and Risk Management model:

Broad, Qualitative	Detailed Specific Checklists, questions, and directions or standards	Relative Risk estimates of index values of criticality, threat, vulnerability and consequences	Absolute Risk Methods estimates actual values of criticality, threat, vulnerability, etc. Value for risk-reduction programs: absolute worth
<p>Examples</p> <ul style="list-style-type: none"> -Directional statements, such as -have back-up power plans -provide redundancy 	<p>Examples</p> <ul style="list-style-type: none"> -Best practices, standards such as those produced by ATIS, IEC, NRIC, etc. -TL9000 	<p>Examples</p> <ul style="list-style-type: none"> -Risk mitigation planning -Completion on business continuity plans utilizing prioritization of sites, recoverability ability, etc. 	<p>Examples</p> <ul style="list-style-type: none"> -Business continuity plans completed with attributes to include such items as revenue loss, resulting in implementation plans -Disaster Recovery Teams -HAZMAT teams

Table 2: Continuum of Vulnerability Assessment and Risk Management Model

2.2.2 Compliance-oriented policies and procedures

Each network operator within the sector has its own responsibilities to protect, operate, maintain, and restore network functions. With more than a hundred years of experience, professionalism, and technology growth, the telecom infrastructure in the US is one of the more reliable in the world; results from ongoing measurement data demonstrate a capacity to increase telecommunications traffic, but with more reliable results each year. Specifically, the telecom infrastructure has FCC-mandated outage reporting rules as well as voluntary reporting processes, which track the reliability of the sector’s infrastructure.

In addition to individual company roles and responsibilities, there are also bilateral and multi-lateral efforts for emergency operations via the NCC Telecom ISAC and mutual aid agreements between and among the network operators. Moreover, the sector has an FCC-approved Telecommunications Service Priority System to ensure that critical NSEP circuits can be provisioned and restored on a priority basis. Still, other sector programs, such as the Government Emergency Telecommunications System (GETS) and Wireless Priority Service (WPS), are useful during emergency or other crisis situations.

The telecom sector uses tools/processes/procedures matched to the task and type of equipment or infrastructure being evaluated. In particular, there are best practices recommended and are used for vulnerability assessments and risk management within the sector. As indicated in the NCC Telecom ISAC response to the International Organization for Standardization Advisory Group for Security (ISO/AGS), such assessments are always in progress, and they are always being updated because threats change. Finally, members of the NCC Telecom ISAC have conducted vulnerability and security risk analysis.

2.2.3 Risk management

Risk management is performed within both the companies and the sector via joint activities of the NCC Telecom ISAC, and also within the NSTAC's National Security and Information Exchange (NSIE). Further, individual service providers perform risk assessment/business continuity processes. Relevant exercises and review of results after real-world events contribute to the constant improvement within the sector. Hence, risk management and vulnerability assessments are ongoing because threats are ongoing and ever-changing.

Within the Telecommunications Service Priority systems (TSP), there are well-defined criteria to identify critical NS/EP facilities. In addition, operators can determine specifically which of their facilities are critical in order to operate and maintain their networks. Moreover, there is dialogue with federal, state, and local authorities, as well as key customers, about additional critical facilities that do not have TSP treatment. The sector and NCC Telecom ISAC prepare and train for an "all hazards" environment because often times, natural disasters can have a larger impact on network infrastructure than any man-made occurrence.

To evaluate vulnerabilities, the sector uses a variety of risk management tools and best practices. In addition, parts of the sector are regulated at the federal level and by 51 states and local public service commissions, who also often impose regulatory and reporting requirements.

Because the sector has dealt with many extreme and unpredictable events over the last 100 years, it has developed the expertise, tools, technology, processes and training to prevent or mitigate failures. Examples of preparedness include back-up power, span switching and auto-rerouting of critical circuits, fiber rings, auto-healing network elements, alarm systems, and best practices.

2.3 Extent of application of appropriate tools through resource allocation

The application of best practices initiatives that limit the probability of occurrences, and also limit duration or severity, are determined by each network operator. Therefore, the communications sector has assessed and applied applicable tools to its network architecture or business processes, as defined by the risk assessment/business continuity plans/models. The application of appropriate tools through resource allocation is done via company internal programs or as part of an industry coordinated effort by the NCC Telecom ISAC or other exercise programs including for example, a TOPOFF.

Many factors support the application of tools within the business model. Examples include:

- TSP for provisioning and restoration priorities.
- Engineered grades of service and with Service Level Agreements (SLA's) that specify the expected or engineered grades of service.
- Redundancy/resiliency attributes.
 - Standards.
 - Return on Investment (ROI) metrics.

Service to customers, including government customers, and support for homeland security and NSEP are part of the fabric and traditions of this sector. But, in addition to providing one of the more resilient and reliable networks in the world, private sector owners must also ensure a reasonable return to those shareholders who invest in these private sector companies.

2.4 Extent of implementation of CIP measures

The list of best practices, initiatives, and standards recommended for use/guidance within the sector is extensive. Examples of CIP guidance to the industry include:

- NRIC Best Practices
- NSTAC guidance
- NRSC quarterly and annual reports
- Sarbanes Oxley
- ISO 17799
- ISO 9000 Series/standard (supplemented by Threat-level Homeland Security Advisory System) – MatchNSIE guidance
- Defense Conditions (DEFCON)
- California privacy standards
- Gramm-Leach-Bliley Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Other government and internal industry guidelines (e.g., customer, internal best practices, etc.) are evaluated and determined which are most appropriate
- Others: TIA, ITU, IEC, JTC-1, IETF, IEEE, ATIS (standards groups)
- Customer-driven requirements

Service providers and vendors integrate the tools and practices as applicable to their environment. The sector has plans for action, as required, including

- Loss of power and other contingencies
- Mutual aid agreements
- Dispersed critical response organizations across the nation (geographic diversity)
- Alternate Emergency Operations Centers (EOC)/Network Operations Centers (NOC) as well as primary
- Planned diversity, flexibility, and experience: supplemented by testing/drills
- Sector testing and responding (planned with scenarios), training
- Command and control processes for incident response, such as allocation of resources for technical support, and on-site support

Experience in planning, and operating during incident management sessions has helped the communications sector immensely. Specifically, there are set ways to respond; staff are trained and therefore, work efficiently, and thus allocate resources. If an incident occurs, resources are quickly and appropriately applied. For example, Cells on Wheels (COW's) was used to obtain greater capacity after 9/11. Also, resources are applied in the preventive stage, and network engineers plan for back-ups, generators, batteries, redundancy, etc. This risk-based approach for resiliency and return on investment (ROI) may differ across the sector, but NSEP perspective is a driver for all parts of the sector.

2.5 Extent of evaluation of CIP effectiveness

Evaluation initiatives are ongoing in the industry. With the FCC Outage reporting rules, along with NCC Telecom ISAC, NSIE, NRIC processes and follow-ups, and NRSC reports, constant evaluation for effectiveness and enhancement at the industry level occur.

Also, the NRSC evaluates the major outage reports sent to the FCC by the service providers, and results are published quarterly. Rigorous analysis and consistency of approach have been status quo for more than 10 years. Thus, statistical process control is used extensively; third party statisticians are funded to complete the analysis annually, thereby eliminating any corporation influence over the product.

At the individual service provider and vendor level, continual evaluations occur as a result of the incident management process. Accordingly, root cause analysis defining direct and root cause, improvements, and process failure mode analysis are all part of the operational business process. Consequently, changes are incorporated or processes reinforced as part of this quality performance cycle. Also important, companies have regular, evolving processes to identify threats, and vulnerabilities/risks in a planned way. Because exercise is equally important, service providers participate in recovery plans, such as disaster recovery and HAZMAT drills; and incident management is constantly being exercised, whether planned or actual.

The NRSC's quarterly reports provide a industry evaluation process. Industry participation at NRIC has included periodic surveys on the use of best practices, cost of best practice implementation, etc. within the sector. Likewise, Sarbanes Oxley is an external audit process. In addition to these evaluations and audit processes, network engineers evaluate network footprints with new capacity augments/infrastructure upgrades.

3. Risk Reduction Programs and Processes

Considerations for future work (below) incorporate the recommendations and comments from NCC focus group members and this team. These recommendations are actionable and should be completed for further process improvement; yet the recommendations require cooperation from both the government and telecommunications sectors, along with the NCR.

3.1 Risk Reduction Project/Investment Recommendations

The successes, to date, within the telecommunications sector comes from the ability of the private and government sectors to join together to solve common CIP issues. NSTAC and NRIC are two examples of this process. Fostering a continued partnership between the government sector and the telecommunications industry in order to resolve common issues is a critical component to future successes.

3.1.1 Tactical Steps for Immediate Benefit on the Ground

The following are tactical steps recommended:

- Develop a credentialing process for incidents and planned events that would be of immediate benefit to the communications sector
- Create a single Point of Contact (POC) for perimeter control process and, once established, maintain the rules; eliminate the need to change the process during the incident or function
- Develop a methodology to have one source for requests to the telecommunications sector in connection with studies, evaluations, tabletops, etc.: not 50 states, multiple counties and cities, and including the NCR. Creating a process to coordinate and prioritize requests to the communications sector for studies, exercises, drills, etc., from all levels of the government, is equally beneficial for all parties both private and government.
- Have FEMA abide by the National Response Plan – which has a single POC for the sector during an event

3.1.2 Strategic Steps for Long-Term Benefit on the Ground

For longer term and forward-looking work, the need exists to determine the best way to fund risk management mandated work activities as required by government organizations. For this reason, a study should be commissioned to decide the best way to proceed for the benefit of private industry and the government sector.

- Conduct a study to determine ways to finance security improvement or cost recovery and provide recommendations

3.2 Risk Reduction Process Improvements

As evidenced by the research and focus group, the communications sector has numerous tools and processes to maintain/and or to advance CIP. Tools exist at the industry level, such as the NRSC, for private industry to monitor networks and to provide guidance to the industry on specific best practices or technical knowledge. In particular, the NRIC has provided a wealth of best practices and standards bodies. And the NCC has worked the technical issues of CIP and continues to work new areas of technology demands. Both the private and government sectors have worked proactively to maintain or to improve the CIP profile of this sector. Hence, mutual participation from both parties, along with their continued support needs to continue for the success of the sector.

3.2.1 Recommendations for enhancements in general guidelines and best practice compliance standards

The communications sector process for standards (which is voluntary) is based on consensus. Therefore, Standards Development Organizations (SDO) adhere to the rules or the SDO loses the American National Standards Institute's accreditation. The best practices are based on industry experts who share procedures and practices that have a proven track record within their enterprise. For the past 10 years, the communications industry has contributed, and continues to contribute to the NRIC best practices. Indeed, those who participate in either of the processes mentioned bring a wealth of knowledge and experience, contributed voluntarily, for the improvement of the telecommunications platform. All communities with a stake in critical infrastructure improvement should continue to foster the voluntary contributions of time and resources.

3.2.2. Recommendations for enhancements in risk management (specifically, threat, vulnerability, consequences, risk-reducing initiatives, resource allocation/financing, and decision making)

In the post 9/11 environment, threat mode analysis based on vulnerability, risk mitigation., are new constants in process planning for both the private and public sectors. The following recommendations support the continuing the information exchange, critical to successful sector plans and incident command:

- Continue to officially recognize the NCC/NCS/Telecom ISAC as the source of contact for the communications sector; recommend that more of the non-traditional communications players, such as cable and ISPs participate in the center for better synergy. This trusted organization has the ability to reach senior ranks of the service providers and vendors when required, to reach out to other sectors, and to provide for the NS/EP services for the nation. The continuity of this center and its longevity is a major factor for the success of the CIP programs in the sector. Therefore, maintaining the center should be a priority at all times.
- Continue the federal government's feedback and threat information that is useful to the sector for response and mitigation when working with communications service providers..
- Incorporate the communications sector as full participants with the government sector, for the NSSE process. The NSSE is a special process for significant events that require special handling, many of which happen in the NCR, such as the presidential inauguration.

3.3. Specific recommendations for governance at sector-level

3.3.1 Incentives

The NCS/NCC is recognized by most communications sectors as the point of coordination for all issues of national importance. As noted earlier, participants at the NCS/NCC cover a vast majority of the service providers, vendors and industry associations for the nation. NCC members and this team recommend that the NCR participate fully by having representation in the NCS/NCC for communications sector critical requirements. To achieve this, the first step may be to educate the NCR concerning the role of the NSC/NCC and how the participants/members operate at the center and within their respective organizations. Therefore, a single point of contact from the NCR would be optimal.

Following are informal comments provided by focus team members:

- "There is a process for the Telecom ISAC. The National Response Plan/Federal Emergency Management Agency process exists but lacks industry representation."
- "Post 9/11, the use of the Telecom ISAC's has been beneficial. Although it can be problematic, since ISAC's do not resolve all National Response Plan issues, note however that the Energy ISAC did provide information during the blackout of 2003."
- "The Federal Emergency Management Agency process was most useful during the blackout regarding petroleum needs."
- "In sum, any integration of processes could be via the Telecom ISAC or the National Response Plan/Federal Emergency Management Agency functions."
- "In the longer-term, further integration might be needed for efficiency."

The industry participates in many of the forums, including SDO's, as discussed earlier. Maintaining the infrastructure, whether for physical buildings or access to buildings, or hardware

and software of the networks, takes an enormous amount of effort to stay current. With such a competitive market, having a reliable network that will meet customer requirements is a major factor in all decisions to build or maintain the network. Therefore, the incentive to participate is there for the service providers and vendors as evidenced by their continued funding of the SDO's and the NCC, to name a few.

3.3.2 Organization and Management (e.g. accreditation, enforcement)

The communications sector has voluntarily participated in numerous forums, committees, SDO's, and ad hoc committees. This industry believes in self regulation and supports its stand through participation in such technical committees as NRIC, NRSC, and NCC up to and including funding for such work.

3.4 Specific recommendations addressing dependencies

3.4.1 Intra-sectoral

During 9/11 and the days afterward, the NCC provided coordination between the carriers to accomplish service restoration. Not only was the NCC working to find available sources of equipment, cable, etc., for national services, the executives and managers throughout each corporation, along with the vendors, were communicating needs/requirements to each other. Consequently, the continued existence of the NCS/NCC as it functions today is important to the industry and the government, and should continue to be supported by both sectors. This trusted organization has accomplished significant strides in CIP and NSEP.

In addition, the communications sector has a record of mutual aid. Hurricanes, blizzards, etc., put a strain on the resources of the affected service providers. Yet, service providers have supported each other whether in ad hoc mutual aid (one carrier providing equipment or associates, or vendors providing equipment) or in formal mutual aid agreements. Recently, service providers completed a formal mutual aid agreement during the last NRIC cycle for use when required.

3.4.2 Inter-sectoral

Each enterprise of each sector depends on others to some extent. This reliance on other infrastructures comes in varying degrees and for different purposes (e.g., electric power is a simple example). Further, the creation of the Telecom ISAC/Sector structure is evidence of this dependency. Keeping the NCS/NCC Telecom ISAC at the forefront of the intra-sectoral activities is vital to the communications sector. With its years of experience managing incident response and policy, the NCS/NCC Telecom ISAC can be useful when shared with the other sectors. Finally, the NCS/NCC Telecom ISAC has the confidence of the communications sector because of its longevity in the center and the trust from those within the center.

In addition, the focus team members offered the following recommendations for improvements to processes:

- FEMA must abide by the National Response Plan – which has a single POC for the sector during an event.
- Government agencies look to NCC as a single point of contact to the communications sector: the NCC wants a single POC as well from the government sector.

- Often, sector officials are on scene during an emergency, performing first-responder-related functions (e.g., behind fire, etc. to restore).
- During mitigation and repair, the communications sector needs to have access via a credentialing process to the site location. Although we do not meet first responder definition, and we potentially might have people in harms way, access to the site is often a long and changing process. A need exists for flexibility as select officials often require on location assessments during early phases (mostly once mitigation phase starts).
- Some argue that we need a single process for credentialing – the communications sector can consider an ad hoc validation process as long as it quickly integrates.
- The communications sector relies on local Emergency Operation Centers (EOC's) to provide support – e.g., lack of a credentialing process inhibits quick and efficient restoration and response.
- Others argue that we need a standardized and recognized process the NRP, with perimeter control, whether for building or a whole state; there needs to be a single, standard set of rules that any authority in control of the perimeter can follow.
- Privacy rules are mitigated against cards. Perhaps in response to these concerns, HSPD-12 is limited to government. The communications sector is sensitive to this issue; however, it is willing to provide whatever asked for to get credentialing rights and authorization. Telecom is a critical industry and will work with whatever process is chosen.
- Recognition of communications as an important link between first responders' ability to do the job (resilience of communications).
- A need exists for a single POC for perimeter control during an event, and adherence to the rules/process throughout the event (rules should not change) –stakeholders need to be educated on Critical Infrastructure Protection (CIP) roles and emergency operations. For instance, sometimes the communications sector is out at the incident/event as a first responder. NRIC is dealing with the issue of emergency responders and the sector is participating in:
 - The NCC/NCS and/or the Telecom ISAC are a coordinating point for telecommunications. As with the Blackout of 2003, the NCC/NCS got the power sector to the table to relay relevant information about the expected length of the repair cycle, such as which cities were being prioritized first, etc. This was very helpful to the communications sector for resource allocation, etc.
 - The NCC/NCS/Telecom ISAC should continue to be charged with formalizing the relationships with the other sectors.

3.4.3 Regional

- The NCS/NCC is an established well recognized fully functioning center for coordination among the communications providers, vendors, etc. Hence, the National Capital Region should look to this organization to sustain any events/incidents involving communications for this region. Further, the NCR should participate by having representation (possibly a senior level representative from the Office of the National Region Coordination or other options for consideration) at the NCS/NCC daily and for special events. With the NCR participating, the utility of the center will only increase.

Recommendation:

- Increase the NCR’s awareness and education of the services the NCS/NCC performs for the government and communications sectors; have the National Capital Region participate at the NCS/NCC and/or utilize the NCS/NCC as the single point of contact for any critical communications issues within the region.

3.5 *Measuring Effectiveness*

The industry has many tools to measure the effectiveness of CIP. Exercises and drills, planned and performed on a national scale, is just one method. This industry also sponsors committees, such as the NRSC, which monitors the networks performance with respect to reliability from the FCC reportable outages. The NRSC produces quarterly and annual reports, and on special occasions, study reports to share information with the sector and provide guidance to the sector. (Please refer to link provided in Appendix J for details.)

Finally, the industry at the corporate level has many tools to measure its effectiveness, including key metrics and in-place process controls to measure process effectiveness up to and including root cause analysis.

3.6 *Managing Continuous Improvement*

The communications industry, at the sector level, and the individual service provider/vendor level has been managing continuous improvements for its services well before 9/11. Critical Infrastructure Protection is a composite term representing many business processes. Service providers/vendors have been performing business continuity modeling, disaster recovery drills/exercises, etc., for a long time. Indeed, it is part of the day-to-day critical infrastructure activities to support normal core business. The definition of “critical” differs among various businesses, and could well differ from the federal government’s definition.

Informal focus group comments include:

- “CIP is essential – every sector has its own protection activity for what it thinks is critical but the telecommunications sector has robust programs/processes, which have been on-going for long time in the sector/industry.”
- “Critical infrastructure is at the very top of our core corporations concerns – probably more relevant to the communications sector than to the government.”
- “CIP is something that the telecom sector does (both at the service provider/vendor level and government, e.g., NCC); the sector is best able to do assessments/risk management – the sector completes this and does not believe the government can do this for the sector.”
- “Infrastructure is important to the telecom sector, and therefore terrorism is a legitimate threat for this industry segment. That said – government’s role is to assess threat so that we can best manage vulnerabilities and risks.”
- “The sector and individual service providers and vendors are very focused on all of the practices available – e.g., NRIC; ISO, and Sarbanes Oxley. Therefore, when we develop assessments, they are based on available practices as well as how they serve national responsibilities, customers, and the bottom line.

4. Conclusion

4.1 Challenges

- A key challenge has been and will continue to be the numerous requests for resources from the communications sector to participate in studies, teams, forum, table top exercises, drills, special events, etc. Many of these duplicate others because each state, the federal government, etc., all focus on the critical infrastructure necessary to care for their constituents. A coordination function to prioritize these requests is the challenge and a necessary component to successful activities.
- Creating a process by which the government sector and all sectors can all share answers to secure and improve the vulnerability status. To date, the government sector has not shared threat information nor has it provided feedback.
- The NCR needs to be more visible in the NCC.
- The government's view of the industry is as representatives in the local region (the company whose building and trucks are most visible). However, the government needs a more comprehensive view of sectors and all service providers involved.
- NCR needs, in a telecommunications crisis of national importance, to come to a one-stop-shop--the NCC. It is disruptive to response and restoration operations without this. For example, the designation of National Special Security Events (NSSE) is key to managing in a special situation: it is easier to manage through these special events if information is shared as soon available.

4.2 Areas for Future Investigation

- Conduct tabletop exercises – interdependencies with other sectors.
- Expense reimbursement funding for sector participation is important for continued success.

Appendix A: Methodology for Data Gathering and Analysis Literature Review for Sector (Open Source Tools and Processes)

Methodology

The data gathering for this paper was completed in two parts and only publicly available data were utilized in the creation of this document:

- **Literature review** of available source material such as
 - Network Reliability Interoperability Council (NRIC) reports
 - Best Practices
 - Council reports
 - Network Reliability Steering Committee (NRSC) quarterly and annual reports,
 - Government Accountability Office (GAO) reports
 - National Security Telecommunications Advisory Committee (NSTAC) reports
 - Standards Bodies (see appendix E for complete list)
 - Alliance for Telecommunications Industry Solutions
 - Internet Engineering Task Force (IETF)
 - European Telecommunications Standards Institute (ETSI)
 - International Organization for Standardization (ISO)

- **A Focus Group** meeting was held on March 14 with key members of the National Communications Systems (NCS) and National Coordination Center for Telecommunications (NCC). Participants included a cross representation of the communications industry/sector (refer to appendix C for complete list): Below does not look right.some formatting error

Participants included:

- AT&T
- Bell South
- Qwest
- SBC
- Sprint
- Telecommunications Industry Association (TIA)
- The NCC
- USM
- Verizon

The focus group responded to a series of questions (see appendix B for questionnaire) in a group discussion format.

The Telecommunications Hierarchy

Telecommunications is a very broad set of networks encompassing areas as broad as satellite transmission, radio broadcasts, and mobile phones. While the vast number of applications that fall under telecommunications is large they can be broken into a hierarchy to be made more digestible. In the broadest sense, telecommunications can be divided into two broad sections, applications (end user services) and transport (moving data between end user applications). Further, within transport there is core transport and periphery (edge) transport. Data and analog information can be sent by a variety of means satellite, radio broadcast, fiber optic cable, free

space optics, etc., and it is important to decipher what is at the core of transport and what is tethered to the core to connect end users.

The reason this distinction is important for the examination of critical infrastructure is that the loss of core transport could have higher impacts, if risk mitigation plans are minimal for this area/technology. The loss will not only affect that particular infrastructure, but also all the other infrastructures tethered to it and dependent for their own operation. The core transport infrastructure is long haul fiber optic cables and within cities it is metropolitan area fiber networks. For the National Capital Region, both of these transport infrastructures are essential and serve as tethers connecting all other telecommunications infrastructures and applications. The long haul networks allow the region to communicate with other regions and the metropolitan area networks allow actors to communicate with each other in the region.

As a result of this structure to telecommunications systems, the George Mason University NCR-CIP telecommunications team focused its analysis on firms that provide long haul and metropolitan area networks to the NCR and significant stakeholders in providing telecom service. The NCC Telecom members represent this significant population.

Appendix B: Focus Group Questions

The Telecom Sector focus group meeting examined and responded to the following questions as they apply in the National Capital Region:

Awareness of Critical Infrastructure Protection (CIP) Tools, Procedures and Processes

1. What do you think about critical infrastructure protection, and the practice of vulnerability assessment and risk management? Please describe any sets of guidelines, practices or sets of measures companies adopt for security or reliability purposes.
2. Availability/Application of CIP Tools. What are your roles and responsibilities for routine emergency operations in your company?
3. How are disaster planning processes/vulnerability assessment activities performed?
4. How do you define criteria for judging an asset to be ‘critical?’
5. What types or classes of risks are you most concerned about?
6. Are there particular metrics for critical services?
7. What types of tool/process/procedure are used? Are there accepted standards of VA/RM in your field?
8. What’s the frequency of use?
9. Why do you evaluate vulnerabilities? (IE, regulatory requirements)

Implementation and Resource Allocation

1. How are initiatives to address/mitigate identified vulnerabilities planned?
2. How do you determine what your own capabilities are, as opposed to what is beyond your control?
3. How does your organization plan to prevent serious organization failures from occurring *during* an extreme and/or unpredictable event?
4. How are resources allocated to implement initiatives? Is this based on
5. Predetermined criticality ranking?
6. Identified acceptable levels of risk?
7. Costs of initiatives to reduce likelihood, severity, or duration of disruption?
8. Private returns to owner-operators, versus public returns?
9. Return on investment metrics/measurement?
10. What initiatives and measures have been implemented?
11. How are initiatives evaluated for effectiveness or enhancement over time?

Assuring Organizational Resilience during Extreme Events

1. How much do people talk about failure, and preventing failure in your organization?
2. When someone discovers a mistake or an error, what happens?
3. How often do you train? What about?

Interdependency

1. What other organizations (in your sector and in other sectors) are essential for you to do your work well? For whom are you essential? (Who’s downstream and who’s upstream?)
2. What regulatory bodies do you regularly interact with, and what reports do you file?

Regional Governance and Collaboration

1. What would you change in your current relationship to the public sector to make it more collaborative for critical infrastructure protection?
2. If the crisis impacts multiple sectors (for example an electricity blackout that affects water treatment plants, signal lights, and telecommunications) who's in charge of reaching out across sectors for coordination and information sharing? Is there a current plan for doing so?
3. If an entire region decided to commit to a plan for infrastructure protection, what would be the essential ingredients for coordinated decision-making between the public and private sectors?

Appendix C: Focus Group Members/NCC Membership

- Don Smith, Manager NCC
- Tom Weatherald, Capt. USM
- Dan Bart, TIA
- Rosemary Leffler, SBC
- Tim Bowe and Allison Browney, Sprint
- Ernie Gormsen, Verizon
- Harry Underhill, AT&T
- Cristen Flynn Goodwin, Bell South
- Tom Snee, Qwest
- Ben Stafford, Zeichner Risk Analytics/GMU
- Lee Zeichner, Zeichner Risk Analytics
- PJ Aduskevicz, PJ Aduskevicz Enterprise LLC
- Karl Rauscher, Lucent
- Rick Kemper, CTIA

National Coordinating Center for Telecommunications (NCC) Representatives

In 1982, telecommunications industry and Federal government officials identified the need for a joint mechanism to coordinate initiation and restoration of national security and emergency preparedness (NS/EP) telecommunication services. In 1983, the group recommended to the National Security Telecommunications Advisory Committee (NSTAC) and to President Reagan that a joint industry and government-staffed NCC be created as a central organization to handle emergency telecommunication requests. On January 3, 1984, the NCC opened for business. Today, the NCC is home to the following telecommunications government and industry representatives:

Government

- | | |
|--|--|
| ▶ U.S. Department of State | ▶ Central Intelligence Agency |
| ▶ U.S. Department of the Treasury | ▶ Federal Emergency Management Agency |
| ▶ U.S. Department of Defense | ▶ The Joint Staff |
| ▶ U.S. Department of Justice | ▶ General Services Administration |
| ▶ U.S. Department of Interior | ▶ National Aeronautics and Space Administration |
| ▶ U.S. Department of Agriculture | ▶ Nuclear Regulatory Commission |
| ▶ U.S. Department of Commerce | ▶ National Security Agency |
| ▶ U.S. Department of Health and Human Services | ▶ National Telecommunications and Information Administration |
| ▶ U.S. Department of Transportation | ▶ United States Postal Service |
| ▶ U.S. Department of Energy | ▶ Federal Reserve Board |

- ▶ [U.S. Department of Veteran Affairs](#)
- ▶ [U.S. Department of Homeland Security](#)
- ▶ [Federal Communications Commission](#)

Industry – The NCC’s industry and government representatives use the NCC’s unique organization to work together during day-to-day operations, coordinate NS/EP responses during crises, and produce emergency response plans and procedures as a result of lessons learned during actual events.

- ▶ [Americom](#)
- ▶ [AT&T](#)
- ▶ [Avici](#)
- ▶ [BellSouth](#)
- ▶ [Boeing](#)
- ▶ [Cincinnati Bell](#)
- ▶ [Cingular Wireless](#)
- ▶ [Cisco Systems](#)
- ▶ [Computer Sciences Corporation](#)
- ▶ [Cellular Telecommunications & Internet Association](#)
- ▶ [EDS](#)
- ▶ [Intelsat General Corporation](#)
- ▶ [Intrado](#)
- ▶ [Juniper Networks](#)
- ▶ [Level 3 Communications](#)
- ▶ [Lockheed Martin](#)
- ▶ [Lucent Technologies](#)
- ▶ [MCI](#)
- ▶ [McLeodUSA](#)
- ▶ [Motorola](#)
- ▶ [Nextel](#)
- ▶ [Nortel Networks](#)
- ▶ [Northrop Gruman](#)
- ▶ [Qwest Communications](#)
- ▶ [Raytheon](#)
- ▶ [Science Applications International Corporation](#)
- ▶ [Savvis](#)
- ▶ [SBC Communications](#)
- ▶ [Sprint](#)
- ▶ [Telecommunications Industry Association](#)
- ▶ [United States Telecom Association](#)
- ▶ [Verisign](#)
- ▶ [Verizon](#)

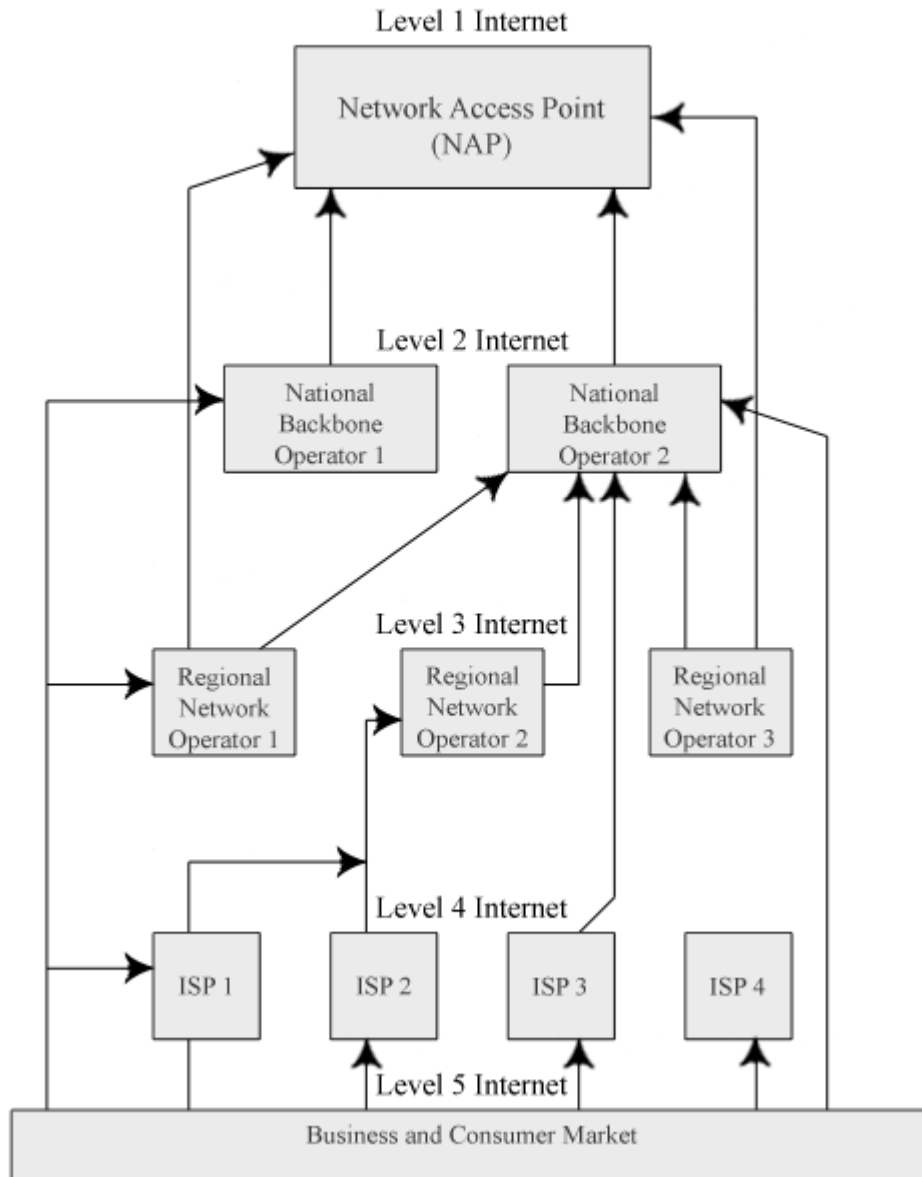
Appendix D: Discussion of the Internet

In order to supply an appreciation of the interplay between different levels of the telecommunications hierarchy, a description is provided below for the operation of the Internet.

Internet Structure

The Internet, like the voice telephone network has a structure and architecture. The Internet is a network of networks. The Internet is composed of a wide variety of small, medium and large networks that all interconnect. Since the Internet is composed of such a wide range of different networks, owners, operators and technologies, it relies on a structured hierarchy and protocol to operate. This hierarchy divides into five levels, illustrated in Figure 1. The first layer is the network access points, designated NAPs. NAPs are hub points where networks can exchange data between each other. A user whose Internet service is provided through a service provider would send an e-mail to a friend who was connected through a different service provider. The e-mail (data) must be transferred between networks, and this is done at NAPs or other transfer points in a process called *peering*.

Figure 1. Network Levels Diagram



(Source: Adapted from Boardwatch 1998)

Level two is comprised of national backbone providers. National backbone providers make available transit services for data between cities and across the United States and the world. If the user above sends an e-mail from his computer in New York to another computer in Washington, DC, the e-mail would traverse a national backbone operator connecting these two cities.

Regional network providers comprise the third level of connection in the hierarchy. If the recipient of the e-mail in the Washington, DC area, actually lives in Springfield, VA, in order to reach the Springfield region south of DC, the e-mail must “hop” onto a regional network, in order to access the many suburbs of northern Virginia. National backbones do not service all cities, just those large enough to create a market opportunity for firms.

Following the hierarchy, the Internet Service Provider (ISP) is the fourth level of service. The e-mail from New York has filtered down to the regional network but our end-user has his personal Internet and e-mail connection through a local ISP. The e-mail then hops off of the regional network onto the local network and is delivered through a dial-up analog modem to the end-user’s house, the fifth level of the hierarchy.

NRIC VI Network Reliability Focus Group (Internet Discussion)

The core backbone will typically consist of relatively high capacity IP routers. Links between core routers will in many cases make use of other equipment, such as (but not limited to) Optical Cross-Connects, Synchronous Optical Network (SONET) gear, and/or Asynchronous Transfer Mode (ATM) switches.

In many cases there may be redundant paths available between core routers. A variety of techniques may be used to allow rapid recovery after link failure, including but not limited to: SONET protection; Internet Protocol (IP) dynamic routing; and Multi-Packet Layer Switching (MPLS) fast re-route. For these reasons, simple (single-device or single-link) outages in the core will in many cases cause minimal or no disruption to the service provided to customers.

The core backbone, will in general, cover a wide area, and may be regional, national, continental, or even worldwide in scope.

In many cases a distribution layer will provide connectivity between the higher capacity core routers and lower capacity devices in the service aggregation layer. In some, but not all cases, the distribution routers will be multi-homed to the core routers, again to provide diverse routing and resilience to failures.

The service aggregation layer consists of a variety of devices, which provide data services to users. For example, devices might provide Digital Subscriber Line (DSL) connectivity, wireless data connectivity, data access over cable networks, or dial-in services over the Public Switched Telephone Network (PSTN). The PSTN itself might be considered to be outside of the scope of the data network, but is still a critical component in the provision of dial-up data services. Service aggregation devices might be either single-homed or dual-homed to the distribution layer, or in some cases to the core backbone.

The interface between the service aggregation layer and the customer may be considered to be the User-to-Network Interface (UNI) for data services.

There are a variety of critical applications that are necessary in the use of data services. For example, Domain Name System (DNS) is in general needed to translate Internet Domain Names into IP addresses. In many cases Remote Access Dial In User Service (RADIUS) is necessary to

authenticate access to a variety of network services, including but not limited to dial-in service. Dynamic Host Configuration Protocol (DHCP) is in some cases necessary in order to allow hosts to obtain temporary IP addresses and other information needed to access the network. In many cases failure of these applications will result in the inability of some or all users to access data services, including a failure to obtain basic IP connectivity.

Other applications will also be used in a data network. For example, users may be expected to make use of applications such as World Wide Web (WWW), Electronic Mail (Email), or File Transfer Protocol (FTP). In general, failure of servers implementing these applications may limit the scope of applications available over the data network, but will not prevent access to basic IP services. Also, since these other applications generally operate directly between the end user and one or more remote servers specific to a particular request, failure of one or more remote servers will in most cases not prevent any user from obtaining similar application services via other remote servers.

No one-service provider directly provides service to every IP address in the world, nor even to a majority of IP addresses. Instead, service providers are interconnected in a variety of ways, such that IP packets destined to addresses served by other providers can be routed from provider to provider to the correct destination. Internet Service Providers (ISP) therefore make use of inter-domain routers, which are routers which forward traffic to and from other service providers. The interface between inter-domain routers in a particular service provider and other inter-domain routers in other service providers may therefore be thought of as a Network-to-Network Interface (NNI).

Figure 2 illustrates the interconnection between service providers.

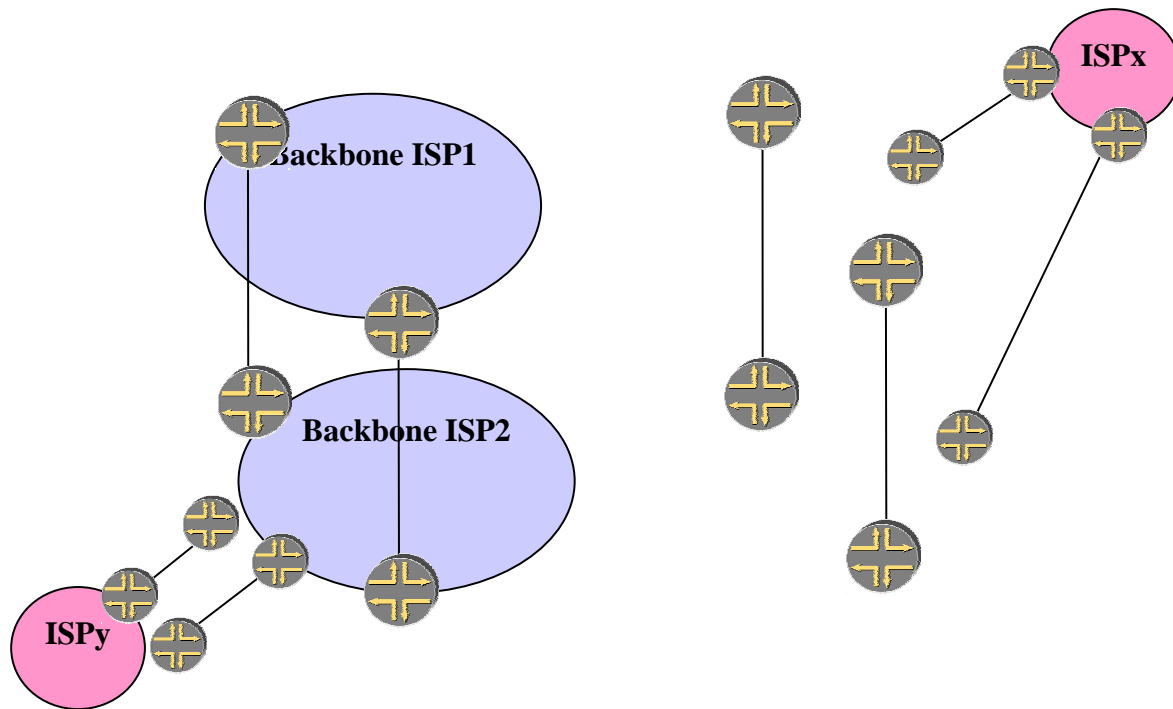


Figure 2: Interconnection of IP Service Providers

Major backbones (such as ISP1 and ISP2 in figure 2) will in general interconnect with each other in order to offer connectivity to other locations throughout the Internet. Major backbones are generally interconnected in multiple locations. This is important for a variety of reasons, including providing diversity. Smaller ISPs will frequently purchase transit service (i.e., service which connects them to the rest of the Internet) from larger ISPs. Even smaller ISPs (such as ISPx and ISPy) will in most cases either be multi-homed to their transit service provider, and/or connected to multiple service providers.

Appendix E: NRIC Physical, and Cyber Best Practices and Disaster Recovery

Identification of Best Practices

Vulnerabilities in the telecommunications sector extend to both the physical infrastructure and the cyber component. This section highlights some of the best practices that have been recognized or implemented for both elements of the infrastructure. See www.nric.org.

Cyber-Security

When an organization decides to setup computer network, cyber security should be an integral part of the architecture being developed for computers and networks. Such architecture should address the issues of compartmentalization of operations based on functionality and accessibility to networks. Given below is a partial list of cyber security recommendations. Although not comprehensive in its scope, this list does offer a typical organization with recommendations that would help make its computer network secure. It is worth noting that detailed recommendations depend on the usage patterns and applications run on the networked computers.

Recommendations:

1. All mission critical applications should be run on **dedicated** computers
2. All computers running mission critical applications should have **backups** to deal with equipment failure, power failure or any other factor that would curtail mission critical operations.
3. Typically an *out-of-box* general-purpose computer equipment when installed on a network comes with default operational and service settings enabled for network access. These **default** settings and services should **be thoroughly examined**. Only those that are required for a specific application and usage should be enabled. If a particular service is not required then it should be disabled. For example, a typical WinTel (Windows OS and Intel CPU) computer comes with the following network protocols enabled,
 - a. TCP/IP
 - b. Microsoft Network
 - c. Netbios
 - d. Novell clientand many more. Some of these protocols have been associated with well publicized vulnerabilities that a malicious agent can utilize to attack such a machine. Thus if such a machine is not going to be part of Microsoft network then one could and should disable Microsoft Network and Netbios protocols.
4. Similarly, those network services that are **not needed should be turned off**. For example, for a typical WinTel machine, services such as Remote Access Service Manager or Remote Access Shell operation are not required. Make sure to go through the entire list of services and disable those that are not required.
5. Encourage use of strong **encryption algorithms** for information exchange over computer networks.
6. **Physical access to mission critical computers should be limited** and access logs should be maintained.
7. Web servers should be **hardened** and should be run with only required set of privileges.
8. Usage of **Firewalls**, anti-Spyware and Virus checking programs should be encouraged.
9. If possible, **running of intrusion detection programs** should be encouraged.

10. All computers should be updated with critical **security patches in timely fashion**.
11. A **periodic audit** check should be done of the hardware and software as well as critical updates and a log should be maintained. For more detailed list of best practice cyber security go to: <http://www.nric.org/fg/nricvifg.html>.

Physical Security

In the past, threat to physical security implied that it came primarily from natural disasters. However, in the post September 11th era, threat to physical security has been viewed mainly as a result of possible physical destruction caused by terrorist attacks. There is very little difference between the destruction caused by natural disasters and that due to terrorism attacks, except that it could also involve additional threats due to chemical, biological or radiological (CBR) attack. Occurrence of CBR would enormously complicate any efforts towards recovery and normalization of operations. CBR event detection, prevention/mitigation offers a new challenge to securing physical infrastructure. The Telecom industry, like any other industry is still coming to grips with these new threats. In the case of critical infrastructures housed inside buildings, environment inspections and procedures established for their normal operations would help mitigate threats posed by chemical/biological events. However, the radiological threat posed by nuclear bomb attack or a dirty bomb would certainly make the task of securing any infrastructure difficult and in that respect, the Telecom industry is no exception. However, some of the best practices that are useful for securing infrastructures against explosives would help at least to some extent to reduce the threat level of radiological event

The best practice recommendations include:

1. The most common practice of **securing a physical perimeter** around a critical infrastructure such as a collocation facility or an antenna tower or even a *welded shut* manhole that houses fiber optic cables.
2. Physical security of any critical infrastructure would undoubtedly involve **limiting physical access** to only those who need to use and operate such facilities. Securing certain perimeter around a physical infrastructure and installing surveillance and monitoring systems where applicable.
3. Maintaining and auditing **entry logs**
4. Creating a clear procedure for **alerting** and notifying authorities of suspicious activities
5. **Training** security personnel, testing their responses to mock attacks and maintaining their readiness by random security alerts and exercising drills.
6. Regular **inspections** fire alarm systems, Environment maintenance units including AHS (Air Handling Unit) and other intrusion detection devices
7. Maintenance and inspection of **backup power** systems such as diesel generators, battery supplies
8. **Securing fuel supplies** for diesel generators
9. **Updating maps** of physical locations of critical infrastructure

In general, Telecom industry prefers self regulating internally agreed upon best practice recommendations that are tailored towards individual actors in the industry and is opposed to

one-size-fits all recommendations imposed from outside. For more detailed description of the best practice recommendations please go to: NRIC's Homeland Security Physical Security (Focus Group 1A) Final report issued in December of 2003. http://www.nric.org/fg/charter_vi/fg1/Rauscher_NRIC_VI_Homeland_Security_Physical_Security_Focus_Group_1A_Final_Report_Issue_3.doc.

Disaster Recovery

NRIC VI performed an in depth study of Disaster Recovery in the communications industry. The team focused on three key areas. More information can be found in the NRIC VI Focus Team Report. Key points to highlight are:

- Contact Information: to allow for effective communication during restoration and a process for updating
- Best Practices to focus on Business Continuity and Disaster Recovery
 - **Business Continuity**
 - Emergency Preparedness
 - Mitigation
 - Preparedness
 - **Disaster Recovery**
 - Response
 - Recovery
 - Resumption of Service
 - Restoration
- Mutual Aid: to facilitate restoration

All these are tools that can be utilized by service providers to enhance their operation and reduce the risks to their network, where appropriate. The Disaster Recovery team re-validated 36 Best Practices from NRIC V and developed 68 new best practices for the industry in NRIC VI.

NRIC VII

NRIC VII continues the work of NRIC VI and adds to the charter to include the critical function of Emergency Services. Listed below are the focus teams of NRIC VII.

Focus Groups

Focus Group 1: Enhanced 911

Subcommittee 1.A: Near Term Issues

Subcommittee 1.B: Long Term Issues

Subcommittee 1.C: Network Outages and Best Practices

Subcommittee 1.D: PSAP / Emergency Communications Beyond E911 (1st Responders)

Focus Group 2: Homeland Security

Subcommittee 2.A: Infrastructure

Subcommittee 2.B: Cyber Security

Focus Group 3: Network Best Practices

Subcommittee 3.A: Wireless Best Practices

Subcommittee 3.B: Public Data Best Practices

Focus Group 4: Broadband

**Appendix F: Proactive Telecomm Industry Initiatives¹
Forums and Standards Organizations**

The Telecommunication Sector has been proactive in the support of critical infrastructure. As stated previously, the telecommunications sector is highly competitive and a reliable infrastructure is one of the keys to business success. Therefore, the telecommunications sector has devoted time, resources, experts, and funding to support forums whether led by the government sector or the private sector. Many of these bodies are forums which were active before 9/11. The difference is the increased focus on terrorist’s modes of threats and vulnerabilities.

All of these forums/bodies contribute to the service provider’s ability to maintain and or improve their respective networks, or work with the government sector on common issues such as critical infrastructure protection. As new technology is introduced, standards need to be developed for the application. Interconnection issues are resolved. New or existing programs such as TSP need to be maintained, etc. The telecommunications sector has been proactive over the years in working to support these bodies either through contributing experts, funding/dues, sponsorships, etc.

Each service provider, vendor, etc. evaluates the set of practices, standards, business policies, rules, etc. and determines which are applicable to their networks/environments. This is based on each service provider's/ vendor's environment and criteria for selection. Principles such as Business Continuity/Risk Management along with entity specific criteria are part of the decision process. Each service provider/vendor has unique architectures, software, etc. One size does not fit all, therefore, a universal mandate or application is not appropriate.

Organization	Narrative
<p>Network Reliability and Interoperability Council (NRIC)</p>	<p>The purpose of the Council is to provide recommendations to the Federal Communications Commission and to the communications industry that, if implemented, shall under all reasonably foreseeable circumstances assure optimal reliability and interoperability of wireless, wire line, satellite, cable, and public data networks. This includes facilitating the reliability, robustness, security, and interoperability of communications networks including emergency communications networks. The scope of this activity also encompasses recommendations that shall ensure the security and sustainability of communications networks throughout the United States; ensure the availability of adequate communications capacity during events or periods of exceptional stress due to natural disaster, terrorist attacks or similar occurrences; and facilitate the rapid restoration of telecommunications services in the event of widespread or major disruptions in the provision of communications services. The Council shall address topics in the areas of Emergency Communications Networks, homeland security best practices, best practices for wireless and public data network services, and broadband.</p> <ul style="list-style-type: none"> • NRIC and other industry forum have over the years and to date developed 801 Best Practices. These Best Practices are by Network Type and Industry Role as noted below: <p>Implementation of NRIC Best Practices is voluntary. The implementation decision is left with the responsible organization and is to be made by individuals with sufficient competence to understand them. http://www.nric.org/ [Frame3]</p>

¹

<p>National Security Telecommunications Advisory Committee (NSTAC)</p>	<p>President Ronald Reagan created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982. Composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies, the NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. Since its inception, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.</p> <ul style="list-style-type: none"> • In November 2002, the Federal Reserve Board (FRB) and BITS briefed the Industry Executive Subcommittee (IES) of NSTAC about the significant dependence of the financial services sector on the telecommunications infrastructure to support core payment, clearance, and settlement processes of financial institutions. To minimize operational risks and ensure the timely delivery of critical financial services, the FRB recommended that the NSTAC analyze telecommunications infrastructure issues relating to network redundancy and diversity. The NSTAC established the Financial Services Task Force (FSTF) to conduct the analysis and released its findings and recommendations in an April 2004 report. • Because the Administration has expressed concern that the concentration of multiple entities' telecommunications assets in specific locations may have implications for the security and reliability of the telecommunications infrastructure, the NSTAC's IES chartered the Vulnerabilities Task Force (VTF) to examine these issues. A February 2003 report addresses the Administration's concerns about the concentration of telecommunications assets in telecom hotels. A few examples of these reports are noted in the table below: <p>[Frame4]</p>
<p>Media Security Reliability Council (MSRC)</p>	<p>The purpose of the Committee is to give members of the broadcast and multi-channel video programming distribution (MVPD) industries the opportunity to provide recommendations to the Federal Communications Commission (FCC) and their industries that, when implemented, will assure optimal reliability, robustness and security of broadcast and MVPD facilities. These recommendations will be based on, among other things, homeland defense and security considerations, and will take into account all reasonably foreseeable circumstances. This will encompass ensuring the security and sustainability of broadcast and MVPD facilities throughout the United States; ensuring the availability of adequate transmission capability during events or periods of exceptional stress due to natural disaster, man-made attacks or similar occurrences; and facilitating the rapid restoration of broadcast and MVPD services in the event of widespread or major disruptions. The Committee will address topics in the areas of security, reliability, and other topics. (www.mediasecurity.org)</p> <p>[Frame5]</p>

<p>The National Coordinating Center for Telecommunications (NCC)</p>	<p>The NCC was created at divestiture for National Security and Emergency Preparedness (NS/EP). The center has been in service for the government and the communications sector for over 20 years. In addition, the NCC Telecom Information Sharing and Analysis Center (ISAC) is an industry/government partnership that provides 24x7 threat analysis, warning and incident coordination for industry participants. The NSTAC, which was established in 1982 by Executive Order 12382 of President Reagan, laid the foundation for the National Coordinating Center for Telecommunications (NCC) when it made its first recommendation that a national coordinating mechanism for emergency telecommunications be formed. Today the reach of the NCC Telecommunications ISAC includes 30 member companies and 3 member associations: 1) the Cellular Telecommunications and Internet Association (CTIA), 2) the Telecommunications Industry Association (TIA), and 3) the United States Telecom Association (USTA). Through member companies and member associations, the reach of the Telecom ISAC within the United States includes:</p> <ul style="list-style-type: none"> • Approximately 95% of wire-line telecommunications service providers, by serving areas and subscribers • Over 60 % of wire-line telecommunications vendors, by sales volume • Approximately 95 % of wireless telecommunications service providers, by serving areas and subscribers • Over 90% of the wireless telecommunications vendors by sales volume • Over 42% of the consumer Internet Service Providers subscribers • Approximately 90% of the Internet Service Providers backbone networks • 6 of the top 10 system integrators in the U.S. Federal IT market • 15% of Domain Name Service root and global Top Level Domain operators
<p>The National Coordinating System (NCS)</p>	<p>NCS was established by Executive Order (EO) 12472 as a Federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spectrum of emergencies. Under the policy objectives stated in EO 12472 and National Security Decision Directive (NSDD) 97, these responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve measurable improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Government during any emergency. (www.ncs.gov)</p>

<p>The NCC Telecommunications Information Sharing and Analysis Center (NCC Telecom ISAC)</p>	<p>The National Coordinating Center for Telecom and its Telecom Information Sharing and Analysis Center (NCC Telecom ISAC), has an operational responsibility as a joint public sector/private sector body to respond to all hazards that can affect the telecommunications infrastructure in the USA. It is a partnership of industry and government. Currently there are 32 industry members, including 3 associations, and 23 federal agencies. In addition, the Sector has three Sector Coordinator organizations that are also members of the NCC Telecom ISAC to extend the reach of the ISAC and to cover other non-operational issues affecting the sector. Those Sector Coordinator organizations under Presidential Decision Directive 63 (PDD-63)/Homeland Security Presidential Directive 7 (HSPD-7) are the Cellular Telecommunications and Internet Association (CTIA), the Telecommunications Industry Association (TIA), and the United States Telecom Association (USTA). Both the Sector Coordinators and the NCC Telecom ISAC (including individual members as appropriate) coordinate with other sectors via the ISAC Council, the Partnership for Critical Infrastructure Security (PCIS), or the American National Standards Institute Homeland Security Standards Panel (ANSI HSSP) or all three of those organizations.</p> <p>These organizations and various members of the NCC Telecom ISAC also cooperate and coordinate internationally on a bilateral basis, regional basis, or international basis with such groups as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), Joint Technical Committee 1 – Information Technology (JTC-1), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the Global Standards Collaboration (GSC), or other national and regional standards groups supporting our sector (<i>e.g.</i>, the European Telecommunications Standards Institute, the Alliance for Telecommunications Industry Solutions (ATIS), the Canadian Standards Association, etc. Many members of the NCC Telecom ISAC are also direct members in each of the standards groups listed.</p>
<p>National Security Information Exchange (NSIE)</p>	<p>The NSIE is an information-sharing forum for industry and government to reduce the vulnerability of telecommunications infrastructure to electronic intrusion.</p>

Alliance for Telecommunications Industry Solutions (ATIS)	<p>ATIS is a standards body encompassing 66 board members from service providers and vendors in North America and Europe. The ATIS board has aggressively promoted to its members the urgency for a solid and time sensitive standards process. This would include critical infrastructure issues. The ATIS board has led the members to prioritize their requirements for standards to meet the significant issues of today.</p> <p>To date, the TOPS Council has reached consensus on the industry’s 16 most critical priorities, including five deemed “most critical.” Focus groups for each of the top five critical priorities were established in 2003, and led by members of the ATIS Board of Directors to examine the priority issues, set milestones, define needed deliverables and standards requirements, and develop a written work-plan that will guide ATIS’ coordination of the priority standards work. Security and VoIP are just two examples of the focus teams. ATIS committees examples:</p> <ul style="list-style-type: none"> ▪ Emergency Services Information Forum ▪ Internet Interoperability Test Coordination ▪ Network Interconnection Interoperability Forum ▪ Network Performance, Reliability and Quality of Service ▪ Network Reliability Steering Committee – Study Groups ❖ The Power Outage Study Group ❖ The Northeast Blackout Power Outages Study Group ❖ The Timing Study Group <p>➤ NRSC also developed a new best practice for guidance for the industry. <i>Service Provider, Network Operators and Property Managers with buildings serviced by more than one emergency generator, should design, install, and maintain each generator as a stand alone unit that is not dependent on the operation of another generator for proper functioning, including fuel source.</i></p> <p>http://www.atis.org/</p>
Internet Engineering Task Forum (IETF)	<p>The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Working groups include: Credential and Provisioning; Intrusion Detection and Exchange Format; Extended Incident Handling; IP Security Protocol; IP Security Policy</p>
The Common Ground Alliance (CGA)	<p>The CGA is a non-profit organization dedicated to shared responsibility in damage prevention and promotion of the damage prevention Best Practices as identified in the Common Ground Study Report. Building on the spirit of shared responsibility resulting from the Common Ground Study, the purpose of the CGA is to ensure public safety, environmental protection, and the integrity of services by promoting effective damage prevention practices.</p>
International Telecommunications Union (ITU)	<p>The ITU, headquartered in Geneva, Switzerland, is an international organization within the United Nations System where governments and the private sector coordinate global telecom networks and services.</p>

<p>European Telecommunications Standards Institute (ETSI)</p>	<p>ETSI is an independent, non-profit organization, whose mission is to produce telecommunications standards for today and for the future.</p> <p>Based in Sophia Antipolis (France), the European Telecommunications Standards Institute (ETSI) is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics.</p> <p>ETSI unites 688 members from 55 countries inside and outside Europe, including manufacturers, network operators, administrations, service providers, research bodies and users - in fact, all the key players in the ICT arena.</p> <p>ETSI plays a major role in developing a wide range of standards and other technical documentation as Europe's contribution to world-wide ICT standardization. This activity is supplemented by interoperability testing services and other specialisms. ETSI's prime objective is to support global harmonization by providing a forum in which all the key players can contribute actively. ETSI is officially recognized by the European Commission and the EFTA secretariat. ETSI's Members determine the Institute's work program, allocate resources and approve its deliverables. As a result, ETSI's activities are closely aligned with market needs and there is wide acceptance of its products. Security Algorithms are a product of ESTI.</p>
<p>Wireless Emergency Response Team (WERT)</p>	<p>WERT provides leading edge advanced wireless expertise, technology and infrastructure support for Search & Rescue operations in national crises.</p> <p>Conducting focused research and reporting key learning's to industry, government and the public</p> <p>Providing emergency guidance for 911 centers, law enforcement, wireless service providers and family members</p> <p>From time to time, WERT may also use it's unique wireless capabilities and expertise to address other critical needs of society.</p> <p>The WERT Final Report for the September 11, 2001 New York City World Trade Center Terrorist Attack (October 2001) documents 134 Key Learning's from the over 250 volunteers directly involved and 23 Recommendations for government and the wireless industry</p>
<p>American National Standards Institute (ANSI)</p>	<p>ANSI functions as the administrator and coordinator of the United States' private-sector voluntary standardization system, including nearly 1000 company, organization, government agency, institutional, and international members. Standards information, conformity assessment, a reference library, and other services are available here.</p>
<p>British Standards Institute (BSI)</p>	<p>BSI is the oldest national standards-making body in the world, is a nonprofit distributing organization facilitating the production of British, European, and international standards. The web site offers information on the organization's services, including recent news and articles from BSI magazines.</p>
<p>The European Committee for Electrotechnical Standardization (CENELEC)</p>	<p>This committee is recognized by the European Commission. CENELEC works with 40,000 technical experts from 19 EC and EFTA countries to publish standards for the European market. The site includes a catalog of publications, organizational strategies, standardization activities, and other relevant material.</p>

GSM World	The GSM Association is the premier global body behind the world’s leading wireless communications standard. It is responsible for the development, deployment, and evolution of the GSM standard for digital wireless communications, and for the promotion of the GSM platform. The site functions as a comprehensive resource for all GSM-related issues.
International Electrotechnical Commission (IEC)	Founded in 1906, the IEC is the world organization that prepares and publishes international standards for all electrical, electronic and related technologies. The site presents information on standards and conformity assessment, IEC structure and management, IEC members and partners, and other relevant information.
International Standards Organization (ISO)	The ISO is a worldwide federation of national standards bodies set up to promote the development of standardization and related activities worldwide. Copies of standards are for sale, and updates on standards revisions, a contact list, news, and other information are available on the site.
National Institute of Standards and Technology	Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department’s Technology Administration . NIST’s mission is to develop and promote measurement, standards, technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs: the NIST Laboratories , conducting research that advances the nation’s technology infrastructure and is needed by U.S. industry to continually improve products and services; the Baldrige National Quality Program , which promotes performance excellence among U.S. manufacturers, service companies, educational institutions, and health care providers; conducts outreach programs and manages the annual Malcolm Baldrige National Quality Award which recognizes performance excellence and quality achievement; the Manufacturing Extension Partnership , a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and the Advanced Technology Program , which accelerates the development of innovative technologies for broad national benefit by co-funding R&D partnerships with the private sector.

Appendix G: Acronyms

ANSI-American National Standards Institute	NANOG-North American Network Operator's Group
ATIS-Alliance for Telecommunications Industry Solutions	NCC-National Coordinating Center for Telecommunications
BSI-British Standards Institute	NCR-National Capital Region
CENELEC-European Committee for Electrotechnical Standardization	NCS-National Communications System
CGA-Common Ground Alliance	NIIF-Network Interconnection Interoperability Forum
CIP-Critical Infrastructure Protection	NISCC-National Infrastructure Security Coordination Center
CIVA/RM-Critical Infrastructure Vulnerability Assessment/Risk Management	NIST-National Institute of Standards and Technology
CQR-Communications Quality and Reliability Committee	NRIC-Network Reliability and Interoperability Council
CTIA-Cellular Telephone Industry Association	NRSC-Network Reliability Steering Committee
DEFCON-Defense Conditions	NS/EP-National Security Emergency Preparedness
DHS-Department of Homeland Security	NSIE-National Security Information Exchange
ESF-European Science Foundation	NSTAC-National Security Telecommunications Advisory Council
ETSI-European Telecommunications Standards Institute	NTIA-National Telecommunication and Information Administration
FCC-Federal Communications Commission	OCS-One Call Systems
FEMA-Federal Emergency Management Agency	OPS-Office of Pipeline Safety
GAO-Government Accounting Office	PDD-Presidential Decision Directive
GETS-Government Emergency Telecommunications Service	POC-Point of Contact
IEC-International Electrotechnical Committee	PSAP-Public Service Answering Point
IEEE-International Electric and Electronic Engineering	PSC-Public Service Commission
IETF-Internet Engineering Task Force	PUC-Public Utility Commission
IP-Internet Protocol	RBOC-Regional Bell Operating Council
ISAC-Information Sharing and Analysis Center	SDO-Standards Development Organization
ISO-International Organization for Standardization	TSP-Telecommunications Service Priority
ISP-Internet Service Provider	USTA-United States Telephone Association
ITU-International Telecommunications Union	VoIP-Voice over Internet Protocol
MSRC-Media Security and Reliability Council	WERT-Wireless Emergency Response Team
	WPS-Wireless Priority Service

Appendix H: Glossary

Critical Infrastructures

PDD-63

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures. Washington DC

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures) and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures. Washington DC

...A network of independent, mostly privately owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.

USA Patriot Act (2001) "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism". 107th Congress of the United States – First Session. Washington, DC October 21, 2001

Critical infrastructures are systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Defending America's Cyberspace – National Plan for Information Systems Protection, January 2000

Vulnerability

As with the definition of Critical Infrastructure, the term vulnerability is defined in different ways. Listed below are a few examples:

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures. Washington DC

A characteristic of a critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

PDD-63 – A description of vulnerability, not a definition

As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

3.4.3 NRIC 6 Physical Security Focus Team

A characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.

Vulnerability Assessment

President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures. Washington DC

Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.

The Technical Committee on Communications, Quality and Reliability (CQR), 1998

Network Reliability is.

1. Availability of end to end functionality for customers.
2. Ability to experience failures or systematic attacks, without impacting customers or operations

Network Security is the surveillance, protection, containment, and deterrence of abuse against assets. This should be within the context of a risk management framework.

Network Security is the property of the network that ensures.

1. Protection
2. Confidentiality
3. Integrity
4. Accountability
5. Availability against internal or external threats

3.5 **Network Security** is both a term and an attribute related to the protection, detection and containment of physical and logical threats to network information, network resources and communication including data systems, applications, centers and human/machine interfaces with respect to availability, confidentiality, integrity, access control, authentication, audit and recovery. It is also an attribute of quality and reliability in relation to the value of the asset to be protected or the criticality of asset to the business.

Network Security in essence is an extension of the internal set of controls reflective of both industry standards and best practices. It involves inferred trust, roles, relationships, responsibilities, and accountabilities for intra-network as well as inter-networks.

Network Security is an essential component of the application, transport, network management, and configuration management. It, like quality, is a journey not a destination.

Appendix I: Bibliography

- Alliance for Telecommunications Industry Solutions (ATIS), Network Reliability Steering Committee, *Second Quarter 2004 Macro-Analysis*
- BITS *Guide to Business-Critical Telecommunications Services*, November 2004
- Commonwealth of Virginia, State Corporation Commission, *Preparation for and Response to Hurricane Isabel by Virginia Telecommunications Providers*, September 2004
- Critical Infrastructure Assurance Office, *Vulnerability Assessment Framework 1.1*, Oct. 1998
- Department of Veterans Affairs (VA), *Physical Security Assessment for VA Facilities*, September 2002
- Homeland Security Presidential Directive / HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003
- Department of Homeland Security, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003
- National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000
- National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications*, December 2000
- National Infrastructure Security Coordination Center, *Good Practice Guide to Telecommunications Resilience*, May 2004
- National Institute of Standards and Technology (NIST), *Security Self-Assessment Guide for IT Systems Questions/Guidance*, August 2001
- NIST, *Publication 800-26, Security Self Assessment Guide for Information Telecommunications Systems*
- NIST, *800-58, Security Guidelines for VoIP systems*
- NIST, *800-34, Contingency Planning Guide for Information Telecommunications Systems*
- NIST, *800-53, Recommended Security Controls for Federal Information Systems*
- NRIC, *Best Practices*, 2004, and all councils www.bell-labs.com/user/krauscher/nric/
- NSTAC *Protecting Systems Task Force Report on Enhancing the Nation's Network Security Efforts*, May 2000

National Security Telecommunications Advisory Committee, *Financial Services Task Force Report*, April 2004

Presidential Decision Directive (PDD) 63: *Critical Infrastructure Protection*, 22 May 1998.

RAND's Vulnerability Assessment and Mitigation Methodology, February 2004: *Finding and Fixing Vulnerabilities in Information Systems*.

Appendix J: Alliance for Telecommunications Industry Solutions

NETWORK RELIABILITY STEERING COMMITTEE

SECOND QUARTER 2004 MACRO-ANALYSIS

Macro-Analysis: Second Quarter 2004

P. J. Aduskevicz

Chair, NRSC

See Website for the latest quarterly report and annual report: <http://www.atis.org/nrsc/index.asp>

Appendix K: Endnotes

¹ As defined in T1.523-2001, an American National Standard for Telecommunications - Telecom Glossary 2000, published by the Alliance for Telecommunications Industry Solutions (ATIS) and found at <http://www.atis.org/tg2k/>

² Source: Although this figure is from the 2002 Business Analyst data, the definition for the Telecom sector is from the 1987 SIC Manual. Hence, it may not reflect the changes that have occurred in this sector over the last dozen years. For that one may have to use the (North American Industrial Classification System) NAICS code adopted by the US Commerce Dept. in the late 1990s. However, commercial products that sell the spatial location data based on the NAICS have been in the market for less than a year.

³ This sector includes telecommunications but some other sub sectors as well such as publishing industries except Internet; Motion picture and sound recording industries; Broadcasting except Internet, Internet publishing and broadcasting; ISP's search portals, and data processing. The estimates of employment for 2001-2003 are based on the 2002 NAICS code. Source: U.S. Department of Commerce, Bureau of Economic Analysis, Regional Economic Accounts

⁴ The estimates of employment for 2001-2003 are based on the 2002 NAICS code. Source: U.S. Department of Commerce, Bureau of Economic Analysis, Regional Economic Accounts

⁵ Source: This data was obtained from the University of Florida's The Infrastructure of the Internet: Telecommunications Facilities and Uneven Access project (BCS-9911222) (Malecki 2002).

⁶ Source: TeleGeography, 2002.

⁷ Source: Charter of the Network Reliability and Interoperability Council – VII. (www.nric.org)

⁸ Source: Charter of the Media Security and Reliability Council (www.mediasecurity.org)

⁹ Source: <http://www.ncs.gov/nstac/nstac.html>

This Page Intentionally Blank