Before the
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of:	)	
	)	
Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload	)	**PS Docket No. 10-92**
	)	
	)	
	)	
	)	

COMMENTS ON NOTICE OF INQUIRY

TELCORDIA TECHNOLOGIES

Telcordia Technologies (Telcordia) hereby submits comments to the Federal Communications Commission (FCC or "Commission") on its Notice of Inquiry (NOI) requesting Comments on broadband survivability in the above-captioned proceeding.[1] The Notice seeks to gather information on a number of issues related to the resilience of the commercial broadband network including single points of failure, public safety communications, physical security best practices, and the redundancy and diversity of the physical network.

BACKGROUND

Telcordia is a software, engineering and consulting company with a vested interest in expanding the deployment of broadband. Telcordia, formerly known as Bell Communications Research (Bellcore), was created in 1984 at the time of the AT&T

[1] Notice of Inquiry "Effects on Broadband Communications Networks Of Damage to or Failure of Network Equipment Or Severe Overload", Public Safety No. 10-92, FCC 10-62, Released April 21, 2010.

divestiture as a unique entity with a mission to provide common R&D as well as technology generic requirements and seamless operational capabilities across all the new service provider boundaries. Telcordia's charter includes technical and management support to protect the integrity and interoperability of the telecommunications infrastructure and, as such, we have worked actively with government and industry in national security and emergency preparedness (NS/EP). Telcordia is vendor neutral and technology agnostic and possesses the depth and breadth of telecommunications experience to handle the full spectrum of broadband and information network engineering and design issues. We offer the following comments on the issues raised by the Commission.

DISCUSSION

Broadband telecommunications and information networking underpin all sectors of our economy and society from finance and business to education, healthcare, energy, public safety, and emergency response. The network infrastructure that delivers this capability is a complex composite built with multiple products and technologies and operated by a variety of carriers, both domestic and foreign. The availability and reliability of this infrastructure is critical to our productivity. The Commission writes in this NOI, "In light of the ever-growing centrality of broadband communications, it is imperative that we understand the resilience and survivability of our national broadband infrastructure."[2]

[2] Notice of Inquiry "Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload", Public Safety No. 10-92, FCC 10-62, Released April 21, 2010, page 2.

A Review on Prioritizing Emergency Communications, Electric Power, and IPv6

In a previous comment[3] we mentioned a number of challenges for delivering robust, secure services in the fragmented, dynamic environment of our broadband industry. We very briefly review those concepts that are germane here, and refer readers to the previous comment for details.

Considerable effort and work are currently underway in defining the standards associated with next generation networks, but the challenge of assuring 9-1-1 service, including multi-media and GIS-intensive services, during emergency situations and conditions of severe overload remains. Telcordia recommends the development and implementation of a multi-level priority policy and associated mechanisms to support next generation 9-1-1 services. Multi-level prioritization will enable high-probability call completion for emergency communications and will provide public safety and first responder communications with priority access to network resources, similar to our legacy NS/EP priority services.

Our nation's critical infrastructure is increasingly inter-dependent and, in particular, the role of electric power in supporting emergency communications requires attention. As smart grid technology is developed and deployed, these interdependencies will become more complex, requiring integrated assessments of survivability and redundancy and cross-sector outage reporting.

We considered the design and development of IPv6 in the technical standards community. While driven largely by impending address exhaustion, IPv6 also serves to integrate network security capability into the Internet architecture. Accelerating the

[3] Telcordia's response to the National Broadband Plan Comment #8 on "Public Safety, Homeland Security, and Cyber Security Elements," Public Notice DA 09-2133, submitted in November, 2009.

migration to IPv6 offers additional capability for providing network security features in the Internet Protocol.

Our Broadband Industry Structure and the Survivability Challenge

Telecommunications carriers undertake many activities aimed at ensuring the reliability of their networks and services. There are also numerous industry and government organizations which specifically address aspects of these critical topics including work in ATIS (Alliance for Telecommunications Industry Solutions), NSTAC (National Security Telecommunications Advisory Committee) and the National Communications System's Route Diversity Project[4]. Nonetheless, the dynamic, complex and heterogeneous structure of the broadband industry can hamper efforts to more accurately assess the survivability and resilience of the network on an end-to-end basis.

Multi-tier business relationships involving carriers, sub-carriers and sub-sub-carriers lead to a lack of transparency on the underlying physical layout. Network operators are continually evolving and reconfiguring their networks to meet market demands and customer needs and to improve quality and reduce costs. This ongoing evolution in the network makes it challenging to ensure levels of redundancy and diversity over the service lifecycle. This is further complicated by the accelerating integration and convergence across different types of carriers, network technologies, and services and by the fast paced change throughout the industry. Every key aspect of telecommunications is experiencing rapid change with evolving types of communications (e.g., machine-to-machine), new devices and emerging services and applications.

[4] See the NCS website at http://www.ncs.gov/rdp/.

Furthermore within this complex and dynamic environment, security and privacy concerns may impede our ability to efficiently identify and mitigate vulnerabilities.

To address these challenges, we need an architectural framework and common data that allow accurate assessment of network survivability and security on an end-to-end basis; which, in turn, would foster an ability for third parties to develop an understanding of the topology of the network-of-networks at the physical layer and of methods to improve the survivability of the network infrastructure. This model framework and information will enable objective analysis of single points of failure and vulnerabilities not only to physical damage and congestion, but also to other threats and attacks. In the remainder of this comment we will focus on emerging standards, technologies and trends that together provide an opportunity for cost-effectively gaining a deeper, broader and more complete understanding of the redundancy and vulnerabilities of our broadband infrastructure in order to improve its availability, reliability and resilience.

Emerging Technologies Hold the Key to Improving Survivability and Resilience

Carriers use a variety of operations systems with disparate database formats to support network planning and engineering functions, to design and provision services, and to maintain inventory and network design information. Although these systems and formats are not interoperable, they do include many common data items. Technical standards organizations continue to make progress in developing standard information models and system interfaces for network management including the Telemanagement Forum's MTOSI (Multi-Technology Operations System Interface) and the International Telecommunication Union's Generic Network Information Model, M.3100. These

standards will increasingly provide the capability for communicating design data among different systems and for supporting applications that interwork across different systems.

RFID is revolutionizing supply chains across a wide range of industries from transportation and pharmaceuticals to military supply and retail sales. While current discussion of RFID and information technology (IT) tends to focus on the use of IT to support RFID applications in other sectors, RFID is emerging within the telecommunications sector as well.[5] A main driver for RFID in telecommunications will be cost savings from better inventory management and asset tracking. However increasing use of RFID-tagged telecommunications equipment will also provide real-time tracking of the location of physical assets in the network and their capabilities, which is critical to understanding the redundancy and survivability of the network.

The last decade has seen an explosion in the availability, quantity and accuracy of geospatial and mapping data of all kinds, along with databases and tools to efficiently store, manipulate, process, and analyze this data. As standards evolve and the use of RFID expands, the availability of location data on telecommunications network elements and equipment will impact network operations across the lifecycle from network design and engineering to deployment, operations, maintenance, upgrade and evolution. From the point of view of survivability and resilience, these emerging technologies can significantly improve the ability of carriers to build-in diversity and redundancy and to track and maintain these characteristics as the physical networks and their

[5] As one example, researchers at Corning Cable Systems have applied for a patent titled *Optically addressed RFID elements* which states: "As fiber optic equipment and networks become more common and more complex, the identification of proper cables, ports and connectors for setting up and maintaining they systems accordingly becomes more complex. ... RFID systems can therefore be applied to fiber optic systems to provide information regarding fibers, connectors, components and ports." From http://www.faqs.org/patents/app/20080218355.

interconnections evolve. The FCC should work with industry to foster working groups and support pilot studies that investigate how to use these emerging technologies to increase the availability, reliability and resilience of our broadband infrastructure.

Towards a More Resilient Broadband Infrastructure

The business environment of our broadband infrastructure presents several critical structural challenges to leveraging these emerging technologies to improve survivability on a nation-wide basis. Effort will be needed to develop an appropriate structure and framework for the required information sharing and analysis across the industry. Strong safeguards are needed to protect proprietary business information of carriers from harmful disclosure. Liability protection is also necessary to support candid discussion of potential risks and vulnerabilities without subjecting participants to increased legal exposure. In addition, there are security and privacy issues that require careful attention to ensure that information on risks and vulnerabilities does not fall into the wrong hands. Nonetheless, there are workable approaches and models that can fully address these legal concerns and provide the necessary protection, including appointing a neutral third party with the requisite objectivity and expertise to facilitate communication on such matters among the members of the industry.

The focus of this NOI is on diversity and survivability at the physical and lower layers in the network hierarchy. We have argued that advances in standards and common data models, in RFID, and in geospatial data processing and analysis will permit cost-effective and automatic approaches both to capture an accurate representation of the underlying physical network-of-networks, and to characterize and improve its

survivability. It is also important to keep in mind the interworking across network layers and, in particular, the critical role that higher layer functionality plays in building in tolerance to lower level failures. Current advances and research in cognitive networks, policy-based management, and autonomic network management are producing promising results for the development of networks with much greater self-managing capabilities, including security management and fault tolerance.[6] As the size and complexity of the broadband infrastructure continue to increase, these technologies will play an ever greater role in improving the availability and reliability of our network, not only for telecommunications but also for other critical and interdependent networks for electric power (SmartGrid), transportation, water, and the like. Support is needed not only for continued R&D in cognitive and autonomic networking in a variety of different threat and service environments, but also in the technology transition work needed to bring these capabilities into productive use.

[6] As one example, the EFIPSANS project in the European Union's 7th Framework Programme is aimed at exposing the features in IPv6 protocols that can be exploited or extended for the design and implementation of autonomic networks and services. See http://www.efipsans.org/.

CONCLUSION

For the foregoing reasons, Telcordia urges the FCC to consider our comments and recommendations. By adopting our recommendations, we believe that the Commission can help ensure that it has the facts and data it needs with respect to the survivability of the nation's broadband communications networks.

Respectfully submitted,

TELCORDIA

By: Deborah J. Nordeen

Deborah Nordeen, Acting President
Advanced Technology Solutions
TELCORDIA
One Telcordia Drive
Piscataway, New Jersey
(732) 699-8013
dnordeen@telcordia.com

June 25, 2010