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

In the Matter of:	)	
	)	
A National Broadband Plan for Our Future-	)	**GN Dockets No. 09-47,09-51, 09-137**
"Public Safety, Homeland Security, and	)	PS Docket Nos. 06-229, 07-100, 07-114
Cyber Security Elements"	)	WT Docket No. 06-150
	)	CC Docket No. 94-102
	)	WC Docket No. 05-196
	)	

COMMENTS –NBP PUBIC COMMENT #8

TELCORDIA TECHNOLOGIES

Telcordia Technologies (Telcordia) hereby submits comments to the Federal Communications Commission (FCC or "Commission") on its Public Notice requesting Comments on Defining "Public Safety, Homeland Security, and Cyber Security" in the above-captioned proceeding.[1] The Notice seeks comments on the Public Safety Mobile Wireless Broadband Networks, Next Generation 911 (NG 911), Cyber Security, and Alerting.

[1] Public Notice, National Broadband Plan –"Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan", GN Dockets No. 09-47,09-51,09-137, PS Docket Nos. 06-229, 07-100, 07-114, WT Docket No. 06-150, CC Docket No. 94-102, and WC Docket No. 05-196, Public Notice DA 09-2133, Released September 28, 2009.

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 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

Telecommunications Industry Structure, Network Architecture, and Threat Environment

Our telecommunications networks are a complex composite of interconnected infrastructure built and operated by a variety of providers, both domestic and foreign. Internet-based services are the dominant and growing component of traffic making the organic nature of Internet topography and its inherent limitations an increasing challenge. The Internet has evolved from its research origins to become the critical infrastructure on which all sectors of the global economy as well as our government, social welfare,

homeland security, public safety, and civil defense depend. The Internet was not originally designed to be secure, per se, nor was it envisioned at the outset to face the magnitude and diversity of cyber threats from hackers, terrorists, criminal organizations, and adversarial nation states. There has been considerable and successful effort directed towards improving the functionality and performance of the Internet by the IETF, W3C, and numerous standards and industry bodies. As one example, the design and development of IPv6, while driven primarily by impending address exhaustion, also integrates network security features into the architecture. In addition, security focused organizations such as the United States Computer Emergency Readiness Team (CERT), the CERT Coordination Team at Carnegie Mellon's Software Engineering Institute, and others have made substantial strides in defense and protection of the Internet against cyber threats. Nonetheless, vulnerabilities and threats continue to grow at the same time as our reliance on the broadband infrastructure across all sectors has increased substantially.

The fragmented environment of our broadband industry poses significant challenges for the delivery of robust, secure services. There is a need for an organizational and architectural overlay that allows accurate assessment of survivability and security, including an understanding of the topography of the network-of-networks at the physical layer. Physical layer redundancy and diversity are critical aspects of fault tolerant and survivable networks, yet building and maintaining diversity is hampered by an understandable lack of transparency on physical network design. This lack of transparency stems in part because of the proprietary and confidential nature of network infrastructure data, and in part because of the complex network and industry relationships

in which service providers may provide service over another entity's assets and/or outsource network operations. Architectures that were diverse may lose diversity over time as upgrades serve to concentrate traffic. As increasingly critical applications and services depend on the network, there is a strong need to create and foster the information sharing necessary to identify and avoid single points of failure.

Our network and services are subject to ever greater threats and attacks ranging from human mistakes, poor designs, and configuration errors to compromised insiders, criminal groups, sophisticated hackers, and the emergence of attacks from foreign-based terrorist organizations. In addition to this evolving threat environment, consumers and businesses face growing problems of spam, viruses, malware, and theft of media, all of which drain resources and reduce productivity. Information sharing regarding threats, vulnerabilities, attacks, and successful response strategies remains difficult because of the potential legal issues and liabilities of industry organizations and the concern by the government and others over potentially dangerous leakage and spread of information on risks and vulnerabilities.

Fault-tolerance and security are critical requirements and we recommend that the FCC establish a framework and appropriate policies to support the coordination and information sharing between service providers, carriers and government agencies that will advance both critical requirements. Addressing the legal issues is paramount so that network designs and service vulnerabilities can be shared without damaging the competitive position of industry entities, without increased risks of lawsuits, and without information leaks that would expose vulnerabilities to criminal elements. While there are existing government-sponsored groups and advisory boards concerned with network

reliability that could be re-purposed to address this gap, we recommend that careful thought be given to creating a forum for coordination and information sharing which is appropriately inclusive of the wide range of important entities and organizations, public and private, and which is designed, organized, and managed as a non-political, problem-solving body.

In the remainder of this Discussion, Telcordia will address the broad challenges in the following areas: The Needs of the Public Safety Community for Mobile Wireless Broadband; Prioritizing Emergency Communications and the Role of Electric Power; Cyber Security; and Trusted Networks: Network Requirements for Public Safety.

Needs of the Public Safety Community for Mobile Wireless Broadband

We encourage the Commission to take an appropriately forward-looking view of the needs for mobile wireless broadband applications for the public safety community. Mobile data traffic is growing at high and sustained rates and the demand for advanced mobile devices and broadband services is exploding. In this environment, future needs for the public safety community will include not only two-way video and multimedia, but also extensive, enhanced sensor networks and sensor data analysis, as well as real-time command and control, logistics, and decision support.

In particular, we expect sensors to play a growing role in disaster response and emergency management. Sensors embedded in first responders' suits will transmit detailed, geo-located, real-time data on physical, chemical, biological, and radiological characteristics of disaster scenes. First responders will be able to deploy low-cost, low-power sensors at emergency sites and these sensors will self-organize to form mobile ad-

hoc networks. Sensors and sensor networks will provide precise, real-time information to assess the magnitude, scope, and attributes of disasters; to target search and rescue operations; and to rapidly deploy the needed materials and supplies for the response. Importantly, sensors worn by first responders will also monitor their precise location, motion, and health status to improve the safety of responders on the job.

These enhanced capabilities in mobile broadband applications for will translate into expanded needs for high-performing, ubiquitous broadband services with appropriate robustness, security, fault-tolerance and reliability to support public safety, civil defense, and emergency response activities.

Prioritizing Emergency Communications and the Role of Electric Power

Considerable effort and work are currently underway in defining the standards associated with next generation 911 networks and alerting mechanisms; however, the deeper challenge of how to complete such calls during emergency situations on often overloaded public communication networks still remains. This issue is particularly critical during medium to large scale emergency situations as the public networks, wired and wireless, become overloaded due to high call volumes. Examples would include not only wide spread weather events, but also more local emergencies in high density locations such as an office park, university, or hospital campus. There are no mechanisms currently implemented on an end-to-end basis across the network that support prioritization of public safety and emergency communications and alerts.

Telcordia recommends the development and implementation of a multi-level priority policy and associated mechanisms to support next generation 9-1-1 services, to

enable high-probability call completion for emergency communications, and to provide public safety and first responder communications with priority access to network resources as needed. Emergency communications increasingly include multi-media and GIS-intensive applications and will require a well-designed network priority scheme. These priority mechanisms will further lead to the development of public safety and homeland security applications that can automatically tailor their communications to available network resources so as to deliver the most critical information most rapidly.

Our nation's critical infrastructure is increasingly inter-dependent and, in particular, the role of electric power in supporting emergency communications requires attention. The requirements for power at subscriber sites for broadband communications service and for end user devices are often confusing for consumers. It is important that service providers clearly articulate the capabilities and limitations for emergency communications to current and prospective customers, including the delivery of alerts during power outages and the use of backup power sources. As smart grid technology is developed and deployed, the interdependence between power and telecommunications will become more complex, but may also provide additional opportunities to deliver various types of more guaranteed power to subscriber sites. With this increased interdependence comes a need for more integrated outage reporting policies, mechanisms, and procedures to better track the robustness and reliability of critical infrastructure and their impacts on one other. This integrated reporting function would include not only power and telecommunications, but also water, transportation, and related infrastructure and will provide a base of knowledge and information that can be used to improve overall performance. In particular, Telcordia recommends that inter-

sector cyber security efforts be established to address the challenges of the increased interdependence among national infrastructure.

Cybersecurity

As new technologies, devices, and applications are introduced into the communications infrastructure, so too are new risks resulting in a situation in which network and service operators must protect against a growing collection of more severe and dangerous vulnerabilities. There are also major concerns due to the technical innovation and collaboration of cyber criminals as they combine different types of malware to create more powerful attacks. As one example, thousands of computer systems have been compromised by the Conflicker worm creating the largest botnet to date and enabling gigabit per second (up to 50gbps so far) denial-of-service attacks against enterprises and service providers. As critical services and associated sensitive information are supported by the broadband infrastructure, it becomes a more attractive target for compromise and theft of personal information and intellectual property and for disruptions of commerce, governments and society.

Large service providers and enterprises invest in current security technology, but it is still difficult and costly to keep pace with the rapid evolution of today's threat environment. Trade associations, standards forums, and government sponsored organizations like the National Security Telecommunications Advisory Committee actively address security issues, but they are fragmented and often hampered by the lack of information sharing addressed earlier. There is a plethora of security standards and best practice guidelines that address specific aspects of the security problem; for

example, ITU security standards (e.g., X.805), NRIC Best Practices and Telcordia's GR 815 for communications network element security. However, security administration across large infrastructures, multiple management domains, and the lifecycle of systems, networks, and services is still very challenging and expensive. Security products continue to evolve but are generally in a catch-up mode in dealing with threats and attacks, resulting in a situation of frequent patching and upgrades.

In addition to the suggestions discussed below under Trusted Networks, Telcordia recommends continued development and funding for innovation which is needed across all areas of security so that solutions advance on pace with the escalating problems. Current research topics, including secure policy definition and compliance, intrusion detection and prevention, software hardening, and resilient architectures, show promise, but significant work is needed to progress from R&D to operational capability. Innovation is needed both on existing challenges and on longer time frames to address the fundamental architecture and constructs of the Internet and how to make them inherently more resilient and secure. To a large extent we currently operate in a 'patch' mode in which much effort is spent repairing existing infrastructure. The National Broadband Plan affords a critical opportunity to get substantially ahead of the curve in creating a robust and secure infrastructure.

Trusted Networks: Network Requirements for Public Safety

To support current and future public safety needs, broadband infrastructure, both wired and mobile, will have to meet a wide variety of requirements related to robustness, security, resilience, availability, and privacy. These requirements are not necessarily

unique to civil defense and emergency response – as we increasingly rely on broadband infrastructure to support all sectors of our economy, that infrastructure will have to be capable of operating in a trusted mode for services and applications that require enhanced reliability. We provide a brief summary of the key aspects of *Trusted Networks* below.

The evolving broadband network will only be as strong as its weakest link, so security, privacy, and assurance requirements must be rapidly developed, uniformly adopted, tested, and certified to ensure the nation's trust in its communication network infrastructure. These requirements must be kept up-to-date as new security threats arise and as technology and services evolve to identify, address and mitigate vulnerabilities that could have catastrophic impact on the US and its economy. Consumers and businesses spend increasingly more time, money and effort trying to protect their networks, applications, and data while these are subject to increasing quantities of spam, viruses, and identity theft. Because of the fundamental nature of information networking as an enabler, the ongoing end-to-end availability of the network and the predictability of its service quality are critically important to the adoption and use of broadband networks and to delivery of benefits to the nation across all sectors of our business and society.

There are four primary components to a solution of trust: Trust in the Network, Trust in Services, and Trust in Information and Trust in Users.

Trust in the network refers to measures taken to increase the network's resilience and resistance to faults that might partially or totally incapacitate it, and to prevent disclosure of sensitive information that might make it vulnerable to privacy and copyright violations and fraud. The access, perimeter, and core network layers need to be secured by addressing the network equipment, systems (e.g., routers, gateways), management

processes, and network interconnection across providers, both wired and wireless. This component also addresses new networking trends like cloud computing with data, applications and services residing in the network, extending the reach and control of the service provider. Trust focuses on fault-tolerance, reliability, availability, rapid restoration, redundancy, and physical security.

Trust in services refers to measures taken to secure transport functions, application software, user interfaces (e.g., web-based), and the directories, proxies, virtualization, and other elements that enable and support service access and use. This includes protection against attacks that deny service or reduce service quality to unusable levels and it involves the full range of services – data, real-time, multi-media, etc. It also involves protection of the supporting structures for services such as addressing (DNS), content distribution management, and authorization. Trust in services focuses on fault-tolerance, availability, redundancy, and cyber security.

Trust in information refers to steps taken to preserve the confidentiality, integrity, provenance and accuracy of the information (e.g., healthcare, public safety) traversing the network. This component includes content management, digital rights management, and protection against theft, falsification, and illegal disclosure of information. Protection of information is a paramount concern of end users and includes data privacy and defense against identity theft. It is imperative that measures taken to protect data and information be robust and work end-to-end. Trust in information focuses on cyber security, privacy, and assurance.

Trust in users refers to policies and mechanisms for authenticating individuals, businesses, and organizations as users of services, applications, and devices; as sources of

content and information; and as participants in on-line transactions and communities. Clearinghouses and other mechanisms are needed for identity management and authorization that can provide strong identity assurance for individuals and groups, preserve privacy, prevent identity theft, and support law enforcement in identifying and prosecuting criminal activity. Trust in users focuses on authentication, authorization, cyber security, and privacy.

To address these four components requires activities across a number of administrative domains with different technologies, architectures, protocols, facilities, processes, and interfaces. Flexibility and adaptability are also necessities as the robustness and security requirements for broadband infrastructure are dynamic and vary depending on the nature of the supported applications, transactions, and user needs. Furthermore, these concepts have to be implemented across all parts of the technology lifecycle from network planning and design; to network management, operations and control; and network expansion, upgrade, and evolution.

The current efforts by service providers, equipment vendors, and standards and industry organizations to improve the security of networks and services have not been sufficient to address the evolving and escalating threats, vulnerabilities, and intrusions. Federal government support is needed for the following activities to develop and maintain *Trusted Networks*:

- Identify key risk areas and vulnerabilities based on comprehensive threat models and security assessments for the all types of networks – wired, wireless and satellite, for their services and applications, for their information and content, and for their users;

- Leverage key outputs from current standards and industry forums and from computer and Internet reliability and security organizations;
- Work with national operations centers to improve policies and practices for identification, isolation, and resolution of faults, outages, intrusions, security and privacy attacks;
- Engage the industry and consumer and business organizations with a series of focused workshops to solicit inputs, promote dialogue, and drive consensus on requirements, policies, and processes;
- Develop baseline requirements focused on securing the availability and performance of network elements, operations systems and control mechanisms, media and management interfaces, applications, and edge devices, and accounting for differing reliability and security requirements;
- Adopt reliability, resilience, security and privacy best practices to address the ongoing management and maintenance of the infrastructure throughout its lifecycle and across all layers of networks;
- Improve policies and mechanisms for identity management and user authentication which preserve privacy, reduce crime, and assure the identity of on-line participants; and
- Advance the resilience, security, and robustness of all aspects of the broadband infrastructure by a balanced program of research and development in both network and information security and on both solutions to near-term problems and fundamental innovations for the longer term.

CONCLUSION

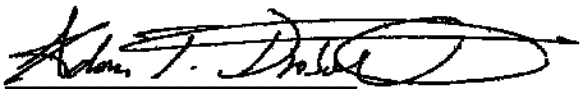
For the foregoing reasons, Telcordia urges the FCC to consider our comments and, in particular, these recommendations:

- Improve transparency and data sharing, with appropriate safeguards and protections, concerning critical national assets and their vulnerabilities and risks to support improvements in survivability, robustness, and information assurance;
- Develop an end-to-end multi-level public safety prioritization mechanism that will provide emergency and first responder communications priority as well as support advanced public safety applications and information exchange;
- Provide leadership and investment in new techniques which address the fundamental constructs, vulnerabilities, and protection of the network, its users, applications and content; and
- Establish inter-sector reliability and security efforts to address the challenges of the increased interdependence across national infrastructure including smart grid technology, transportation, and telecommunications.

We believe that they will enable the FCC to improve public safety, emergency response, and homeland security and to strengthen the integrity of the broadband telecommunications infrastructure in the face of mounting threats.

Respectfully submitted,

TELCORDIA

By: 

Dr. Adam T. Drobot, President

Advanced Technology Solutions
Chief Technology Officer
TELCORDIA
One Telcordia Drive
Piscataway, New Jersey
(732) 699-2100
adrobot@telcordia.com

November 12, 2009