Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of

Improving 9-1-1 Reliability	)	PS Docket No. 13 - 75
	)	
Reliability and Continuity of Communications	)	
Networks, Including Broadband Technologies	)	PS Docket No. 11- 60

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association (TIA),[1] supported by approximately 500 participating members, is a trade association representing the ICT manufacturer, vendor, and supplier interest,[2] responds to the Commission's *Notice of Proposed Rulemaking* (NPRM) in the above-referenced proceeding.[3] TIA appreciates this opportunity to share its insight with the Commission from the perspective of the equipment manufacturer and standard developer.

---

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms, as well as an American National Standards Institute-accredited standard development organization for the telecommunications industry. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on industry standards. Among their numerous lines of business, TIA member companies design, produce, and deploy a wide variety of devices with the goal of making technology accessible to all Americans.

[2] For an overview of the ICT market, technologies and policies that drive innovation and investment, please see TIA's *2013 Policy Playbook* at http://www.tiaonline.org/policy/tia-2013-playbook.

[3] *See* Improving 9-1-1 Reliability, et al., PS Docket Nos. 13-75, 11-60, Notice of Proposed Rulemaking, FCC 13-33 (rel. Mar. 20, 2013) ("NPRM").

I. TIA SUPPORTS THE COMMISSION'S OBJECTIVE OF ENSURING THE RELIABILITY OF PUBLIC SAFETY COMMUNICATIONS

Public safety communications are of vital importance. TIA supports the objective in ensuring that the public can use communications networks to reach emergency services, especially during times of major natural and man-made disasters.[4] TIA appreciates the gravity of issues related to this endeavor and urges the Commission to take as balanced an approach as possible in this undertaking. Such an approach will reflect an understanding of a number of trends that network vendors and network equipment operators have come to find as tried and true principles.

Network reliability is affected by a broad array of factors that may help or hurt the network, including software, hardware, human and inter-government relationship factors.[5] When examining how to make networks more resilient and reliable, TIA urges the Commission to take all of these factors into consideration. The National Security Telecommunications Advisory Committee (NSTAC) concludes that diverse factors are involved with improving networks when it stated that "the evolution of the communications network will be driven by changes in technology, applications, content, devices, and increased requirements for capacity, bandwidth, and spectrum."[6] As noted below, numerous voluntary intra- and inter-industry efforts and public-private partnerships undertake the task of network reliability continuously, producing standards and best practices that are heavily relied upon. TIA supports deference to these efforts in lieu of new regulations on network resiliency and reliability.

---

4 *See* NPRM at ¶¶ 5-6.

5 *See* NSTAC, *Next Generation Networks Task Force Report* (rel. Mar. 28, 2006) at G-1 to G-10.

6 NSTAC, *NSTAC Report to the President on Communications Resiliency* (rel. Apr. 19, 2011) at 4 (NSTAC 2011 Report).

The Commission is encouraged to recognize that no network, no matter the planning or regulation, can be designed and implemented to withstand every possible source of failure.[7] The Commission should also recognize that, in spite of network evolution and development of innovative applications and services, legacy infrastructure is, and will continue to be, a critical aspect of communications networks as technology continues to transition to IP-based delivery systems.[8] Despite this reality, today's networks, including legacy wireline systems, are continually evolving to meet emerging challenges to resiliency with success. From both the operator and equipment vendor perspective, the highest priority is placed on designing such networks to avoid single points of failure; the transition from legacy technology to internet protocol (IP) -based technology is, in fact, one of the most noteworthy fundamental improvements towards increased resiliency due to the nature of IP.[9] Indeed, the degree of reliance and service expected by Americans on communications networks would not be to the degree that it currently is if networks were not resilient or reliable, and a diversity of solutions that employ primary and secondary backup systems are used to help avoid failures. As this

---

[7] *See* NSTAC 2011 Report at 1 ("While it would be near impossible to develop and maintain networks that are invulnerable to disruption, ensuring long-term communications resilience requires that the Government understand future systems and the future technology landscape when investing in and planning for durable, survivable communications for Government officials, first responders, and the general population.").

[8] "For many years the NS/EP community has relied extensively on public telecommunications networks for a large portion of its NS/EP communications needs. This reliance has increased in recent years as the functionality of public networks has improved and as the Federal Government has found more efficient and effective ways to use public telecommunications services. As public network providers have deployed more advanced equipment, the increased use of public telecommunications networks has often also brought the benefits of new features at substantially more cost-effective rates to the Federal Government. Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 7, *Final Report: Planning for NS/EP Next Generation Network Priority Services during Pandemic Events* (rel. Dec. 2010) at 14 (CSRIC WG7 2010 Report).

[9] IP communications allow for a message to be broken down into packets that are sent off individually in multiple directions in search of the most efficient and least congested route. IP also allows for increased awareness of the cause of message failures. *See* Nuechterlein, J., Weiser, P., *Digital Crossroads: American Telecommunications Policy in the Internet Age* (2007) at 121-123.

transition occurs, TIA expects that outages due to single points of failure will increasingly become a problem of the past.[10]

Network operators routinely make hyper-local decisions on how to address resiliency challenges based on direct knowledge of unique threats and priorities guided by already-existing industry standards and best practices. All these critical decisions are balanced with the availability of investment capital. Continued adherence to the Commission's technology-neutral policy will ensure competition in the marketplace, leading to equipment that responds as quickly as possible to the needs of network operators. The imposition of any new network reliability regulations, even those targeted primarily for public safety communications would hinder the development of these time-tested successful efforts as described below.

II. THE FCC SHOULD SUPPORT NETWORK PROVIDERS AND VENDORS AS THEY CONTINUE TO VOLUNTARILY UNDERTAKE SIGNIFICANT EFFORTS TO ENSURE NETWORK RELIABILITY

The Commission requests input on relevant industry standards and industry best practices.[11] TIA supports a reliability ecosystem – consisting of industry voluntary `and consensus-based standards, best practices, self-evaluation efforts, and public-private partnership efforts. Furthermore, there are several non-regulatory actions that the Commission is encouraged to take to further ensure network reliability.

---

[10] *Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket No. 11-47, *Effects on Broadband Communications Networks of Damage or Failure of Network Equipment or Severe Overload*, PS Docket No. 10-92, *Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, EB Docket No. 06-119, *Notice of Inquiry*, FCC 11-55 (rel. April. 7, 2011) (NOI). Reliability NOI at ¶ 40-41.

[11] *See* NPRM at ¶ 21.

Voluntary, Consensus-Driven Standards. Through the years, network operators and vendors have made great strides in network resiliency through voluntary, consensus-based standards development. TIA has been instrumental in the standards making process both within TIA and in other standard development bodies, and continues to strive for greater network reliability and resiliency. The Commission is urged to recognize that the vast majority of standards developed by TIA have resiliency and reliability factored into them.

In its history, TIA has issued over 3,500 ICT industry standards and related documents, the vast majority of which are ingrained with resiliency and reliability principles.[12] Traditionally, TIA's standards work has focused on vital technical areas such as mobile and personal private radio, point-to-point communications, multimedia access, satellite equipment and systems, user premises cabling and fiber optic cabling. However, in recent years, TIA has expanded its standards focus to areas such as smart device communications and machine-to-machine (M2M) connections and smart utility networks. Further, while working on these cutting edge segments, TIA coordinates with dozens of global standards developing organizations, and continues its outreach.

Of particular relevance to the FCC questions regarding standards central offices the TIA-942.[13] To be clear, TIA-942 is intended more generally for data centers and is not specifically intended for telephone central offices. The purpose of this Standard is to provide requirements and

[12] See Appendix 1, which includes a fully list and description of TIA standards committees and their activities. In addition, TIA publishes an annual report, titled the *TIA 2012-2013 Standards & Technology Annual Report*, that includes the latest actions taken by each respective TIA engineering committee toward the development of standards for the advancement of global communications, which is available at https://www.tiaonline.org/sites/default/files/pages/STAR4.24.13.pdf.

[13] *See* NPRM at ¶ 38.

guidelines for the design and installation of a data center or computer room. It is intended for use by designers who need a comprehensive understanding of the data center design including the facility planning, the cabling system, and the network design. This standard presents an infrastructure topology for accessing and connecting the respective elements in the various cabling system configurations currently found in the data center environment. In order to determine the performance requirements of a generic cabling system, various telecommunications services and applications were considered. In addition, this Standard addresses the floor layout topology related to achieving the proper balance between security, rack density and manageability. The standard specifies a generic telecommunications cabling system for the data center and related facilities whose primary function is information technology. Such application spaces may be dedicated to a private company or institution, or occupied by one or more service providers to host Internet connections, and data storage devices. Data centers support a wide range of transmission protocols. Data centers can be categorized according to whether they serve the private domain ("enterprise" data centers) or the public domain (internet data centers, co-location data centers, and other service provider data centers). Enterprise facilities include private corporations, institutions or government agencies, and may involve the establishment of either intranets or extranets. Internet facilities include traditional telephone service providers, unregulated competitive service providers and related commercial operators. The topologies proposed in this document, however, are intended to be applicable to both in satisfying their respective requirements for connectivity (internet access and wide-area communications), operational hosting (web hosting, file storage and backup, database management, etc.), and additional services (application hosting, content distribution, etc.).

Failsafe power, environmental controls and fire suppression, and system redundancy and security are also common requirements to facilities that serve both the private and public domain.

Of particular relevance to the Commission's inquiry is the work of a subgroup within TIA's TR-42 standards committee, (Telecommunications Cabling Systems),[14]. TIA has convened TR-42.13.3, a reliability working group that has labored to prepare and maintains reliability standards and associated test methods for fiber optic interconnecting devices, materials and similar types of passive components. This group responsively examines necessary areas for best practices development, and continued work is planned.

TIA -942 incorporates an annex for data center tiered reliability. Each of the four tiers details architectural, security, electrical, mechanical and telecommunications recommendations. Breaking data center reliability into these four tiers provides a framework with which to compare one data center with another.. The TIA-942 standard incorporates a data center classification hierarchy denoted by tier numbers 1 through 4, ranging from "Basic Data Centers" to "Fault Tolerant Data Centers."

[14] See Appendix. TIA's TR-42 develops and maintains voluntary telecommunications standards for telecommunications cabling infrastructure in user-owned buildings, such as commercial buildings, residential buildings, homes, data centers, industrial buildings, etc. The generic cabling topologies, design, distances and outlet configurations as well as specifics for these locations are addressed. The committee's standards work covers requirements for copper and optical fiber cabling components (such as cables, connectors and cable assemblies), installation, and field testing in addition to the administration, pathways and spaces to support the cabling.

These tiers are summarized below:

1. Tier 1 Data Centers -Basic Data Centers
   - Single path for power and cooling
   - No redundant components
   - Annual downtime of 28.8 hours (99.671%)

2. Tier 2 Data Centers Redundant Components Data Centers
   - Single path for power and cooling
   - N+1 redundant components
   - Annual downtime of 22.0 hours (99.749%)

3. Tier 3 Data Centers - Concurrently Maintainable Data Centers
   - Single active path for power and cooling, one inactive redundant path
   - N+1 redundant components
   - Annual downtime of 1.6 hours (99.982%)

4. Tier 4 Data Centers -Fault Tolerant Data Centers
   - Dual active paths for power and cooling
   - 2 (N+1) redundant components
   - Annual downtime of 24 minutes (99.995%)

Best Practices Preferable. TIA believes that the use of non-mandatory best practices has resulted in immeasurable increases in network resiliency and reliability. Given the fact that each best practice is not relevant for each area, sector, node, etc. of the communications industry, because they are not mandated, network operators are allowed for the flexibility to employ the best equipment and systems that meets their specific challenges to network reliability. There are currently numerous voluntary industry efforts underway that continually formulate, aggregate, and update best practices, and network operators and equipment vendors regularly look to best practices, both internal and external to their organization.

Given the abundance of best practice work today, TIA strongly urges the Commission to allow for these successful efforts to continue to evolve and succeed, and to refrain from adopting new unnecessary regulations on network reliability.

Public-Private Efforts. Numerous private-public efforts currently exist that work to improve network reliability today. As the NPRM notes the Communications Sector Coordinating Council (CSCC)[15] provides input to the Federal government on man-made and natural threats to critical communications, and TIA is a member of its Cybersecurity Task Force.

On the Commission's part, TIA believes that it should continue to utilize advisory groups to facilitate network resiliency and reliability. The CSRIC, which TIA is a member of, exists to ensure, among other things, optimal security and reliability of communications systems, which include telecommunications, media, and public safety.[16] Adoption of new rules could, aside from hampering voluntary industry efforts as noted above, likewise derail the efforts of the CSRIC. Similar effects would be felt by the FCC's Media Security and Reliability Council and Emergency Response Interoperability Center Public Safety Advisory Committee (ERIC PSAC). The Commission should continue to support each of these committees in reaching the goal of network resiliency and reliability.

Adequate Central Office Backup Power. TIA concurs with the Commission that power continuity is vital to network reliability. Communications network providers and vendors understand this and other factors that cause outages. On their own initiative, they have worked for many years towards ensuring network dependability, which has resulted in increasingly resilient and reliable networks. As a result of no uniform mandates for key aspects of network reliability such as

---

[15] The Communications Sector Coordinating Council (CSCC), with its government partners, works to protect the Nation's communications critical infrastructure and key resources (CIKR) from harm and to ensure that the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. U.S. Communications Sector Coordinating Council, Background, *available at* http://www.commscc.org/ (last visited May 7, 2013).

[16] *See* http://transition.fcc.gov/pshs/advisory/csric/.

backup power, each operator has been able to make the most responsible decision to address such concerns in the most efficient manner. How each operator accomplishes this objective varies from system to system, depending on the needs of the operator. It should be noted that most critical facilities, including data centers, already have backup power without a Commission requirement.

V. CONCLUSION

In light of the public's dependence on communications networks to contact public safety resources, the resiliency and reliability of these communications networks is of paramount importance. TIA supports the Commission's efforts to ensure that these networks are reliable and resilient and encourages the Commission to encourage network operators to take all appropriate measures directed toward improving the reliability of their networks.

Respectfully submitted,

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

By: */s/ Danielle Coffey*

Danielle Coffey
Vice President, Government Affairs

Mark Uncapher
Director, Regulatory and Government Affairs

Brian Scarpelli
Manager, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road, Suite 200
Arlington, VA 22201
(703) 907-7700
May 13, 2013