BEFORE THE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

In the Matter of:	)	
	)	
Developing a Framework	)	**Docket No. 130208119-3119-01**
To Improve Critical Infrastructure Cybersecurity	)	
	)	

COMMENTS OF THE INDEPENDENT TELEPHONE AND TELECOMMUNICATIONS ALLIANCE

The Independent Telephone and Telecommunications Alliance ("ITTA") hereby submits its comments in response to the Request for Information ("RFI") issued by the National Institute of Standards and Technology ("NIST") seeking information "to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed" to develop a framework ("Cybersecurity Framework" or "Framework") to reduce cyber risks to critical infrastructure.[1] The Framework will "consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" and "will incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[2]

I. INTRODUCTION AND SUMMARY

ITTA represents mid-size telecommunications carriers who offer a wide range of wired communications services including voice, data, and video to millions of consumers in 44 states.[3]

---

[1] *Developing a Framework to Improve Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, U.S. Department of Commerce, Docket No. 130208119-3119-01, 78 Fed. Reg. 13024 (Feb. 26, 2013) ("*RFI*").

[2] *RFI*, at 13024.

[3] ITTA members include CenturyLink Communications, Cincinnati Bell, Comporium Communications, Consolidated Communications, FairPoint Communications, Frontier Communications, Hargray Communications, HickoryTech Communications, and TDS Telecom.

In addition to residential and small business communications services, ITTA members provide high-capacity data connections and transport to a variety of entities including local and federal government agencies, private financial services institutions, investor-owned utility providers, healthcare providers, and numerous others who depend daily on the reliability and security of ITTA members' landline communications networks.

ITTA recognizes the challenges that face policymakers as they develop our country's policy to protect against cyber threats. ITTA member companies acknowledge that the threat of a cyber-attack crippling our economy and having a devastating effect on the health and security of our country is demonstrable, and they have responded by investing tens of millions of dollars annually to secure their networks from physical and cyber threats. Effective cybersecurity requires coordination among many different government agencies and, importantly, the expertise and experience of various private industry sectors including the communications industry represented by ITTA.

The communications industry is constantly evolving and many of the laws governing various aspects of the industry were arguably obsolete the day after the bills containing them were signed into law. In fact, some of the laws governing the communications industry today are actually hurting investment, competition, and innovation. Given the reality that the communications industry is in a constant state of innovation and change that is largely being driven by consumers' demand for more robust services, including additional security protection platforms, when developing a Cybersecurity Framework, policymakers should resist attempts to apply mandatory standards and a "one-size-fits-all" approach toward protecting and advancing the safety of the country's communications networks. In addition, the Cybersecurity Framework should make clear that nothing in it is intended to suggest an expansion of the existing statutory

authority of any federal agency. Federal agencies, including independent agencies, must operate within the boundaries of their statutory authority when considering regulatory or other actions to address cybersecurity.

Importantly, policymakers should not overlook current voluntary best practices in the communications industry and should resist the temptation to promote or adopt mandatory requirements or standards. The Cybersecurity Framework should facilitate information-sharing between government and the private sector and should encourage widespread intelligence-sharing and limit provider exposure when engaging in good faith in such activities.

ITTA recognizes that the Executive Order and, thus, the Cybersecurity Framework cannot provide liability protection as an incentive for the private sector to participate in an information sharing program. To achieve the greatest participation by the private sector, however, ITTA has endorsed federal legislation that would provide liability protection to communications providers in exchange for participating in a voluntary information sharing program between government and the private sector.[4]

II. A ONE-SIZE-FITS-ALL APPROACH TO REGULATING CYBERSECURITY WILL COMPROMISE THE GOAL

America's communications networks can quickly adapt to meet the demands of both business and residential consumers while, at the same time, detecting and resolving cyber threats as they are discovered and become apparent. One of the greatest assets of the broadband components of the nation's communications networks is providers' ability to upgrade and manage their infrastructure to accommodate demand while adding additional security protection capabilities without having to deal with the regulatory burdens often associated with providing more traditional communications services.

[4] *See* H.R. 624, Cyber Intelligence Sharing and Protection Act of 2013 (CISPA).

ITTA cautions NIST against developing a Cybersecurity Framework that adopts mandatory performance metrics and enforces a one-size-fits-all approach to communications networks. Such an approach would tie the hands of communications providers and diminish the ability they have today to recognize and resolve a cyber-attack in its infancy before major damage can be done. As cautioned by ITTA member CenturyLink in testimony before Congress, "cybersecurity can devolve into a checklist exercise that diverts resources away from effective, evolving protections, into expensive compliance measures that may be already outdated by the time they are implemented."[5]

ITTA commends NIST for its statement that the Framework will incorporate "voluntary consensus standards and industry best practices to the full extent possible and will be consistent with voluntary international consensus-based standards when such international standards will advance the objective of the Executive Order."[6] However, although the NIST references the need for the Framework to be "flexible" and "voluntary," ITTA remains concerned regarding the provision of the Presidential Policy Directive that directs independent regulatory agencies, including the Federal Communications Commission ("FCC"), to exercise their authority and expertise and to partner with the Department of Homeland Security and the Department of State to identify risks and vulnerabilities within the telecommunications sector.[7]

Currently, the FCC's authority to adopt rules mandating certain cybersecurity measures by providers is very circumscribed. However, the parameters of the FCC's authority over the

[5] Congressional Testimony by Mr. David Mahon, Chief Security Officer, CenturyLink Communications, Subcommittee on Communications and the Internet Hearing, *Cybersecurity The Pivotal Role of the Communications Network* (March 7, 2012) at p.6.

[6] *RFI*, at 13025.

[7] Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013) ("PPD-21").

Internet is the subject of a pending case before the U.S. Court of Appeals for the District of Columbia[8] and depending upon the outcome of that case, any voluntary cybersecurity standard adopted by the industry could arguably be imposed by the FCC as a mandatory rule. To insure against this possible outcome, ITTA recommends that NIST and the other expert agencies working on creating the Cybersecurity Framework make clear that independent regulatory agencies will not be allowed to mandate or enforce industry best practices or industry standards but instead should foster a collegial, cooperative, and constructive voluntary framework to bring subject matter experts to the discussion table early and often for the betterment of our protection efforts.

Therefore, to better identify and assist NIST in the drafting of the Cybersecurity Framework, ITTA hereby identifies a number of well-recognized and successful frameworks, standards, guidelines, and best practices currently in place to help protect and assist communications providers in protecting their networks from cyber-attacks.

The Communications Security, Reliability and Interoperability Council ("CSRIC") has been a successful example of various industry participants coming together to identify potential solutions and create a beneficial set of voluntary best practices to advise and provide recommendations to the FCC on protecting consumers from cyber threats. In March 2011, CSRIC Working Group 2A produced a final report detailing cybersecurity best practices.[9]

---

[8] *Verizon v. FCC*, No 11-355 (D.C. Cir.).

[9] CSRIC Working Group 2A Final Report, *Cyber Security Best Practices* (Mar. 2011), available at http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG2A_Report_Cyber_Security_Best_Practices.pdf.

In addition, ITTA members have identified a number of internal procedures with regard to security governance that are consistent with or conform to ISO 27001[10] and NIST 800-53.[11] Examples include, but are not limited to, constant network monitoring on a real-time basis to identify potential threats to customers or to the network and processes for eliminating identified cybersecurity risks as they become apparent. In addition, all new network elements and their configurations undergo a rigorous security testing review before being deployed in the network and ITTA members place important network elements in locations that have appropriate physical security controls.

Finally, what is perhaps most important but the hardest to effectively and efficiently influence is proactive consumer education and awareness. ITTA members respect and protect the privacy of their customers with vigor while remaining compliant with applicable local, state, and federal law. Education of the public regarding cyber threats is often a joint public service project coordinated by ITTA members and local businesses, news publications, and through local and federal public safety and regulatory agencies (including the FCC). Therefore, ITTA recommends that NIST, when developing the Cybersecurity Framework, consider the importance and costs associated with consumer education of the potential threats of a cyber-attack and find opportunities to partner in educating consumers on basic "house cleaning" procedures they can perform on their computers and networks to mitigate potential cyber-attacks.

Many of the critical infrastructure customers served by ITTA members, including private financial institutions, investor-owned utility providers, and local, state, and federal government

---

[10] International Organization for Standardization ("ISO"), available at http://www.17799.com/.

[11] National Institute of Standards and Technology, *Recommended Security Controls for Federal Information Systems and Organization* (Aug. 2009), available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

agencies have also implemented internal procedures to protect their networks from cyber-attacks. The combination of internal protections and customer demand for specific security safeguards and protections has resulted in tens of millions of dollars annually being spent to safeguard communications networks. ITTA, as an association dedicated to advocacy for mid-size communications carriers, is also a useful forum for the sharing of information with companies of similar size and network capabilities. ITTA will continue to foster that interconnected dialogue as we move forward with our participation on this critical issue.

It should be kept in mind that the nation's communications networks are just one component in protecting our country's critical infrastructure. The responsibility to protect against cyber-attacks is a shared fiduciary and operational responsibility requiring involvement by numerous important constituencies including, but not limited to, the communications networks of our nation. While the analogy of the "weakest link" can often times be overused with respect to protecting our critical infrastructure from cyber-attack, the weakest link analogy is appropriate and efforts by policymakers to fill in the gaps in our cyber policy should appropriately be directed at the weakest links.

Respectfully submitted,

By: /s/ Paul Raak

Genevieve Morelli
Paul D. Raak
ITTA
1101 Vermont Ave., NW, Suite 501
Washington, D.C. 20005
(202) 898-1520
gmorelli@itta.us
praak@itta.us

April 8, 2013