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

In the Matter of	)	
	)	
	)	PS Docket No. 10-93
Cyber Security Certification Program	)	
	)	

To: The Commission

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association (TIA) hereby submits comments to the Federal Communications Commission (Commission) in the above-captioned proceeding.[1] TIA appreciates the opportunity to discuss the potential of creating a cyber security program within the Commission.

TIA represents the global information and communications technology (ICT) industry through standards development, advocacy, tradeshows, business opportunities, market intelligence and world-wide environmental regulatory analysis. With roots dating back to 1924, TIA enhances the business environment for broadband, mobile wireless, information technology, networks, cable, satellite and unified communications.

[1] *See* In the Matter of Cyber Security Certification Program, Notice of Inquiry, PS Docket No. 10-93 (rel. Apr. 21, 2010) (Cyber Security NOI)

Members' products and services empower communications in every industry and market, including healthcare, education, security, public safety, transportation, government, the military, the environment and entertainment. TIA is accredited by the American National Standards Institute (ANSI).

SUMMARY

Cyber security is vital to our nation, and much work is already being done in the federal government to protect against cyber attacks. In order to assess the level of risk of cyber attacks, better data must be assimilated. Moreover, certification programs have not been widely embraced to secure critical infrastructure and key resources (CIKR) by industry. However, there are several other incentives proffered that should increase cyber security efforts in the private sector. As the Commission considers its proposed certification program, it must assess likely impact upon global cyber security efforts. Finally, it should be noted that a cyber security program as proposed by the Commission could restrict entities from implementing flexible practices that respond to ever-changing cyber security needs.

DISCUSSION

I. MORE DATA IS NEEDED TO ASSESS THE THREAT OF CYBER ATTACK.

The Commission has provided some data indicating that there are significant threats to cyber security in the United States.[2] Reported annual increases in malware reports are routine, and different data establishing cyber threats is difficult to correlate across data

[2] *See id.* at 2-3 (noting increasing malware reports by PandaLabs, a commercial security enterprise).

sets. In fact, the Organisation of Economic Co-operation and Development (OECD) has recently reported that the level of malware contained in emails is difficult to comprehend due to disparate measurement techniques.[3] Accordingly, the level of cyber security cannot be measured without a more comprehensive assessment that evaluates disparate data from public and private interests to establish the severity of cyber security threats.

II. THE PROPOSED CERTIFICATION PROGRAM MAY NOT BE THE MOST EFFECTIVE PROTECTION AGAINST CYBER ATTACKS.

a. Ongoing Certification Initiatives Have Proven to Discourage Participation

Certifications, while valuable in many ways, are very difficult to establish for cyber security for several reasons. From a practical perspective, certifications can be time consuming and costly, and may delay important security related actions. An example can be gleaned from the Common Criteria for Information Technology Security Evaluation (CC) efforts. CC is an international standard for evaluating security functionality within products that are either primarily focused on providing information assurance capabilities or are focused on providing a specific functionality type that relies upon certain information assurance capabilities. In addition, the CC standard requires review of the developer's configuration management procedures, delivery processes, and development security controls in place to adequately ensure the evaluated product is properly maintained and securely delivered to the end-user. The ICT industry is very committed to the CC and is working to improve its ability to drive assurance in security products. However, over the past ten years, the CC process has been slow and costly to

[3] See The Organisation for Economic Co-operation and Development, Malware: A Security Threat to the Internet Economy 27 (2008), available at: http://www.oecd.org/dataoecd/53/34/40724457.pdf.

participating companies. These cost and time delays have proven to be a disincentive to participation by industry.

In another initiative, as the Commission notes in its NOI, the Department of Homeland Security is working on protecting Americans from cyber attacks through public-private initiatives.[4] While this is a preliminary program, it should be noted that participation is low. We suggest that the Commission survey this effort to determine its effectiveness prior to implementing potentially overlapping programs.

b. **Other Incentives Provide Effective Solutions to Cyber Threats**

A robust study by the IT Sector Coordinating Council was done in 2008 on incentives for cyber security as part of Project 12 of the Comprehensive National Cyber Initiative (CNCI).[5] That effort explored the possibility of voluntary certification programs for cyber security practices. After significant debate and discussion, the report determined that many other incentives would drive more secure systems. The report noted that cyber security best practices differ based upon CIKR dynamics:

> …no one perfect set of [cyber security] practices exists (due in part to the plethora of devices, applications, and versions of different technologies in use at any one time in a specific environment), and CIKR owners will be most successful in their endeavor to improve cyber security by assessing risk to their information systems and networks and seeking solutions that are commensurate with their unique risk profiles.[6]

---

[4] *See* Cyber Security NOI at 3.
[5] *See* Incentives Recommendations Report, Comprehensive National Cyber security Initiative, Cross Sector Cyber Security Working Group Incentives Subgroup, (September 2009) (CNCI Incentives Subgroup Report).
[6] *Id.* at 4.

Further, the report made clear that best practices must be adapted as technology and security needs change: "already-identified effective practices need to be continually adapted to keep pace with the changing technological and security needs that are inherent parts of the cyber landscape."[7]

Due to the identified disparate and ever-changing cyber security needs of entities, the CNCI Incentives Subgroup Report recommended several incentives for companies to maintain effective cyber security practices. Noticeably absent was a recommendation for a government-imposed certification program. First, the report stated a need to address Federal Government cyber security needs; there are opportunities to leverage the purchasing power of the Federal government to "incentivize companies that do business with the government to adopt good cyber security practices or deploy best known/successful methods to protect the systems and networks they own from attack and/or compromise."[8] Further, the report stated that grants should be provided to accelerate adoption of cyber security standards and practices.[9] Moreover, the report noted that the Federal government should reduce, rather than increase, regulatory complexity for CIKR.[10] In addition, the report stated, there should be direct federal funding for cyber security research and development (R&D) of new cyber security technologies and practices through one or more federally funded R&D centers or academic partnerships.[11] The report also made clear that the Federal government should

[7] *Id.* at 5.
[8] *Id.* at 7.
[9] *See id.* at 7-8.
[10] *See id.* at 8-9.
[11] *See id.* at 9-10.

extend grants to companies developing and implementing cyber security technologies and practices.[12]

As the CNCI Incentives Subgroup Report makes clear, the Federal government must provide incentives for cyber security enhancement among entities. The report lists non-certification steps that will most effectively accomplish this goal. These recommendations should be considered as primary steps that the federal government should take to ensure cyber security prior creating a certification program.

c. The Proposed Certification Program Could Negatively Affect Global Cyber Security Efforts.

Certification regimes such as that being discussed by the Commission tend to motivate other countries to also change existing requirements or create new security certification regimes. This can lead to overly expansive and intrusive security and certification requirements that are costly, risk exposure of technical information or intellectual property, create trade barriers, and do not improve security. Paradoxically, the expansion of multiple security certification schemes may ultimately weaken security by taking scarce resources away from actual security improvement.

Global schemes offer a better and more efficient alternative to a potentially bifurcated system of multiple third party security assessment and certification schemes. A bifurcated system could create barriers to trade, hinder U.S. competitiveness, and

[12] *See id.* at 10.

potentially compromise the intellectual property of vendors. It is important to note that certification schemes are inherently based on standards. Given the global nature of ICTs, these standards must be global in nature by definition. It is unclear what global standard will be considered for the proposed Commission program, but TIA urges the Commission to refrain from imposing country-specific standards or practices. Such action could again isolate U.S. cyber security efforts and create global reactions that could defeat the goal of ensuring superior cyber security protection.

III. A CYBER SECURITY CERTIFICATION PROGRAM COULD STIFLE NEEDED FLEXIBILITY

It is important to note that cyber security requirements vary from sector to sector and business to business. Thus, a "one size fits all" approach to cyber security certification is unlikely to result in more secure systems. Further, the cyber security space is rapidly changing, and certification schemes may not promote the flexibility necessary to address emerging and developing threats. However, if certification requirements are high-level enough to be acceptable by all parties and provide significant flexibility, they could result in the adoption of minimum requirements and best practices rather than the most robust, secure solutions and practices available.

IV. CONCLUSION.

For the foregoing reasons, TIA urges to take into consideration its recommendation on the Commission's proposed cyber security certification program.

Respectfully submitted,

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION

By: ___/s/_____

Danielle Coffey
Vice President,
Government Affairs

Patrick Sullivan
Director,
Technical and Government Affairs

TELECOMMUNICATIONS
INDUSTRY ASSOCIATION
10 G Street N.E.
Suite 550
Washington, D.C. 20002
(202) 346-3240

July 12, 2010