

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

COMMENTS

The Alliance for Telecommunications Industry Solutions (ATIS) hereby submits these comments in response to the April 21, 2010, *Notice of Inquiry (NOI)* in the above-referenced docket concerning the possible establishment of a voluntary cyber security certification program. ATIS does not believe that such a program is necessary. Service providers are already incited to provide secure and reliable broadband communications and there is significant and effective industry work targeted at cyber security. ATIS also notes that there are technical and practical challenges that may frustrate the implementation of an effective certification program. To enhance cyber security, ATIS recommends that the Commission consider instead supporting and publicizing industry cyber security work and enhancing its cyber security educational efforts.

I. Background

ATIS is a global standards development and technical planning organization that leads, develops and promotes worldwide technical and operations standards for information, entertainment and communications technologies. ATIS' membership is diverse and includes all stakeholders from the information and communications technologies industry – wireline and wireless service providers, equipment manufacturers, competitive local exchange carriers, providers of commercial mobile radio services, broadband providers, software developers, consumer electronics companies, digital rights management companies, and internet service providers.

Nearly 600 industry subject matter experts work collaboratively in ATIS' 18 open industry committees. ATIS' committees focus on a broad range of priorities, including network architectures and platforms, the ordering and billing of services, E-911, the seamless delivery of converged wireline and wireless services such as IPTV over multimedia platforms, and the networks of the future.

One of ATIS' core priorities relates to the reliability and security of communications networks. Such work is accomplished in the following ATIS committees:

Network Reliability Steering Committee (NRSC). NRSC strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry. The NRSC addresses network reliability improvement opportunities in an open environment and advises the communications industry through the development of standards, technical requirements, technical reports, bulletins, Best Practices, and annual reports. The NRSC is comprised of industry experts with primary responsibility for examining, responding to and preventing outages for communications companies. NRSC is also reviewing cyber security Best Practices.

Network Performance, Reliability and Quality of Service Committee (PRQC). PRQC develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks. PRQC also identifies and defines performance and measurement parameters for the speed, accuracy, dependability, availability, and robustness of connection establishment/disengagement and information transfer, and develops transmission planning guidance for the deployment of signal processing devices such as echo cancellers and VoIP elements.

Packet Technologies and Systems Committee (PTSC). PTSC develops and recommends standards and technical reports related to packet services, architectures, and signaling, and related subjects, including next generation carrier interconnection, and signaling architecture and control. One of PTSC's subcommittees, Security (PTSC SEC), develops and recommends implementable security standards for evolving packet-based network technologies and their interworking with other networks.

Telecommunications Fraud Prevention Committee (TFPC). TFPC identifies and addresses fraud vulnerabilities for current and future networks, architectures, services, and products. TFPC works with network security and architectural experts to investigate current fraud activities within the industry and develop and publish recommendations to mitigate identified vulnerabilities.

II. The Proposed Cyber Security Certification Program Is Not Necessary

The central question in the *NOI* is whether the Commission should establish a voluntary incentive-based certification program under which providers could receive security assessments by third-party auditors based on compliance with cyber security practices.¹ While ATIS supports the Commission's goal of enhancing cyber security, ATIS does not believe that such a program is necessary to provide incentives for broadband service providers to implement cyber security practices. ATIS also believes that, given the significant work underway in the industry related to cyber security, such a program is not necessary to enhance existing security practices.

It is very important to note that service providers have every incentive to provide

¹ *NOI* at ¶12.

reliable and secure broadband service to consumers. Service providers' businesses depend on the provision of such communications and they invest heavily in protecting and enhancing their networks.² The provision of reliable and secure communications is particularly important given the competitive nature of the US broadband market, in which most customers may choose from multiple wireline and mobile broadband providers.³ Therefore, reliability and security are vitally important to providers in their efforts to attract new, and retain existing, customers. Compared to these marketplace incentives, the existence of a voluntary or mandated cyber security certification program would be insignificant.

ATIS notes that the proposed certification program appears to be based on the belief that the existing industry work is not sufficient or effective in addressing cyber security. The Commission questions whether there is wide-spread adherence to Network Reliability and Interoperability Council (NRIC) cyber security Best Practices and whether providers have an effective way of benchmarking their cyber security practices against those of competing providers and states that, in its opinion, these Best Practices provide too little specific guidance for network operators to meet objectively measurable security criteria.⁴

ATIS disagrees that the industry's cyber security work is insufficient to protect networks and consumers. Significant work has been completed and is underway by the industry to promote and enhance reliability and security. For instance, many of ATIS'

² The ten largest service providers have annual capital investments in excess of \$50 billion. Connecting American: The National Broadband Plan at p. 18

³ *Id.* at pp. 37, 39.

⁴ *NOI* at ¶7.

committees have initiated work programs that are related to these issues. The ATIS NRSC has begun an examination of cyber security as part of its mission to enhance the reliability of communications networks and has initiated an examination of industry cyber security Best Practices. The ATIS PTSC is developing security and authentication standards regarding Next Generation Networks and is working on security guidelines and standards for external interfaces, such as User to Network Interfaces, Access Network Interfaces and Network to Network Interfaces (NNI). The ATIS Chief Information Officer (CIO) Council, which identifies and discusses information technology (IT) issues, is addressing the IT impacts of cyber security on service provider data networks. There are also numerous other groups working on cyber security issues, including the Communications Security, Reliability and Interoperability Committee (CSRIC), which has a working group specifically tasked with examining cyber security Best Practices.⁵

ATIS notes that the industry's work in the cyber security arena has been and continues to be effective. For example, industry-developed voluntary NRIC security Best Practices are extremely important and widely-used tools. As applicable, individual service providers have also developed and implemented their own security practices that incorporate the relevant elements of these NRIC Best Practices. ATIS believes that its NRSC is another good example of how the industry has been effective in its efforts to enhance reliability and security. Through its consensus-based and open processes, the

⁵ CSRIC Working Group 2A's mission includes taking "a fresh look at cyber security best practices, including all segments of the communications industry and public safety communities."

NRSC develops and updates voluntary standards and Best Practices that represent the best thinking of the industry.⁶

III. There are Technical and Practical Challenges to Creating an Effective Cyber Security Certification Program

ATIS also notes that there are technical and practical challenges to the development and implementation of an effective cyber security certification program.

For example, because broadband networks are extremely complex ecosystems, a certification program would not be effective in addressing all aspects of network security. The security of these networks is affected by technologies that are put in place and managed by service providers; as well as, by equipment that is under the exclusive control of end-users. Given that significant vulnerability stems from client-side (i.e. end-user) equipment and applications, any provider-based certification program may not prevent security issues that arise from consumer equipment or applications.

Moreover, given the evolving nature of broadband networks and technologies, ATIS does not believe that any certification program could provide an accurate and up-to-date assessment of security. Networks have changed substantially since the first broadband services were offered. New technologies have significantly improved the speeds of these networks and have allowed for the emergence of new platforms. Accompanying the evolution of the network has been an advancement of cyber security practices and technologies driven by providers' needs to compete successfully while offering reliable, secure communications. Consequently, any certification program assessment of cyber

⁶ The ATIS NRSC recently submitted its industry-developed best practices to the Commission's CSRIC for consideration as CSRIC best practices.

security would quickly become out-of-date.

In addition to the technical issues outlined above, ATIS also believes that there are practical challenges to the development and implementation of a certification program. For instance, ATIS believes that there may be significant risks associated with service providers sharing information regarding their implementation of cyber security Best Practices under a certification program. This information may contain commercially sensitive information pertaining to a providers' network. Such information may also contain details that are sensitive from a security perspective and that could be misused if they were to fall into the hands of bad actors.

It also may be very difficult to assess security based on Best Practices, technical specification or standards. As noted above, carriers use a combination of existing Best Practices and carrier-specific security measures to protect their networks. Such decisions are made based on evaluations by security subject matter expert evaluations, risk assessments, and/or other considerations. In some situations, an industry Best Practice may be superseded by a more stringent provider-specific internal practice that is unique to that provider's technology or network.

Another concern associated with the certification program is whether this program will actually benefit consumers. ATIS believes that the cyber security certification program could confuse or mislead consumers regarding the security of broadband networks. Consumers may not understand, for example, that certification does not guarantee the security of the network against all current and future threats or that the steps

taken to secure the network may not fully protect their equipment and/or applications from cyber threats.

IV. Alternative Cyber Security Measures Should Be Considered

In the *NOI*, the Commission asks whether there are other cyber security measures that the Commission should consider to enhance cyber security and raise awareness of Best Practices.⁷ As ATIS has stated above, ATIS does not believe that a cyber security certification program is necessary or will be effective. As an alternative, ATIS recommends that the Commission: (1) continue its participation in, and support of, industry groups such as the ATIS NRSC that work to enhance network reliability and security through voluntary consensus-based processes; (2) publicize industry work; and (3) enhance consumer education and awareness of its educational efforts on cyber security issues, including digital hygiene (e.g. not sharing user ids or passwords, password protecting important documents, not opening email attachments from unknown sources, not accepting SPAM, etc.). ATIS also recommends that the Commission consider holding workshops to educate the public on the final report of the CSRIC Cyber Security Working Group.

⁷ *NOI* at 59.

V. Conclusion

While ATIS supports the Commission's goal of enhancing cyber security, ATIS does not believe that a voluntary or mandated cyber security certification program is necessary. Service providers are already incented to provide secure and reliable broadband communications and there is significant industry work targeted at cyber security. There are also technical and practical challenges to the development and implementation of an effective certification program. ATIS recommends that the Commission consider instead supporting and publicizing industry cyber security work and enhancing its cyber security educational efforts.

Respectfully submitted,

Alliance for Telecommunications Industry Solutions
By:



Thomas Goode
General Counsel

Dated: July 12, 2010