



## TABLE OF CONTENTS

	<b>Page</b>
I. INTRODUCTION AND SUMMARY .....	1
II. CYBER SECURITY IS A CRITICAL COMPONENT OF WIRELESS NETWORK MANAGEMENT .....	2
III. VOLUNTARY INDUSTRY EFFORTS HAVE BEEN LARGELY SUCCESSFUL IN ESTABLISHING PRACTICES AND TECHNIQUES FOR PROTECTING WIRELESS NETWORKS .....	4
IV. COMMISSION-ESTABLISHED CERTIFICATION REQUIREMENTS ARE UNLIKELY TO SIGNIFICANTLY PROMOTE CYBER SECURITY .....	6
V. CONCLUSION.....	10



As a result, wireless broadband service providers have been largely successful in preventing serious cyber attacks to this point, due to their use of dynamic network management techniques.

In addition to the efforts of individual service providers to protect their networks, significant industry-wide collaborative initiatives to share information and develop best practices are ongoing. CTIA and its member companies participate in numerous industry programs and public-private partnerships focused on issues central to cyber security. Through these efforts, the industry is constantly developing new security techniques to protect the entire wireless broadband ecosystem.

While CTIA acknowledges the importance of cyber security, CTIA believes the proposed voluntary certification program may not have the desired outcome. In addition to being logistically challenging, the program is unlikely to provide sufficient flexibility to address the realities of cyber threats, and it may even leave networks more vulnerable to attack. The Commission could better promote cyber security by coordinating its efforts with those already underway by other federal agencies and focusing on public-private partnerships such as the Communications Security, Reliability, and Interoperability Council; the National Communications System; and the United States Computer Emergency Readiness Team.

## **II. CYBER SECURITY IS A CRITICAL COMPONENT OF WIRELESS NETWORK MANAGEMENT.**

As discussed extensively at the FCC's September 30, 2009 National Broadband Plan workshop on cyber security, cyber attacks are fluid and ever-evolving, so methodologies and practices also must be dynamic to respond immediately to new threats.<sup>3</sup> Fortunately, mobile broadband networks, which are closely monitored by network operators, and wireless devices,

---

<sup>3</sup> See generally Remarks at the Cyber Security Workshop (Sept. 30, 2009) transcript available at [http://www.broadband.gov/docs/ws\\_26\\_cyber\\_security.pdf](http://www.broadband.gov/docs/ws_26_cyber_security.pdf) ("Cyber Security Workshop Transcript").

which run on many different operating system platforms and often have built-in security measures beyond those on PC operating systems, are generally recognized as being secure.

In the NOI, the Commission asserts a belief that there is insufficient information in the marketplace for consumers to gauge the level of cyber security protection offered by communications service providers and that “[t]he reduced incentive for heightened cyber security likely is compounded because a particular provider may not be motivated to exceed the security level” of other network operators.<sup>4</sup> The reality of the competitive wireless broadband ecosystem is actually quite different. Wireless service providers have extensive market incentives to invest in state-of-the-art cyber security measures because of steep competition based on network reliability and service quality. Because they are so rare, significant breaches of wireless broadband network security receive substantial attention and can have very real consequences in the marketplace. Furthermore, because true mobile broadband service is still in its infancy, it is essential that users trust the security of their personal information if adoption of next generation wireless broadband networks is to flourish. Unless wireless broadband service providers predict and respond to the constantly morphing and growing cyber security challenges with dynamic and secure infrastructure protections, customer confidence will suffer—leading to loss of subscribers and revenue.

The key to providing effective cyber security and thereby maintaining consumer trust is careful and targeted network management. Because cyber attackers are both ingenious and highly motivated, any static defenses are likely to be quickly defeated and exploited—meaning that wireless service providers must be constantly vigilant. Thus, network security is quite literally a 24-hour-a-day commitment for network operators. As described at the Commission’s

---

<sup>4</sup> NOI at 4348, ¶ 7.

cyber security workshop, broadband network management techniques range from spam blocking and monitoring of traffic patterns from known origins of malicious activity (*e.g.*, botnets or spam generators) to tracking of different trends on the ports of the networks themselves. Further complicating the situation for mobile network operators are the special concerns imposed by the temporal and geographic nature of network use in a spectrally-constrained environment. Network management activities must be keyed in to these practical realities so that legitimate spikes in traffic are recognized and accommodated and service quality is maintained throughout the network.

To complement this network monitoring, it is crucial for broadband service providers to have the flexibility to address perceived threats dynamically and effectively. Wireless providers and manufacturers are constantly responding to newly identified vulnerabilities as quickly and efficiently as possible, however, it is impossible to stop every attack. Because the success of their businesses hinges on the robust availability of their service, no regulatory regime could provide a better incentive for wireless broadband service providers to innovate and invest in cyber security than already exists in the marketplace. As discussed further below,<sup>5</sup> any prescriptive set of practices and security criteria established by a regulatory body are likely to be quickly outdated, leaving them at best irrelevant and at worst an impediment to implementing new and innovative measures to combat cyber risks.

### **III. VOLUNTARY INDUSTRY EFFORTS HAVE BEEN LARGELY SUCCESSFUL IN ESTABLISHING PRACTICES AND TECHNIQUES FOR PROTECTING WIRELESS NETWORKS.**

The success of the wireless industry's cyber security practices is best evidenced by the relative lack of major exploits of cyber vulnerabilities on wireless broadband networks to date.

---

<sup>5</sup> See Section IV. *infra*.

Where vulnerabilities have been exposed, however, they generally have been addressed quickly and proactively in an attempt to minimize any potential consumer harm. Yet, the wireless industry is not resting on its laurels. Efforts to develop and implement improved cyber security practices have been ongoing for years within the industry, and continue in earnest.

One example of an industry-led initiative to integrate cyber security planning into the business practices of wireless broadband service providers is CTIA's Business Continuity / Disaster Recovery program. As discussed in detail in CTIA's recent comments submitted in response to the *Network Survivability NOI*,<sup>6</sup> the Business Continuity / Disaster Recovery program offers certification to wireless network operators who demonstrate that they have designed and implemented strategies to prevent and respond to network damage resulting from emergencies and that they have taken steps to ensure continuity of service during such times. Cyber attacks are among the risks that must necessarily be planned for and addressed through the Business Continuity / Disaster Recovery program, and participating network operators have plans in place to address such occurrences.

Wireless broadband service providers also utilize a number of other industry best practices to reasonably manage and fortify their networks against cyber attacks. Among these, network operators have the benefit of the extensive best practices promulgated by the Network Reliability and Interoperability Council ("NRIC"), which issued over 200 recommendations pertaining specifically to cyber security.<sup>7</sup> Last year, the Commission rechartered the Communications Security, Reliability, and Interoperability Council ("CSRIC"), whose

---

<sup>6</sup> See Comments of CTIA – The Wireless Association®, PS Docket No. 10-92, at 5-6, Appx. A (filed June 25, 2010).

<sup>7</sup> See "NRIC Best Practices" <https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm> (last visited July 9, 2010).

recommendations are certain to provide another equally useful set of tools for wireless providers to employ in securing their networks.<sup>8</sup> CTIA and several wireless industry members are represented in the CSRIC membership and are continuing their active collaboration with this important body.

There are literally dozens of other federal and local agencies with which the wireless industry collaborates to address cyber security and network reliability issues. For example, CTIA and its operator members work closely with the National Communications System (“NCS”) and the United States Computer Emergency Readiness Team (“US-CERT”) to share information when unusual activities are detected and to fortify networks to minimize vulnerabilities. The result of this widespread coordination has been the development of a constantly evolving core of knowledge, techniques and best practices that have promoted effective cyber security throughout the wireless industry.<sup>9</sup>

#### **IV. COMMISSION-ESTABLISHED CERTIFICATION REQUIREMENTS ARE UNLIKELY TO SIGNIFICANTLY PROMOTE CYBER SECURITY.**

Although the Commission’s desire to promote further cyber security innovation by industry and awareness by consumers is laudable, serious implementation problems as well as questions regarding actual consumer benefit undercut the likely effectiveness of the proposed voluntary certification program. Instead, the Commission should focus on collaborating with

---

<sup>8</sup> See “CSRIC” <http://www.fcc.gov/pshs/advisory/csric/> (last visited July 9, 2010).

<sup>9</sup> It is worth noting that legislation currently before the U.S. Congress would further promote coordination between industry and the government in developing improved cyber security practices. For example, the Rockefeller-Snowe Cybersecurity Act of 2009 contemplates the creation of a “Cybersecurity Advisory Panel” composed of private sector, government and academic experts, as well as the promotion of increased cyber security research and development through the National Science Foundation and the establishment of the Department of Commerce as a clearinghouse for information related to the security of critical infrastructure networks. See Cyber Security Act of 2009, S. 772, 111th Cong. (2009).

other government agencies and public-private partnerships to have a more positive impact on cyber security.

At best, the certification program appears to offer little additional benefit and will likely not elicit broad support; at worst it could actually make the job of securing networks more difficult for broadband service providers. CTIA is concerned that the publication of industry-wide cyber security standards could increase the overall vulnerability of participating networks. By announcing a uniform framework for industry cyber security practices, the certification program risks service providers' expending significant resources that ultimately may provide a clear roadmap for hackers and other bad actors to circumvent network protections and exploit security vulnerabilities. Moreover, as discussed above, cyber security currently forms one basis for competition between carriers seeking to provide greater service reliability and consumer protection than other market participants. By providing a single set of standards that all operators could choose to adopt, the Commission risks removing this competitive dynamic and the constant innovation it breeds.

The potential beneficial effects of the proposed certification program are also limited by its narrow scope. Today, most cyber attacks are accomplished through exploiting vulnerabilities in operating systems and applications, as opposed to weaknesses in the network itself. Although service providers are constantly striving to provide the best protection for their users, there is only so much that can be accomplished from the network operator perspective when users run compromised applications. As the FCC and the public have embraced "open" operating systems, applications, handsets, and unlicensed Wi-Fi networks and carriers have abandoned the earlier "walled garden," any approach to cyber security should recognize that users must take responsibility for safeguarding their own security. Indeed, wireless carriers increasingly may not

even play a role in their subscribers' Internet access through a wireless device and may have no visibility into the subscriber's online use at all. The Commission's efforts to provide consumers with information shouldn't mislead consumers into thinking their carrier necessarily can safeguard their wireless broadband use of open applications or unlicensed Wi-Fi networks. Thus, the proposed certification program, by purporting to apply additional compliance burdens only on network operators, will likely only serve to reduce their operational flexibility without having a measurable effect on these other aspects of the broadband ecosystem that may actually represent a greater overall threat.

Above all else, to best protect their networks, wireless broadband service providers require flexibility to be innovative and dynamic in their responses to cyber threats. The nature of cyber threats often changes more quickly than the techniques used to combat them. Even where a vulnerability is recognized and a fix designed before an exploit happens, often the publication of this fix leads cyber attackers to develop and distribute an exploit before the public has time to respond. When suspicious activity or a new attack is detected on the network, service providers must respond immediately and effectively before widespread damage occurs.

In light of this need for flexibility, industry-wide certification criteria that are meaningful and effective would be difficult to compose. Any government-established, fixed standards or practices would be soon outdated by the quick pace of development of cyber threats. It is highly unlikely that this process would facilitate the needed nimble, rapid response and development of new protective measures to counter the latest iterations of cyber attacks. Yet network providers would be put in the situation of having to direct resources to abiding by established certification criteria that may serve to hamstring other initiatives that providers could (and should) be taking. This strict compliance with the program could very well reduce the ability of network operators

to respond appropriately to potential vulnerabilities. To the extent the Commission could craft certification standards that are sufficiently flexible to fit the amorphous demands of effective cyber security, these standards would likely provide no more specificity or greater protection than the steps already being taken by the industry.

Finally, it is unclear that the Commission is truly the most appropriate agency within the Federal government to be overseeing such an effort in light of the numerous other efforts already planned or underway at different agencies. The Department of Homeland Security may have more insight and experience with cyber security issues, particularly due to its operation of the National Cybersecurity and Communications Integration Center (“NCCIC”). The Department of Commerce and the National Telecommunications and Information Administration (“NTIA”) are also investigating cyber security issues.<sup>10</sup> Moreover, multiple pieces of legislation currently before the U.S. Congress would establish a permanent, Senate-confirmed office within the Executive Office of the President with virtually plenary supervisory authority over all Federal cyber security initiatives.<sup>11</sup>

Indeed, a common complaint about the Federal government’s approach to cyber security is that it is overly balkanized and uncoordinated, with various agencies performing duplicative or even conflicting actions. To illustrate, the Government Accountability Office (“GAO”) recently released an analysis of the cyber security research and development (“R&D”) initiatives being

---

<sup>10</sup> See, e.g., National Telecommunications and Information Administration, Cybersecurity and Innovation in the Information Economy, Meeting Notice, 75 Fed. Reg. 36633-34 (June 28, 2010).

<sup>11</sup> See A Bill To Establish, Within the Executive Office of the President, the Office of National Cybersecurity Advisor, S.778, 111th Cong. (2009); Cyber Security Act of 2009, S. 772, 111th Cong. (2009); Protecting Cyberspace as a National Asset, S3480 111th Cong. (2010). Indeed, both the Rockefeller-Snowe and the Lieberman bills include mechanisms by which key industry members would share information with the government and attempt to develop best practices. In some cases, these bills provide important liability and confidentiality protections for participating industry members that are not contemplated in the Commission’s proposal.

pursued by the Federal government.<sup>12</sup> Ultimately, the report concludes that although steps to coordinate the various cyber security R&D programs have been taken, significant challenges still exist that demand strong central coordination. “Specifically, the absence of a national cybersecurity R&D agenda and leadership increases the risk that efforts will not reflect national priorities, key decisions will be postponed and federal agencies will lack overall direction for their efforts.”<sup>13</sup>

Although CTIA does not endorse any particular solution to these larger coordination challenges at this time, the GAO report demonstrates that there are significant gains to be made from streamlining and improving processes within the government itself that do not pose the same risks of hindering existing private sector efforts as the Commission’s current proposal. CTIA believes that the current industry practices, based on voluntary procedures and guidelines, is the appropriate framework and allows wireless service providers the flexibility to respond to cyber threats. Any government activity in this area should be focused and fully coordinated with all affected and interested agencies.

## **V. CONCLUSION**

The wireless industry recognizes the crucial role of cyber security and the competitive need to remain constantly vigilant with respect to the protection of its consumers’ information. The key to effective cyber security is reasonable and intelligent network management informed by industry-developed best practices and strategies. Although CTIA shares the Commission’s desire to see the nation’s wireless broadband networks even further fortified against cyber attack, it has significant doubts about the effectiveness of the proposed voluntary certification program.

---

<sup>12</sup> See Government Accountability Office, Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development, GAO-10-466 (June 2010) available at <http://www.gao.gov/new.items/d10466.pdf>.

<sup>13</sup> *Id.* at 21.

CTIA urges the Commission to seek out opportunities to collaborate with other Federal agencies in promoting cyber security to achieve the most effective and focused results.

Respectfully submitted,

By: /s/ Brian M. Josef

Brian M. Josef  
Director, Regulatory Affairs

Christopher Guttman-McCabe  
Vice President, Regulatory Affairs

Michael F. Altschul  
Senior Vice President and General Counsel

**CTIA-The Wireless Association®**  
1400 Sixteenth Street, NW  
Suite 600  
Washington, DC 20036  
(202) 785-0081

July 12, 2010