

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

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

To: The Commission

**REPLY COMMENTS OF T-MOBILE USA, INC.**

T-Mobile USA, Inc. (“T-Mobile”) hereby replies to comments submitted in response to the Commission’s *Notice of Inquiry* in the above-referenced proceeding.<sup>1</sup> T-Mobile agrees with the vast majority of commenting parties that Commission involvement in wireless broadband cyber security is not necessary at this time.<sup>2</sup> In the highly competitive mobile broadband wireless marketplace, wireless carriers such as T-Mobile have enormous market-driven incentives to protect the security of broadband infrastructure. Moreover, as discussed below, the adoption of cyber security guidelines may actually undermine industry efforts. T-Mobile believes the better approach would be to work toward consolidating the various existing cyber security efforts and to support the current endeavors of broadband providers and other relevant

---

<sup>1</sup> *In the Matter of Cyber Security Certification Program*, PS Docket No. 10-93, *Notice of Inquiry*, 25 FCC Rcd 4345 (2010) (“*NOR*”).

<sup>2</sup> See Alliance for Telecommunications Industry Solutions (“ATIS”) Comments, PS Docket No. 10-93, at 1 (July 12, 2010); AT&T Inc. Comments, PS Docket No. 10-93, at 2 (July 12, 2010); CTIA – The Wireless Association® (“CTIA”) Comments, PS Docket No. 10-93, at 1 (July 12, 2010); MetroPCS Communications, Inc. (“MetroPCS”) Comments, PS Docket No. 10-93, at 1, 6 (July 12, 2010); National Cable & Telecommunications Association (“NCTA”) Comments, PS Docket No. 10-93, at 1 (July 12, 2010); Qwest Communications International Inc. (“Qwest”) Comments, PS Docket No. 10-93, at 4, 8-13 (July 12, 2010); Sprint Nextel Corporation (“Sprint”) Comments, PS Docket No. 10-93, at 1 (July 12, 2010); Telecommunications Industry Association (“TIA”) Comments, PS Docket No. 10-93, at 3-6 (July 12, 2010); Verizon and Verizon Wireless (collectively “Verizon”) Comments, PS Docket No. 10-93, at 1 (July 12, 2010).

stakeholders to defend their networks against cyber threats, particularly in light of current Executive Branch and legislative efforts to comprehensively address the issue.

**I. MARKET-BASED INCENTIVES AND BEST PRACTICES ENSURE THAT CARRIERS ADEQUATELY ADDRESS CYBER SECURITY**

The proposed cyber security certification program appears to be premised on the belief that broadband providers lack incentives to ensure cyber security.<sup>3</sup> The record is not fully supportive of this rationale.<sup>4</sup>

The wireless broadband market is highly competitive. And, a strong brand and image are essential to retaining and attracting subscribers.<sup>5</sup> Although rare, significant cyber security breaches are highly publicized and detrimental to the organizations subject to such breaches. Customers that lose critical data or have personal information stolen are more likely to switch providers to remedy the perceived security flaws. As a result, wireless broadband providers have every business incentive to manage their networks to ensure ample protections are in place for safeguarding network and consumer information, and to maintain service continuity even in the event of a cyber attack. Indeed, wireless carriers continuously work to enhance practices that ensure cyber security and to quickly remedy any breaches even in the absence of government mandates.

---

<sup>3</sup> See *NOI*, 25 FCC Rcd at 4346 (indicating that the program may be necessary to “create business incentives for providers of communications services to sustain a high level of cyber security culture and practice”); *id.* at 4348 (indicating that the lack of public information regarding the cyber security practices of carriers “likely removes at least one significant incentive for providers fully to implement the NRIC best practices, in that they do not risk losing customers to networks with better security practices”).

<sup>4</sup> ATIS Comments at 3-4; AT&T Comments at 8-16; MetroPCS Comments at 2; Sprint Comments at 3-4; USTA Comments at 1, 6-7; Verizon Comments at 2-8.

<sup>5</sup> See T-Mobile Comments, PS Docket No. 07-114 at 11 (Nov. 12, 2009).

As a charter member of the Commission’s Communications Security, Reliability, and Interoperability Council (“CSRIC”), and participant on predecessor advisory councils, T-Mobile has demonstrated an ongoing commitment to promoting cyber security. In addition, T-Mobile is a member of the Alliance for Telecommunications Industry Solutions (“ATIS”),<sup>6</sup> which has two committees addressing security issues: the Network Performance, Reliability and Quality of Service Committee,<sup>7</sup> and the Packet Technologies and Systems Committee.<sup>8</sup>

Key, high ranking personnel at T-Mobile serve on standards bodies and advisory councils who actively evaluate cyber security issues. For instance, T-Mobile’s Senior Vice President for Engineering Operations sits on the CSRIC. In addition, T-Mobile Directors serve as co-chairs of various sub-teams for CSRIC Working Group 6, including the Cyber Security Sub-Team, which focuses on developing and organizing cyber security best practices.<sup>9</sup> T-Mobile’s Chief Network Officer serves on the ATIS Board of Directors.

Moreover, T-Mobile has been involved with the Department of Homeland Security’s (“DHS”) transition to a consolidated cyber security watch program, the National Cybersecurity and Communications Integration Center (“NCCIC”), and is aligned with the International

---

<sup>6</sup> See <http://www.atis.org/about>; <http://www.atis.org/Membership/members.html> (Develops standards for the telecommunications industry and is accredited by the American National Standards Institute (“ANSI”)); *see also* ATIS Comments at 2.

<sup>7</sup> See <http://www.atis.org/0010/index.asp> (Recommends standards related to, among other things, “security aspects of communications networks”).

<sup>8</sup> See <http://www.atis.org/0191/sec.asp> (Through its Security Subcommittee, “[c]oordinates and develops implementable security standards relevant to packet-based US telecommunications networks.”); *see also* ATIS Comments at 2-3.

<sup>9</sup> See Communications Security, Reliability & Interoperability Council (CSRIC) Members, *available at* <http://www.fcc.gov/pshs/advisory/csric/members.html>; Working Group 6 membership *available at* <http://www.fcc.gov/pshs/advisory/csric/wg-6-members.pdf>.

Organization for Standardization (“ISO”) 27000-series, which provides best practice recommendations on information security management and controls.

Given the marketplace incentives to ensure cyber security and the efforts undertaken by wireless carriers to date, in addition to the existing federal government initiatives, a cyber security certification program is not critical. T-Mobile, as well as other wireless carriers and broadband providers, already recognize the importance of cyber security – and network security in general – and continuously strive to ensure cyber security in the absence of formalized Commission standards.<sup>10</sup>

## **II. ADOPTION OF A VOLUNTARY CYBER SECURITY CERTIFICATION PROGRAM MAY UNDERMINE CYBER SECURITY**

T-Mobile agrees with a common theme expressed throughout many of the comments – a voluntary cyber security certification program may not necessarily enhance cyber security, but actually undermine existing efforts.<sup>11</sup> First, the proposed certification program is focused on network security rather than security issues relating to actions taken by end-users that are unrelated to the network,<sup>12</sup> and where the bulk of security problems arise.<sup>13</sup> As noted in the Brecht Concept Paper: “human operators, manufactured and custom computer software, and manufactured computer hardware each contribute more relative vulnerability than does the

---

<sup>10</sup> See ATIS Comments at 1, 3-6; AT&T Comments at 8-16; CTIA Comments at 2-4; MetroPCS Comments at 2-4; NCTA Comments at 2-3, 8; Qwest Comments at 11.

<sup>11</sup> See AT&T Comments at 17-20; CTIA Comments at 7; NCTA Comments at 5-6; Sprint Comments at 4-8; TIA Comments at 3 (“certifications can be time consuming and costly, and may delay important security related actions”), 6-7; USTA Comments at 7-10; Qwest Comments at 12.

<sup>12</sup> See ATIS Comments at 6; AT&T Comments at 4-6; CTIA Comments at 8; NCTA Comments at 8-9; Qwest Comments at 8-9; USTA Comments at 3, 5.

<sup>13</sup> See CTIA Comments at 7; USTA Comments at 17 (citing a recent report by the SANS Institute and a concept paper submitted by Lyle A. Brecht of Capital Markets Research as part of the White House’s sixty-day cyber review (“Brecht Concept Paper”).

network infrastructure.”<sup>14</sup> Although one commenter mentioned attempted cyber attacks on network providers,<sup>15</sup> there is no other mention by commenters in the record that there have been significant cyber security breaches on the network-side. Thus, the proposed certification program appears to be a regulatory solution to a non-existent (or relatively small) problem.<sup>16</sup> In contrast, a focus on educating consumers about security measures may be beneficial in helping to mitigate potential threats.

Second, networks are not uniformly designed, and therefore it will be difficult to develop uniform industry standards.<sup>17</sup> Although some networks may share similar characteristics, such as the air interface protocol used, the configuration of each network will vary greatly based on company-specific business models.<sup>18</sup> Thus, adoption of uniform cyber security standards may penalize some companies whose networks do not easily fit within the scope of the standards or create unique problems not envisioned by the standards.

Third, cyber threats are dynamic, thus requiring broadband networks providers to continuously adjust to evaluate these potential vulnerabilities. It is essential that broadband providers continue to have the flexibility to implement new security protocols based on new network designs and to address emerging cyber threats. It would be challenging for any cyber

---

<sup>14</sup> See *National Cyber Systems Infrastructure Security Review* (Feb. 15, 2009) available at <http://www.whitehouse.gov/files/documents/cyber/Brecht%20Lyle%20-%20NATIONAL%20CYBER%20SYSTEMS%20INFRASTRUCTURE%20SECURITY%20REVIEW%20CONCEPT%20PAPER.pdf>.

<sup>15</sup> Qwest Comments at 9.

<sup>16</sup> A certification program risks giving consumers misplaced expectations regarding the security of networks by de-emphasizing the impact of consumer actions on security. See, e.g., ATIS Comments at 7-8; AT&T Comments at iii.

<sup>17</sup> See MetroPCS Comments at 3, 5; Sprint Comments at 6-7.

<sup>18</sup> See MetroPCS Comments at 3; Sprint Comments at 6-7.

security certification program to keep pace with this rapid evolution.<sup>19</sup> Any standards adopted for a certification program would be outdated virtually on the date of adoption.<sup>20</sup>

T-Mobile also agrees with commenters that the adoption of a cyber security certification program may unintentionally undermine cyber security.<sup>21</sup> As CTIA noted:

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 . . . 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.<sup>22</sup>

Because broadband providers currently have the flexibility to design and deploy different security protocols, it is more difficult for bad actors to undermine the security of numerous networks at once. If broadband providers are required to follow a common security protocol for purposes of obtaining a cyber security certification, however, the possibility of widespread network breaches increases. Specifically, if a hacker is able to breach one of these required

---

<sup>19</sup> See ATIS Comments at 6-7; MetroPCS Comments at 3.

<sup>20</sup> See ATIS Comments at 6-7; AT&T Comments at 18; CTIA Comments at 8; MetroPCS Comments at 7; Sprint Comments at 6. Rather than focus on additional cyber security initiatives, the Federal Government should take steps to deter bad actors by increasing the penalties associated with compromising broadband networks and end-user computers and applications. *Accord* AT&T Comments at n. 2. Given the proliferation of cyber threats by hackers targeted at end-user software applications, existing laws and regulations clearly do not provide the necessary deterrence. In fact, there are numerous stories of hackers being rewarded by the government with high paying jobs. See, e.g., "Hacker 'Mudge' gets DARPA job," CNET News (Feb. 10, 2010) available at [http://news.cnet.com/8301-27080\\_3-10450552-245.html](http://news.cnet.com/8301-27080_3-10450552-245.html); "For hire: Hackers to help Pentagon prevent attacks," CNN (Aug. 1, 2000) available at <http://edition.cnn.com/2000/TECH/computing/08/01/pentagon.at.defcon.idg>.

<sup>21</sup> See AT&T Comments at 17-20; CTIA Comments at 7; NCTA Comments at 6; Qwest Comments at 12; Sprint Comments at 7-8.

<sup>22</sup> CTIA Comments at 7.

security measures, the vulnerability will be shared by all providers with the security certification.<sup>23</sup> The risk of such bad acts is magnified by the lack of confidentiality protections under the proposed certification program.<sup>24</sup> Moreover, a certification program may unintentionally stifle the development of cutting edge, innovative security measures out of concern that such measures may run afoul of the program guidelines.<sup>25</sup>

### **III. THE CYBER SECURITY EFFORTS OF THE GOVERNMENT AND INDUSTRY SHOULD BE CONSOLIDATED**

The record demonstrates that more than 55 government-initiated private-public partnerships already exist to address cyber security issues.<sup>26</sup> The proliferation of these partnerships is due in large part to numerous agencies attempting to address cyber security in an uncoordinated manner.<sup>27</sup> In evaluating cyber security for the Obama Administration, the National Security Advisory Committee issued a report finding that the foundational step in making meaningful progress in the cyber security area is the consolidation of “Federal cybersecurity activities under a single, central organizing governance structure.”<sup>28</sup> In other words, “the federal government must speak with one voice” on cyber security.<sup>29</sup> Efforts currently underway in Congress to address cyber security regulatory responsibilities within the

---

<sup>23</sup> *Accord* NCTA Comments at 6.

<sup>24</sup> *See* CTIA Comments at 9, n.11; Sprint Comments at 7.

<sup>25</sup> AT&T Comments at 18; Qwest Comments at 12.

<sup>26</sup> *See* AT&T Comments at 11 (citing article by Melissa Hathaway, former Acting Senior Director for Cybersecurity, National Security Council).

<sup>27</sup> GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative* at 2 (Mar. 2010) available at <http://www.gao.gov/new.items/d10338.pdf>; *see* AT&T Comments at 12.

<sup>28</sup> *See* Letter from Edward A. Mueller, NSTAC Chair, to President Barack H. Obama at 1 (Mar. 12, 2009); *see also* National Security Telecommunications Advisory Committee Report, *NSTAC Response to Sixty-Day Cyber Study Group* at 5 (Mar. 12, 2009) (“*NSTAC Sixty-Day Report*”).

<sup>29</sup> Qwest Comments at 4.

Federal government further counsel against any Commission-administered program at this time. Thus, rather than establish yet another federal mandate regarding cyber security, the Commission should coordinate with and defer to existing federal agency efforts on this issue and take steps to promote the consolidation of cyber security initiatives.<sup>30</sup>

### CONCLUSION

For the foregoing reasons, the Commission should refrain from establishing a cyber security certification program. There is no evidence that such a program is necessary to address network security issues and marketplace incentives already are driving broadband providers to adopt stringent security protocols and react rapidly to cyber threats. Furthermore, the Commission's resources would be better spent consolidating and continuing to support the various, parallel federal efforts currently underway to address cyber security.

Respectfully submitted,

**T-MOBILE USA, INC.**

By: /s/ Kathleen O'Brien Ham  
Kathleen O'Brien Ham  
Harold Salters  
Shellie Blakeney  
T-Mobile USA, Inc.  
401 Ninth Street, NW Suite 550  
Washington, DC 20005  
(202) 654-5900

September 8, 2010

---

<sup>30</sup> *Accord* CTIA Comments at 9-10; Qwest Comments at 7; Verizon Comments at 8-12.