



May 23, 2016

**VIA ELECTRONIC FILING**

Ms. Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 Twelfth Street, SW  
Washington, DC 20554

**Re: Ex Parte Presentation, *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, GN Docket No. 14-177; IB Docket No. 15-256; RM-11664, WT Docket No. 10-112; IB Docket No. 97-95**

Dear Ms. Dortch,

The Federal Communications Commission ("Commission" or "FCC") has asked about security in the above-captioned proceedings to establish flexible service rules for mobile use of the millimeter wave ("mmW") bands to facilitate Fifth Generation ("5G") mobile services.<sup>1</sup> The FCC has long supported industry leadership and working groups like the Communications Security, Reliability and Interoperability Council ("CSRIC") to address evolving and highly technical issues affecting the entire global ecosystem. The FCC promotes partnerships, rather than regulation, on cybersecurity because, as Chairman Wheeler rightly notes, "[t]he pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking."<sup>2</sup> As detailed herein, CTIA urges the Commission to maintain an ongoing dialogue with the wireless industry on important and complex 5G security issues and encourage actions that can be taken in standards groups and by CSRIC.

Any move by the Commission to regulate nascent 5G security in this proceeding would depart from that history and undermine ongoing global collaboration. Given the complex technical issues involved, FCC regulation also would be nearly impossible to execute and could have serious unintended consequences. The Commission should instead continue to rely on industry actions that can be taken in standards groups and by CSRIC to bring together the wireless ecosystem to continue work on emerging 5G architecture. Such an approach will better ensure that the wireless industry has the flexibility needed to ensure against security

---

<sup>1</sup> *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services*, Notice of Proposed Rulemaking, 30 FCC Rcd 11878, ¶¶ 260-65 (2015) ("*NPRM*").

<sup>2</sup> Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute (June 12, 2014), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-327591A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf). Likewise, the Public Safety & Homeland Security Bureau ("PSHSB") plans to seek information about security in voluntary, confidential meetings, as contemplated by the forthcoming Policy Statement on Cyber Assurance Meetings.



threats while recognizing the different use cases and changing technologies that will be deployed in the mmW bands.

***The global wireless ecosystem is committed to 5G security.***

Complex 5G standards are in the early stages of development, with the final phase set to be completed in late 2019 or 2020.<sup>3</sup> As commenters in the record have noted, industry incentives align with the interests of users and the FCC. Indeed, “security has been a design component in third and fourth generations of mobile broadband technologies, and is increasingly required by its members’ customers throughout the ecosystem. Security is now a market imperative.”<sup>4</sup>

Moreover, industry is “actively engaged in a wide range of efforts to assure that network and device security is preserved to the maximum extent feasible.”<sup>5</sup> The global ecosystem is working on all aspects of 5G security, using multi-layered approaches, including original equipment manufacturers (“OEMs”), operating system (“OS”) providers, wireless carriers, and application designers. For instance, Nokia is conducting research on security for 5G mobile networks<sup>6</sup> and Ericsson has been working on 5G issues.<sup>7</sup> Wireless carriers also are beginning preliminary 5G testing in 2016. 5G is the future of global wireless service, and multiple groups are actively addressing security.

Technical complexities associated with 5G deployments have already been identified and analyzed in white papers issued by the FCC’s Technological Advisory Council (“TAC”), through its cybersecurity efforts, and the wireless industry is committed to addressing these concerns both before and after these nascent technologies develop. For example, the TAC’s efforts looked at applying security to Internet of Things (“IoT”) devices and noted several security challenges, but also concluded that “established and emerging private sector capabilities are beginning to emerge and mature” and “industry organizations ... are prioritizing security-related

---

<sup>3</sup> 5G Americas, Notice of *Ex Parte*, GN Docket No. 14-177, at 1 (filed Apr. 8, 2016) (“5G Americas *Ex Parte*”).

<sup>4</sup> *Id.* at 1-2; see also Reply Comments of Straight Path Communications Inc., GN Docket No. 14-177, at 24-25 (filed Feb. 26, 2016) (“Equipment vendors, network operators, application developers, and service providers will all have business interests to provide security and protection against theft and privacy intrusion in the products and services they provide.”).

<sup>5</sup> Comments of the Telecommunications Industry Association, GN Docket No. 14-177, at 36 (filed Jan. 27, 2016) (“TIA Comments”).

<sup>6</sup> Reply Comments of Nokia, GN Docket No. 14-177, at 8 (filed Feb. 26, 2016).

<sup>7</sup> Ericsson, Notice of *Ex Parte*, GN Docket No. 14-177 (filed Feb. 23, 2016) (discussing white paper, *5G Security: Scenarios and Solutions*).



technology and best practices.”<sup>8</sup> In addition, the TAC noted that “[t]here are numerous efforts underway to enhance” security “within multiple standards organizations.”<sup>9</sup> Similarly, the TAC Cybersecurity Working Group examined security challenges and opportunities related to emerging software defined network (“SDN”) technology and network function virtualization (“NFV”).<sup>10</sup> The TAC noted that both are “very young in terms of technological maturity” and that existing gaps “point to future work for the FCC and other organizations as SDN and NFV mature and operational standards and best practices are adopted.”<sup>11</sup> Standards bodies and industry are actively addressing the issues identified by the TAC and others, as expected. For example:

- Several working groups of 3GPP, a consensus-based global organization open to participation by stakeholders throughout the wireless ecosystem, are engaged on 5G security, including development of radio access technology and network standards.<sup>12</sup> Topics include network access and authentication for SDN/NFV, data integrity, subscriber privacy, identity protection, end-to-end data protection, attack mitigation, and credential management;
- ATIS is taking a leadership role to ensure 5G can deliver the promised convergence of services onto a common framework, with enhancements to efficiency and security.<sup>13</sup> ATIS is developing an overall industry cybersecurity framework focused on the needs of industry. Work began by documenting the baseline for the current cybersecurity landscape, including existing ATIS initiatives and National Institute of Standards and Technology (“NIST”)/U.S. government cybersecurity frameworks and guidelines, as well as analyzing the expected threat landscape over the next three years. The effort aims to create a representative set of threat vectors that can be used as a basis for prioritizing scenarios. Based on this analysis, the cybersecurity effort is developing practices for the transition towards SDN/NFV/cloud-based infrastructure and protecting security in the

---

<sup>8</sup> See *Technical Considerations White Paper*, Release Version 1.1 at 4 (Dec. 2015), <https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf>.

<sup>9</sup> *Id.* at 28.

<sup>10</sup> See *White Paper: Considerations for Securing SDN/NFV* (Jan. 2016), <https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20SDN-NFV%20-SWG-WP-Final.pdf> (“TAC SDN/NFV White Paper”).

<sup>11</sup> *Id.* at 65.

<sup>12</sup> See 3GPP, *Tentative 3GPP Timeline for 5G* (Mar. 17, 2015), [http://www.3gpp.org/news-events/3gpp-news/1674-timeline\\_5g](http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g) (identifying working group activities and key milestones).

<sup>13</sup> See ATIS, *5G Reimagined: A North American Perspective*, White Paper (Nov. 2015), [https://access.atis.org/apps/group\\_public/download.php/27373/ATIS-I-0000050.pdf](https://access.atis.org/apps/group_public/download.php/27373/ATIS-I-0000050.pdf).



context of complex supply chains. Further work will consider the role of security-by-design in areas such as IoT and network application program interfaces (“ APIs”);

- IEEE is working on issues related to new wireless applications likely to run on 5G, such as security for dedicated short-range communications used by autonomous vehicles;<sup>14</sup>
- NIST is working on several efforts related to 5G;<sup>15</sup> and
- The TAC presently is continuing to investigate cybersecurity issues related to IoT and 5G.<sup>16</sup>

The FCC should monitor these ongoing efforts and encourage domestic and global stakeholders to address security as 5G devices, applications, and uses develop.

***Regulation is not the right way to address 5G security.***

Cybersecurity is complex and moves at a very fast speed. As industry innovates to deal with emerging use cases and challenges in next-generation wireless systems, the Commission should not mandate solutions in these proceedings.<sup>17</sup>

*First*, prescriptive security regulations for 5G are premature given that there is much still unknown about 5G deployments and attendant security challenges. Among other things, as a recent TAC report observed, attack surfaces in new technologies are “not static,”<sup>18</sup> and need further analysis. As noted above, standards bodies are actively focused on 5G security as a priority, and CTIA’s Cybersecurity Working Group is defining security use cases for 5G. Collaborative efforts such as these should be encouraged rather than replaced by static regulations that could have unintended consequences.

Security-related regulations are doubly premature in light of the emerging use cases for 5G, the Internet of Things, and machine-to-machine, the development of which could be

---

<sup>14</sup> See John Kenney, Dedicated Short-Range Communications (DSRC) Standards in the United States, 99 Proceedings of the IEEE 7 (July 2011), [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5888501&url=http%3A%2F%2Fieeexplore.ieee.org%2Fexpls%2Fabs\\_all.jsp%3Farnumber%3D5888501](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5888501&url=http%3A%2F%2Fieeexplore.ieee.org%2Fexpls%2Fabs_all.jsp%3Farnumber%3D5888501).

<sup>15</sup> See, e.g., NIST Communications Technology Laboratory, <http://www.nist.gov/ctl/wireless-networks/5g-networks.cfm>. Other NIST efforts have looked at various aspects of mobile security.

<sup>16</sup> See TAC, Mar. 9, 2016 Meeting Presentation, at 5-7, <https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting3916/TAC-Presentations-3-9-16.pdf>.

<sup>17</sup> CTIA has previously urged the FCC to consider 5G security holistically. See Comments of CTIA, GN Docket No. 14-177, at 3, 34 (filed Jan. 28, 2016).

<sup>18</sup> See, e.g., TAC SDN/NFV White Paper at 47.



distorted by regulation. For example, requiring that security be built into mmW equipment, rather than other parts of the network, could influence or limit the types of services that could use the spectrum.<sup>19</sup> Mandating specifications could “at best, leave other elements of networks vulnerable and, at worst, could preclude better solutions when networks as a whole are evaluated.”<sup>20</sup> Pursuing security through federal regulation may also hinder international harmonization. Mandating a solution may risk U.S. leadership in wireless innovation by pushing innovators’ new advances to other parts of the globe that support a more nimble and flexible regulatory regime for 5G.

*Second*, regulation simply cannot keep pace with the technological complexity and change expected in 5G generally and with respect to security specifically. “Given the rapid evolution of technology, the adoption of standardized security or architectural methods could potentially freeze current technology in place and limit flexible network management.”<sup>21</sup> In today’s complex, global wireless environment, flexibility is key. Industry best practices and collaborative efforts help players and technology rapidly adjust to ever-changing threats. By contrast, standardized security provides a roadmap for hackers and criminals.<sup>22</sup> While cybersecurity is a poor candidate for regulation generally, it is doubly so here given that 5G has not matured enough to inform any federal security rules. This is why the TAC called for industry to “continue to, via the FCC, grow consensus and use cases which include both SDN and NFV” and address other security challenges in a framework that “maintains the flexibility and choice to allow organizations to deploy SDN and NFV as they please.”<sup>23</sup>

*Finally*, it is not clear what the FCC could propose in this highly complex and technical area that could improve on private efforts and avoid unintended consequences. The general approach in the *NPRM* confirms that issues are insufficiently developed. For example, the *NPRM* appears to conflate data and network security, and it cites a third party’s “CIA triad” concept of confidentiality, integrity, and availability.<sup>24</sup> While helpful, these concepts are not a general

---

<sup>19</sup> TIA Comments at 36.

<sup>20</sup> *Id.*

<sup>21</sup> Comments of Straight Path Communications Inc., GN Docket No. 14-177 at 39 (filed Jan. 27, 2016); *see also* TIA Comments at 36-37 (“The Commission’s pro-flexibility, technology-neutral policies suggest that the better approach is to allow the marketplace to work, freeing network operators to provide security through the mechanisms that best fit their business plans and technology choices.”).

<sup>22</sup> *See, e.g.*, CTIA, *Today’s Mobile Cybersecurity: Blueprint for the Future*, at 24 (rel. Feb. 12, 2013).

<sup>23</sup> *See* TAC SDN/NFV White Paper at 52, 66.

<sup>24</sup> *Spectrum Frontiers NPRM* ¶ 261.



consensus method for evaluating all cyber issues.<sup>25</sup> The *NPRM* does not propose anything like a workable regime for 5G security, and nothing in the record supports adopting a particular approach or wresting current and future security initiatives from the private sector.

As discussed in more detail below, CTIA urges the FCC to instead facilitate a collaborative, industry-based approach to 5G security through CSRIC.

***The Commission should look to CSRIC to promote collaboration on 5G security.***

The FCC has lauded multi-stakeholder efforts to create flexible approaches and is coordinating with other agencies on collaborative processes to address cybersecurity.<sup>26</sup> 5G security will be an ongoing, technically sophisticated effort, requiring active engagement from all aspects of the global mobile ecosystem. As a result, CSRIC is the best forum for the FCC to help address 5G security. CSRIC's purpose is to "provide recommendations to the FCC regarding ways the agency can strive for security, reliability, and interoperability of communications systems."<sup>27</sup> CSRIC working groups for years have tackled myriad highly complex and competitively sensitive issues that would be difficult to address through static demands in Title 47 of the Code of Federal Regulations.

CSRIC is flexible and promotes collaboration in a non-regulatory setting. These attributes are particularly important when dealing with technical issues at the heart of the next critical phase of wireless innovation and competition. CSRIC's structure enables the private sector to share information, work toward common interests, and provide guidance to the FCC. Importantly, CSRIC uses and informs domestic and international standards that will help shape the future of 5G, which has global implications, making balkanization a very real threat.

CSRIC's multistakeholder, non-regulatory approach has been successful, helping to address complex and diverse issues in 3G and 4G, including E911, location accuracy, VoLTE, and transitions between generations of wireless services. CSRIC has ably addressed myriad

---

<sup>25</sup> Indeed, this triad is referenced elsewhere as one of many possible security approaches, see, e.g., TAC SDN/NFV White Paper at 62.

<sup>26</sup> For example, Chairman Wheeler has praised CSRIC's work, noting that a recent report "contains a compelling set of recommendations for cyber risk management throughout all segments of the communications sector. It articulates a comprehensive approach, rooted in the NIST Framework, while also taking note of the unique challenges that face providers of various kinds." Remarks of FCC Chairman Tom Wheeler, RSA Conference (Apr. 21, 2015), [https://apps.fcc.gov/edocs\\_public/attachmatch/DOC-333127A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/DOC-333127A1.pdf).

<sup>27</sup> Charter of the FCC's Communications Security, Reliability, and Interoperability Council, <https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC%20Charter%20Renewal%202011%20FINAL.pdf>.



security issues, including developing best practices, codes of conduct, and mechanisms for the communications industry to improve its management of cyber risks and deploy the cybersecurity framework developed by NIST. CSRIC also has made technical recommendations for Internet security, including on domain name security, routing, and other approaches. Various CSRIC working groups continue to develop technical and operational recommendations on complicated aspects of security and have repeatedly observed that the pace of change in security is incredibly rapid.

CTIA urges the FCC to use this construct for 5G security issues, which will rapidly evolve over the next few years. By harnessing industry and global efforts, CSRIC can coordinate and promote U.S.-developed practices, tools, and methods for enhancing global 5G security. The best way to ensure that the United States continues to lead the world in wireless is by promoting innovation and collaboration, rather than top-down regulation. There is no reason for the FCC to depart from this effective model.

\* \* \* \* \*

The wireless industry has been and continues to be committed to ensuring the security of the mobile devices and services on which consumers rely every day, a commitment which extends to innovative next-generation wireless offerings contemplated in these proceedings. The nascence of 5G technologies, coupled with the ever-changing nature of security challenges, raises particular concerns if the Commission were to depart from the its longstanding support of global collaboration on cybersecurity. CTIA therefore urges the Commission to maintain an ongoing dialogue with the wireless industry on these important and complex issues and encourage actions that can be taken in standards groups and by CSRIC.

CTIA and the wireless ecosystem look forward to continued dialogue with the Commission on 5G security issues. Pursuant to Section 1.1206 of the Commission's rules, a copy



of this letter and attachment is being filed in ECFS. Please do not hesitate to contact the undersigned with any questions.

Sincerely,

/s/ Thomas K. Sawanobori

Thomas K. Sawanobori  
Chief Technology Officer  
CTIA

John A. Marinho  
Vice President, Technology & Cybersecurity  
CTIA