

June 17, 2016

**BY ELECTRONIC FILING**

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554

*Re: 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:

In its proceeding on flexible use of high-band spectrum, expected to include Fifth Generation (“5G”) mobile broadband, the Federal Communications Commission has asked for comments on the development of security for such services. During 5G Americas’ meeting with the Commission earlier this spring on this topic, we noted that the industry is in the best position to develop security solutions for 5G services and provided an overview of the efforts of some of these standards groups.<sup>1</sup> 5G Americas is the voice for 5G and LTE in our Region, fostering the deployment of these services throughout our hemisphere. Our members have a clear stake in ensuring the security of technology deployed for 5G services. Industry is therefore in the best position to address security of 5G services and applications through the combined expertise of standards development organizations focusing on these services and applications. In this letter, 5G Americas provides additional detail on the security-related working groups of one of these standards groups in particular: 3GPP, the Third Generation Partnership Project, for which 5G Americas is a Market Representation Partner (“MRP”). 5G Americas encourages the Commission to direct its security-related efforts to supporting these industry efforts.

---

<sup>1</sup> See Letter from Patricia Paoletta, Counsel to 5G Americas, to Marlene H. Dortch, Secretary, Federal Communications Commission, GN Docket No. 14-177, et al. (Apr. 8, 2016) (discussing 5G security).

**I. Standards group organizations like 3GPP are best-positioned to develop robust security recommendations and standards.**

As 5G Americas noted in its April meeting with the Commission, there are a number of standards development organizations focusing on security for 5G and the Internet of Things (“IoT”). Each group is uniquely positioned to address security challenges specific to the technology related to their particular sector. For instance, 5G Americas’ members are particularly active in 3GPP’s efforts on mobile wireless network and device security. Accordingly, we are able to provide more detail on some of 3GPP’s latest working groups focused on security as an example of current industry efforts.<sup>2</sup>

3GPP is an open forum that unites seven telecommunications standard development organizations and allows members to produce specifications and studies with broad industry consensus.<sup>3</sup> These specifications are contribution-driven, based on contributions by member companies to working groups and at the technical specification group level. One of the four technical specification groups in 3GPP is “Service & Systems Aspects” (“SA”). Within that Technical Group, two important working groups have formed to study issues relevant to next generation security. SA Working Group 2 (“SA2”) studies definition, evolution, and maintenance of the overall architecture, including the assignment of functions to particular subsystems.<sup>4</sup> SA Working Group 3 (“SA3”) is responsible for “security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols.”<sup>5</sup> SA3 performs analysis of potential threats to 3GPP systems, and based on that analysis, will “determine the security and privacy requirements for 3GPP systems, and specify the security architectures and protocols.”<sup>6</sup>

In its February 2016 meeting, 3GPP SA3 approved two study items for 3GPP Release 14 on security aspects of V2X communication (encompassing vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communication) and next generation systems: (1) Security Aspects for Long-Term Evolution (“LTE”) support of V2X services and (2) Security Aspects of the Next Generation Systems. For these two items, SA3 will issue a series of

---

<sup>2</sup> GSMA, another mobile industry association with some membership overlap, but with global as opposed to regional reach like 5G Americas, has recently held a conference dedicated to 5G and IoT security and privacy. *See, e.g.*, GSMA Mobile 360 Series – Privacy and Security, The Hague, Netherlands, May 10-11, 2016, available at <http://www.mobile360series.com/privacy-security/#conference>.

<sup>3</sup> *About 3GPP*, 3GPP, <http://www.3gpp.org/about-3gpp>.

<sup>4</sup> *SA2 – Architecture*, 3GPP, <http://www.3gpp.org/specifications-groups/sa-plenary/sa2-architecture>.

<sup>5</sup> *SA3 – Security*, 3GPP, <http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security>.

<sup>6</sup> *Id.*

technical reports for V2X and 5G usage, identifying security threats, defining security requirements, and proposing potential solutions. The key security work will focus on analyzing message authenticity mechanisms for broadcast messages, message authenticity, and confidentiality for closed-group communication, and protecting user identity and privacy while making sure that the proposed security solutions are practical and deployable.

In its May 2016 meeting, 3GPP SA3 began work on the two items, considering over 60 contributions related to architecture and security for next generation technology. The contributions spanned a wide range of topics including architecture, authentication, security context and key management, authorization, backwards compatibility, relays, network slicing, interconnect network security, radio access network (RAN) security, credential provisioning, privacy, security visibility and configurability, security within next-generation user equipment (NG-UE), and user plane security.

The two recently identified study items for SA3 provide insight into the level of detail with which working groups can address security challenges.

*Security Aspects for LTE support of V2X services.* This study item, which will be included in the 3GPP SA3 Technical Report (“TR”) 33.885, focuses on the use cases and potential requirements for LTE support for vehicular communications services (described in 3GPP SA1 TR 22.885) and potential architecture enhancement (described in 3GPP SA2 TR 23.785). This study item has focused on security threats analysis and requirements for V2X message broadcasting for the following three categories of use cases: (1) V2V/P broadcast messages initiated by an UE for public V2X service information dissemination; (2) V2V/P broadcast messages initiated by an authority UE for authorized V2X information announcement; and (3) V2V/P close-group multicast messages initiated by a UE, and consumed by UEs, which participate in a group-based application/service, which may restrict V2X messages from consumptions by public UE.

At its May 2016 meeting, SA3 reviewed several input contributions on security issues and proposed solutions from various companies. The group reviewed and approved a number of input contributions on V2X security requirements, including on authorization, credential provisioning, communication, and privacy for inclusion in TR 33.885.

The group proposed and discussed two security solutions (including authorization, credential provisioning, and communication security) for V2V/P: Layer-2 and application-based security approaches. SA3 noted that both solutions come with *pros* and *cons*. As a result, SA3 will further evaluate both of the proposed solutions in its upcoming meetings. One of the key open issues identified for further studies is the competing concerns of privacy and identity hiding.

*Security Aspects of the Next Generation Systems.* This study item focuses on security aspects of the next generation systems and evaluation of possible technical solutions for inclusion in the 3GPP SA3 TR 33.899. Key security issues under this study item include

improving the existing security of fourth generation network and new security design due to the fact that the next generation systems will include both 3GPP and non-3GPP access and extended usages encompassing massive IoT, critical communications, enhanced mobile broadband, and associated network operations.

With respect to security improvement under this item, SA3 agreed on the importance of strengthening security to prevent disclosure of Ki (shared secret key, provisioned at the time of manufacturing, that resides in the Universal Integrated Circuit Card (“UICC”)) to attackers via various weak links. Examples of concerns include hacking at the factory, hacking of the communication channel over which Ki is transported from SIM vendor or subscription manager to mobile operator, hacking into the mobile operators, and insider attacks at a mobile operator or SIM vendor.

With respect to security design under this item, SA3 agreed on the importance of defining a unified and adaptive authentication framework for both access and services. This “unified” authentication framework will support many needed aspects of security, including both 3GPP and non-3GPP access usages; adaptive security enabling operators to compose a “slice” security model; meeting business cases and needs; handling different credential types; cryptographic separation of credentials used for different access and services; alternate methods to hardware UICC for storing credentials/security algorithms/user identity; efficiency and minimal overhead of authentication signaling; use of device identity for authentication and device provisioning; and user privacy.

## **II. FCC and other agencies should focus efforts on support of standards groups.**

As we stated in the April 2016 meeting, the Commission should support efforts of groups like 3GPP and gather more information on their and the industry’s activities. 5G Americas is pleased that the FCC has already begun to information gather through its Technological Advisory Council (“TAC”). As the Commission knows, the TAC has published a number of White Papers on technical complexities related to 5G deployment and is outlining a list of key principles that should be built into the 5G ecosystem, including on security.<sup>7</sup> Based on these key security principles (including denial of service, key management, identity management, encryption, protecting the control plane, and isolation mechanisms), the TAC expects to develop an action plan to use them as a guiding measure in the standards development process.<sup>8</sup> CTIA also recommends the Commission’s private sector advisory council, the Communications

---

<sup>7</sup> See Letter from Thomas K. Sawanobori, Chief Technology Officer, CTIA – The Wireless Association, to Marlene H. Dortch, Secretary, Federal Communications Commission, GN Docket No. 14-177, et al. (May 23, 2016) (discussing TAC’s White Papers on IoT).

<sup>8</sup> See *Mobile Device Theft Prevention WG Report to the FCC TAC*, FCC Technology Advisory Council (June 9, 2016), <https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting6916/TAC-Presentations6-9-16.pdf>.

Security, Reliability and Interoperability Council, as an avenue to address evolving and highly technical security issues. 5G Americas supports that recommendation.

The Federal Trade Commission (“FTC”) has also held workshops and issued reports with recommendations for companies involved in IoT, which is one area of applications that will benefit from the transition to 5G. In one of its recent workshops, the FTC acknowledged that there is “no one-size-fits-all checklist to guarantee the security of connected devices.”<sup>9</sup> The FTC therefore built its recommendations on “input from industry, consumers, academics, and others.” This kind of approach—creating a forum for industry discussion—is a constructive way for the Commission to gather information on 5G security before developing any recommendations. As for the need for any prescriptive action, the FTC has made clear that it considers security practices to be part of its mandate.<sup>10</sup> Indeed, the FTC has said that its priorities for 2016 in the area of data privacy and security are big data, connected devices, and sensitive information.<sup>11</sup> Recently, the FTC has taken a number of enforcement actions to ensure that IoT products provide the security marketed by their vendor.<sup>12</sup>

As the United States moves towards 5G deployment, the Commission should be cautious of imposing security requirements for flexible use wireless services while the standards are under development. Such precipitous action could stifle innovation. 5G Americas agrees with the Commission that because technology is always evolving, industry must continue to evolve its security measures to effectively manage a dynamic threat environment. Accordingly, 5G Americas recommends that the Commission focus its efforts on supporting industry in its participation in the various standards groups that are currently working to develop security recommendations for broadband services in upper millimeter wave spectrum. Just as the Commission will allow flexible use of such spectrum, it should allow the mobile industry

---

<sup>9</sup> *Careful Connections: Building Security in the Internet of Things*, Federal Trade Commission, at 1 (Jan. 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf>.

<sup>10</sup> *Comments of Federal Trade Commission* at 1, Docket No. 160331306-6306-01, RIN 0660-XC024 (filed June 2, 2016) (citing 15 U.S.C. § 45(a)).

<sup>11</sup> *N.Y. AG’s Office Avoids Duplicating FTC’s Work on Data Privacy, Security*, T.R. DAILY (June 6, 2016) (discussing FTC’s enforcement actions for privacy and security, and statements from the New York State Attorney General’s Office that it would not duplicate efforts of FTC) (available by subscription).

<sup>12</sup> *See, e.g.*, Press Release, *Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers’ Privacy*, Federal Trade Commission (Sept. 4, 2013), [www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-homes](http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-homes). *See also* FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

Ms. Marlene H. Dortch  
Federal Communications Commission  
17 June 2016  
Page 6

flexibility in the means through which it meets the market and existing legal imperative for 5G and IoT security.

Should you have any questions, please contact me by telephone at +1 202 730 1314 or by e-mail at [tpaoletta@hwglaw.com](mailto:tpaoletta@hwglaw.com).

Respectfully submitted,



---

Patricia Paoletta  
*Counsel for 5G Americas*

cc: Jeffery Goldthorp  
Ahmed Lahjouji  
John Schauble  
Greg Intoccia  
Bahman Badipour