Federal Communications Commission
Washington, D.C. 20554

September 19, 2016

To : Dr. Anand Prasad, 3GPP SA 3 Chairman
Cc : Erik Guttman, 3GPP TSG SA Chairman,
Dino Flore, 3GPP TSG RAN Chairman
3GPP Mobile Competence Centre, c/o ETSI
650, Route des Lucioles 06921 Sophia-Antipolis Cedex
France

Dear Chairman Prasad:

The Federal Communications Commission (Commission) is determined to ensure that 5G systems and services in the U.S. marketplace have cybersecurity engineered into networks and devices. On July 14th of this year, the Federal Communications Commission (Commission) adopted a Report and Order and Further Notice of Proposed Rulemaking making spectrum bands above 24 GHz in the U.S. available for flexible use wireless services, including for next generation (i.e., 5G) networks and technologies[1].

In establishing the framework for these spectrum bands, the FCC rules promote security by design within the new networks and technologies that will utilize the spectrum without creating a significant regulatory burden. These rules require licensees to file a statement before deployment that includes, at a high level, certain security-related information, such as a description of participation in standards body security work, its intended approach to security, and the implications their security by design will have for other parts of the 5G ecosystem. It is our intent to ensure that other spectrum bands used for 5G not specifically cited in GN Docket No.14-177 effectively address cybersecurity in a transparent manner ensuring that all parts of the ecosystem plan to leverage their engineering efforts and contribute to an objective security architecture.

The Commission commends the 3rd Generation Partnership Program (3GPP) Services Systems Aspect Working Group 3 (SA-3) on Security on the work-in-progress Study on Architecture and Security for Next Generation Systems. The Commission appreciates the opportunity to monitor the discussions and developments of the Committee concerning technical and policy ideas. We strongly encourage the Committee's timely resolution of existing protocol exploits and its efforts to address issues during the protocol specification phase instead of the latter phases of implementation and deployment.

The Commission would also like to bring to the attention of SA Working Group 3 the current work-in-progress from Working Group 5 (Cybersecurity Information Sharing) of the Communications Security, Reliability, and Interoperability Council (CSRIC) and the Technical Advisory Council (TAC)

---

[1] In the matter of the Use of Spectrum Bands Above 24 GHz For Mobile Radio Services, GN Docket No.14-177, available at: http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0728/FCC-16-89A1.pdf

cybersecurity working group, which are councils set up under the U.S. Federal Advisory Committee Act (FACA). Working Group 5 of the CSRIC shall provide recommendations to the FCC concerning strategy, procedures, and steps necessary to help incorporate the concept of "security by design" into the fabric of 5G, its design specifications, and consequently 5G's complex multi-product line ecosystem. These recommendations are due to the FCC in December 2016 and shall be made available to general public.

Finally, the Commission intends to periodically document high level and on-going activity concerning cybersecurity for 5G. This activity includes efforts from stakeholders that may or may not be a part of the 3GPP standards development organization. The Commission believes that this will complement the on-going efforts of SA-3 and advance our mutual goals of promoting cost effective, advanced consumer functionality with security by design.

We look forward to the outcome of the next plenary, the ad-hoc meeting on NextGen, and future meetings of SA-3.

Sincerely,

David G. Simpson, Rear Admiral (Ret.), USN
Chief, Public Safety and Homeland Security Bureau