November 1, 2021

Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

<u>Re</u>: ET Docket No. 21-353 Spectrum Requirements for the Internet of Things

Dear Secretary Dortch:

NPSTC submits these comments in response to the Notice of Inquiry in the above-captioned proceeding regarding the Internet of Things (IoT)[1]

The National Public Safety Telecommunications Council (NPSTC) is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. Accordingly, NPSTC provides guidance on issues that can either negatively impact or benefit the operation of public safety communications.

---

[1] *Notice of Inquiry,* ET Docket No. 21-353 released September 30, 2021.

American Association of State Highway and Transportation Officials | American Radio Relay League | Association of Fish and Wildlife Agencies | Association of Public Safety Communications Officials | Forestry Conservation Communications Association | International Association of Chiefs of Police | International Association of Emergency Managers | International Association of Fire Chiefs | International Municipal Signal Association | National Association of State Chief Information Officers | National Association of State Emergency Medical Services Officials | National Association of State Foresters | National Association of State Technology Directors | National Council of Statewide Interoperability Coordinators | National Emergency Number Association | National Sheriffs' Association

9615 E County Line Rd, Ste. B-246 Centennial, CO 80112· Website www.NPSTC.org

The Commission issued the Notice of Inquiry (NOI) at the direction of Congress.[2] In

conformance with that direction, the NOI's focus is on spectrum for commercial and unlicensed

IoT. The questions required by Congress and posed in the NOI are as follows:

> (A) whether adequate spectrum is available, or is planned for allocation, for commercial wireless services that could support the growing IoT;
> (B) if adequate spectrum is not available for the purposes described in subparagraph (A), how to ensure that adequate spectrum is available for increased demand with respect to the IoT;
> (C) what regulatory barriers may exist to providing any needed spectrum that would support uses relating to the IoT; and
> (D) what the role of unlicensed and licensed spectrum is and will be in the growth of the IoT.[3]

While the focus of the NOI is primarily on spectrum for commercial and unlicensed uses,

the Commission has recognized in the NOI that IoT does have applications to benefit public

safety, critical infrastructure and industrial applications:

> IoT-networked devices are used to monitor power grids….The IoT can be used to link devices worn on a person's body, which can help improve patient monitoring and telehealth applications. IoT technologies are also developing to improve public safety and aid first responders, such as by providing faster field response, real-time data link with information critical to the safety and abilities of firefighters. The myriad use cases of IoT are helping to drive innovation in a wide variety of settings, including industrial, government, commercial, and residential. (footnotes deleted)[4]

As it develops its record that may lead to a subsequent Notice of Proposed Rulemaking for

IoT, NPSTC urges the Commission to expand its focus to include IoT spectrum for public safety

and other critical internal uses, not just IoT spectrum for licensed commercial wireless providers

and unlicensed consumer WiFi networks. While commercial wireless may be adequate for a few

---

[2] Notice of Inquiry (NOI) at paragraph 1.
[3] NOI at paragraph 5.
[4] NOI at paragraph 3.

of these IoT applications, public safety and other critical users are likely to require higher levels of reliability and security for many of its IoT use cases.

Currently, IoT is in its infancy. Additional knowledge about the spectrum and operational requirements should be gained as more IoT uses are field-tested in actual public safety and critical infrastructure operational environments. IoT for public safety can potentially incorporate video, data and voice elements, each of which will require different bandwidths for reliable and efficient operation. Also, the number of requisite devices for a given individual application or incident will vary. In addition, the proximity of multiple devices from one another, either for the same incident or for multiple nearby applications, will impact the number of "channels" required and the degree of channel re-use possible without interference. All these factors contribute to a determination of the aggregate amount of spectrum required.

Additional work is needed to characterize which public safety IoT uses require dedicated spectrum and which might be accommodated sufficiently on commercial wireless networks. Then, spectrum estimates will be needed for both categories. For dedicated public safety spectrum, NPSTC believes additional spectrum will need to be identified. **The Commission should <u>not</u> rely on trying to repurpose public safety spectrum that already supports mobile use, fixed links or broadband data, i.e., public safety communications that will continue to be required.**

Given the nascent nature of IoT at present, NPSTC believes one element of determining spectrum requirements is a better understanding of IoT use cases in various market segments. NPSTC, through its IoT Working Group, has studied some sample use cases of IoT for public safety, as well as potential implementation requirements and challenges. We believe the information developed in the resulting NPSTC reports on IoT could be helpful as the Commission

moves forward to provide greater focus on IoT, possibly including a Notice of Proposed Rulemaking.

Accordingly, as part of its comments to the NOI, NPSTC submits two reports related to IoT for public safety as attachments: 1) Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes, June 2019; and 2) Public Safety Internet of Things: Outreach Report to Public Safety, April 2020. The first report provides a snapshot of eight sample use cases in which IoT can be beneficial to public safety. Of course, these use cases are not static; as technology and deployments advance, public safety will find additional IoT uses that will be beneficial to and ultimately essential for law enforcement, firefighters, emergency medical personnel and overall emergency management.[5] The latter report is designed primarily to provide information and resources to help agencies navigate through the public safety IoT planning and evaluation process. As it assesses what actions it should take to help enable the development and deployment of IoT, NPSTC believes the information in both reports can be beneficial to the Commission.

The NPSTC IoT Working Group is also conducting further studies on topics including baseline requirements for public safety IoT device cybersecurity, public safety IoT governance best practices, requirements for integrating public safety IoT with Smart Cities and other IoT initiatives. Once those studies are completed and related reports are finalized and approved, NPSTC can consider entering those documents into the record of this proceeding as well.

---

[5] For example, the Department of Homeland Security (DHS) has an initiative to evaluate the use of sensors in connection with wildfires. See https://www.dhs.gov/science-and-technology/news/2021/09/14/feature-article-st-wildfire-sensor-initiative-heats-up

Respectfully submitted,

Ralph A. Haller, Chairman

National Public Safety Telecommunications Council

Attachments:

1) Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes, June 2019

2) Public Safety Internet of Things: Outreach Report to Public Safety, April 2020.