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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Implementation of Signaling System 7 Security Best Practices | ) | PS Docket No. 18-99 |
| | ) | |

## COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. ("T-Mobile")[1] is pleased to respond to the Public Notice in the above-referenced proceeding.[2] The Public Notice seeks input on the implementation and effectiveness of the March 2017 recommendations by the Communications Security, Reliability, and Interoperability Council ("CSRIC") regarding security risks related to Signaling System 7 ("SS7"). T-Mobile actively participated in CSRIC V's Working Group 10, which developed these recommendations, and has completed the implementation of the carrier-specific recommendations in its ongoing operations. In T-Mobile's view, that process has been a success. Any additional steps by the Commission to address SS7 security issues thus should be focused on further promoting voluntary use of these CSRIC recommendations throughout the ecosystem and supporting this model for private sector leadership.

[1] T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

[2] Public Notice, *Public Safety and Homeland Security Bureau Seeks Comment on Implementation of Signaling System 7 Security Best Practices*, DA 18-333, PS Docket No. 18-99 (Apr. 3, 2018) ("Public Notice").

## DISCUSSION

As a leading network owner and provider of nationwide wireless voice, text, and data services to over 72 million subscribers,[3] T-Mobile necessarily must prioritize cybersecurity in its operations and in its provision of services to customers. Accordingly, T-Mobile maintains a robust, aggressive, and forward-looking security program to protect all of its networks and its customers. It is worth noting that T-Mobile's legacy network, which relies on SS7 technology, only carries approximately 10 percent of T-Mobile's traffic and that the percentage of traffic continues to diminish.

In the course of these efforts, T-Mobile works closely with domestic and international peers across the global wireless ecosystem. The company actively participates in the cybersecurity efforts of various groups, including CTIA – The Wireless Association®, the Communications Sector Coordinating Council, the Communications Information Sharing and Analysis Center ("Comm ISAC"), and the United States Chamber of Commerce. As a member, T-Mobile supports the GSM Association's ("GSMA") cybersecurity work and participates in the 3rd Generation Partnership Project's ("3GPP") SA3 working group, which develops global security standards for wireless networks and is developing standards for 5G networks.

Moreover, T-Mobile actively shares threat and other security-related information with its peers in industry and partners in government, in a variety of settings. For example, T-Mobile participated in CTIA's Threat Indicator Pilot, which recently conducted a

[3] *T-Mobile Reports Record Financial Results Across the Board for FY 2017, Issues Strong Guidance for 2018 and Beyond*, Feb. 8, 2018, https://newsroom.t-mobile.com/news-and-blogs/tmus-q4-2017-earnings.htm.

table-top exercise of threat indicator information sharing to mitigate a simulated telephone denial-of-service attack. T-Mobile is active with the National Coordinating Center for Communications ("NCC") through the Comm ISAC, which promotes voluntary information sharing and collaboration on cybersecurity.

T-Mobile also regularly engages with government agencies and Congress on cybersecurity. T-Mobile serves on the executive committee of the Communications Sector Coordinating Council, supported by the Department of Homeland Security ("DHS"), to coordinate the cybersecurity efforts of the communications sector.[4] For years, T-Mobile has worked through the National Cybersecurity and Communications Integration Center ("NCCIC") and collaborated with other parts of DHS, including the Office of Science and Technology, on enhancing security. T-Mobile has consistently promoted a collaborative relationship with DHS, discussing details of SS7 architectures and vulnerabilities on multiple occasions in recent years. In addition, representatives of T-Mobile currently serve as the chair of CSRIC VI and as members of two CSRIC VI working groups – including Working Group 3 (Network Reliability and Security Risk Reduction), which is continuing the efforts begun by CSRIC V Working Group 10 as described in its final report.[5]

In that same spirit of collaboration, T-Mobile below responds to the three primary areas of inquiry set forth in the Public Notice.

---

[4] U.S. Communications Sector Coordinating Council, Leadership, https://www.comms-scc.org/leadership.

[5] *Legacy Systems Risk Reductions, Final Report*, CSRIC V Working Group 10 (Mar. 15, 2017), *available at* https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf ("Working Group 10 Report").

***Progress.*** T-Mobile has implemented the carrier-specific best practices recommended by Working Group 10. For example, per recommendation 5.2.1 (Signaling Security Monitoring and Filtering), T-Mobile has deployed a new SS7 special-purpose firewall, enabling T-Mobile to enhance its ability to monitor and filter SS7 traffic. T-Mobile conducts periodic testing and third-party assessments to assure the effectiveness of our cybersecurity systems and controls. Following conversations with Senator Wyden's office, T-Mobile updated its consumer education materials to include a link to CTIA information about encryption (per recommendation 5.2.9),[6] and as described above, it continues to engage actively with various government and industry stakeholders to share threat information, through the CTIA pilot and other means (per recommendation 5.2.4). In taking these steps, T-Mobile encountered no particular barriers or challenges. Indeed, T-Mobile has long taken issues related to SS7 security seriously and was thus well-positioned to act promptly and effectively on the recommendations.[7] In fact, in cases such as T-Mobile's implementation of SMS Home Routing several years ago to protect the privacy of its customers, T-Mobile's existing practices helped contribute to the best practices that CSRIC ultimately recommended.

***Evaluation.*** In T-Mobile's experience, the recommendations have been effective in mitigating potential SS7 vulnerabilities. Both before and after implementation,

---

[6] *See, e.g.*, T-Mobile, Privacy & Security Resources, https://www.t-mobile.com/company/privacy-resources/account-security/sim-security.html.

[7] Disclosure of T-Mobile's specific security practices, such as the protocols and tools it uses to monitor and filter SS7 traffic, would undermine their utility, to the detriment of its networks. *See, e.g.*, Letter to The Honorable Ron Wyden, U.S. Senate, from Anthony Russo, Vice President, Federal Legislative Affairs, T-Mobile US, Inc. (Oct. 13, 2017), https://www.wyden.senate.gov/imo/media/doc/10-13%20%20T%20Mobile%20Response.pdf.

T-Mobile detected no SS7 breaches – a quantitative indicator of success. T-Mobile believes that a key reason for this success is that Working Group 10's report properly contextualizes threats to SS7 technology. The recommendations allow T-Mobile and other wireless carriers to maintain a balance between security and avoiding collateral network impacts. Accordingly, T-Mobile does not believe it necessary at this time to explore alternative approaches.[8] The CSRIC recommendations comprise an effective level of security against SS7 vulnerabilities. To the extent individual customers seek additional security beyond that already afforded to them, they can readily use end-to-end encryption.

***Other Considerations.*** As discussed above, T-Mobile actively shares risk information – including on potential SS7 security risks – with industry and government stakeholders, through a variety of mechanisms and arrangements. Regarding the Public Notice's inquiry about practices with respect to the retention of SS7 network logs,[9] extended retention of the billions of daily SS7 records that are generated is neither technically feasible nor operationally valuable for network security purposes.

Finally, T-Mobile emphasizes one additional issue that the Public Notice does not mention, but that is critical in this and other communications security contexts: coordination among the agencies with active roles on security matters such as those pertaining to SS7. In particular, the Commission should consider using this inquiry to clarify the complementary roles and responsibilities of the Commission and DHS on issues involving SS7 security and related matters. As the Sector Specific Agency for the

[8] Public Notice at 2.

[9] *Id.*

Communications Sector, DHS has important responsibilities for and operational knowledge of the issues discussed in the Public Notice. DHS's ongoing role and activities need not compete with those of the Commission, which brings its own particular experience, expertise, and processes to bear on these matters – including CSRIC's model of meaningful private sector leadership in communications security and reliability. Instead, precisely because both DHS and the Commission have long been involved with industry in addressing the security challenges that arise in the context of SS7 technology and other arenas, this proceeding offers a logical opportunity for the agencies to discuss ways to promote coordination, avoid duplication of efforts, and advance the partnership between the Commission, DHS, and the carriers who developed and implement these recommendations. This partnership is necessary to develop dynamic and ever-improving voluntary solutions that harness business and operational imperatives to address sophisticated and ever-advancing security threats in a far more flexible and effective manner than is possible with more prescriptive approaches that lock in solutions that may become outdated.

## CONCLUSION

T-Mobile looks forward to continuing its effective collaboration with government and industry to address wireless network security in general and SS7 security issues in particular.

Respectfully submitted,

By: /s/ _____

Steve Sharkey
Cathleen Massey
Drew Morin
T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
Washington, DC 20004
(202) 654-5900

May 3, 2018