T-Mobile
601 Pennsylvania Ave NW
Suite 800N
Washington, DC 20004

October 13, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Re: Response to the Letter Dated September 14, 2017

Dear Senator Wyden:

Thank you for your letter dated September 14, 2017 ("the Letter") regarding the steps that T-Mobile US, Inc. ("T-Mobile") has taken to secure our network from cyberattacks and address security issues related to Signaling System No. 7 ("SS7").

THE SECURITY OF OUR NETWORK IS A PRIORITY

To meet consumers' increasing demands, T-Mobile invests aggressively in its network to expand coverage and deliver faster speeds. Consumers also need our network to be secure. While the company is securing the legacy network, which relies on SS7 technology, we are also securing our LTE network, which carries approximately 90% of our traffic and does not rely on SS7 technology. At the same time, we are developing the secure 5G network of tomorrow. To that end, T-Mobile works closely with domestic and international peers across the global wireless ecosystem, and with government partners.

For example, T-Mobile partners with AT&T, Sprint, and Verizon on the recently announced Mobile Authentication Task Force.[1] The Company actively participates in the cybersecurity efforts of various groups, including CTIA-The Wireless Association and the United States Chamber of Commerce. As a member, T-Mobile supports GSMA's cybersecurity work, and T-Mobile participates in 3GPP's SA3, which develops global security standards for wireless networks and is developing standards for 5G networks.

T-Mobile collaborates with the government on cybersecurity as well. For example, T-Mobile is on the executive committee of the Communication Sector Coordinating Council, created by the Department of Homeland Security ("DHS") to coordinate the cybersecurity efforts of the communications sector.[2] Additionally, T-Mobile is active with the Communications Information Sharing and Analysis Center, which promotes voluntary information sharing and collaboration on cybersecurity. As discussed below, T-Mobile has engaged with government agencies and Congress on cybersecurity, driving collaboration on SS7 with DHS.

[1] *See* http://www.tmonews.com/2017/09/t-mobile-partnering-three-major-u-s-carriers-form-mobile-authentication-taskforce/ .
[2] *See* https://www.comms-scc.org/leadership.

T-Mobile

T-MOBILE IS AWARE OF SS7 SECURITY ISSUES AND IS ADDRESSING THEM WITH BEST PRACTICES AND COLLABORATION

SS7 is a legacy technology that presents unique challenges to modern wireless networks. SS7 technology was developed four decades ago, when the number of communication service providers was small and the trust framework was inherently simple. As a result, a comprehensive threat model was never one of the design parameters for SS7.[3] Today, the wireless ecosystem and the threat landscape have changed dramatically, resulting in challenges that could not have been contemplated when SS7 was designed. For example, the explosive growth of mobility and global roaming expanded the number of service providers from less than a dozen to nearly 800 global carriers today. This has expanded both the community of trust and the attack surface.

The wireless industry, including T-Mobile, recognizes SS7 risks and has implemented countermeasures to mitigate or eliminate them.[4] T-Mobile uses network security protocols to address SS7 vulnerabilities, monitoring and filtering traffic and using sophisticated tools to protect users. Publicly discussing these protocols or tools in detail would undermine their utility.

T-Mobile also has been engaged with government agencies and Congress on SS7. For years, T-Mobile has worked through the National Cybersecurity and Communications Integration Center 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 on multiple occasions over the past year.

A prime example of collaboration on SS7 is the Communications Security, Reliability and Interoperability Council V ("CSRIC") at the Federal Communications Commission, whose Working Group 10 addressed legacy SS7 vulnerabilities. T-Mobile actively participated in Working Group 10, which included experts from across the communications ecosystem as well as officials from the FCC, DHS and the National Institute of Standards and Technology ("NIST"). The Working Group released a final report, *Legacy Systems and Services Risk Reduction* (the "CSRIC SS7 Report"),[5] on March 15, 2017.

As shown in the CSRIC SS7 Report, industry's approach to SS7 reflects risk management in action. The CSRIC SS7 Report properly contextualizes threats to SS7 technology. The risks are complex and technical responses must take care to avoid collateral network impacts because "the overwhelming amount of SS7 traffic is legitimate."[6] The CSRIC SS7 Report rightly notes that newer networks and technologies, such as 5G and Diameter, will not face the same risks.[7] Innovation enables us to design security in new ways that will increase security while reducing

[3] *SS7 Vulneratbility isn't a Flaw – it Was Designed That Way*, Larry Loeb, April 26, 2016, *available at* https://securityintelligence.com/ss7-vulnerability-isnt-a-flaw-it-was-designed-that-way/
[4] *Id.* at 11; Diana Goovaerts, *CTIA Reassurance, Call for Investigation Follow Report Detailing SS7 Hack*, Wireless Week (Apr. 18, 2016 4:11 PM).
[5] *Legacy Systems Risk Reductions, Final Report*, CSRIC V Working Group 10, at 6 (March 15, 2017), *available at* https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf ("*CSRIC SS7 Report*").
[6] *Id.* at 3 (emphasis added).
[7] *Id.* at 12.

the significance of SS7. This investment in the future of 5G is vital to enhance security and maintain U.S. leadership in the global wireless marketplace.

The CSRIC SS7 Report identified mitigations for SS7 risks, which the FCC's Public Safety and Homeland Security Bureau endorsed.[8] Recommendations include:

- Continue to implement signaling interconnection monitoring and filtering.
- Use GSMA security best practices and guidelines to secure signaling interconnection.
- Utilize signaling aggregators to address security, monitoring and filtering.
- Leverage and expand existing threat information sharing resources.
- Continue efforts regarding automated threat information sharing in the pilot administered by CTIA.
- Participate in industry and standards forums and adopt GSMA controls to address emerging risks in the overall approach to 5G security.
- Explore further work as it relates to circles of trust.
- Work on security assessment of network signaling infrastructure to detect and mitigate possible threat vectors.
- Encourage use of encryption technologies, particularly for VIPs.[9]

T-Mobile has implemented these recommendations and is committed to securing its network from SS7 exploits. For example, T-Mobile participated in CTIA's Threat Indicator Pilot, which recently conducted a table top exercise of threat indicator information sharing to mitigate a simulated telephone denial-of-service attack. Such collaboration will address SS7 and other security challenges that may arise.

RESPONSES TO YOUR SPECIFIC QUESTIONS

1. ***Has your company retained outside security experts to conduct SS7-focused penetration tests of your network? If so, have your staff addressed all of the security issues identified by the penetration testing team(s)? If any identified issues have yet to be resolved, why have these not been resolved?***

T-Mobile retained outside security experts to conduct SS7-focused penetration testing of our network. Based on the results, we have implemented improvements to address the security issues identified.

2. ***DHS has stated that the agency does not currently have the authority to conduct external SS7 penetration tests of U.S. wireless networks and that U.S. carriers have declined to share copies of the reports produced by the third party penetration testing firms they have retained.***

[8] *See FCC's Public Safety and Homeland Security Bureau Encourages Implementation of CSRIC Signaling System 7 Security Best Practices*, Public Notice, DA-17-799 (Aug. 24, 2017).
[9] *CSRIC SS7 Report*, Section 5.

T · ·Mobile·

a. Has your company refused DHS permission to test your network's security against SS7-related attacks? If so, why?

DHS has not asked T-Mobile for permission to perform penetration testing on the company's network. If a formal request to test our network were to be made by DHS, T-Mobile would carefully consider the increased security risk of any such request.

The results of penetration testing are highly sensitive. Penetration testing is done by companies on a regular basis to identify potential vulnerabilities in a network or system for risk evaluation. If results are disclosed, it increases the risk of exposing potential vulnerabilities and of T-Mobile's network being compromised. Nor is it clear how government penetration testing would benefit T-Mobile customers, as T-Mobile's staff is the best equipped to manage appropriate penetration testing of our live network without causing collateral harm.

b. Has your company refused a request by DHS for copies of SS7 penetration test reports? If so, why?

T-Mobile has not received a request from DHS for copies of SS7 penetration test reports.

c. Do you believe that it would be unreasonable for GSA to require, as a condition of selling wireless service to the U.S. government, that wireless carriers permit DHS to conduct external penetration tests of their networks or that they share copies of third party penetration test reports with DHS? If so, why?

We believe such a requirement would be unreasonable. First, the greater the number of parties with access to highly sensitive network security data, the greater the risk that this data could be compromised, with no additional benefit to the security of our customers as already noted in response to Question 2(a.) above. Second, it does not make sense for government to rely on SS7 security as a factor in purchasing, as SS7 currently plays a relatively minor role in modern (mostly LTE) networks and will play a diminishing role in the future. As industry has explained to DHS and others, there are many ways to address particular government mobile security needs, including those of senior officials. Agencies should use mobile device management, appropriate data and device encryption, and better cyber hygiene. Industry is discussing such steps with DHS and GSA.

3. Has your company implemented "SMS Home Routing"? If not, do you have any plans to do so, and if so, by when?

T-Mobile has implemented "SMS Home Routing."

4. Does your company currently have a "SS7 firewall" in place which is configured to inspect and filter all incoming SS7 messages to stop known SS7-exploitation techniques?

T-Mobile uses layered protective measures and network tools—including firewalls, robust inspection, and filtering—to address SS7-exploitation techniques. T-Mobile has deployed an SS7

specific firewall in our network that is currently going through integration testing prior to production launch this Quarter.

5. ***Does your company currently have a "Diameter firewall" in place, which is configured to inspect and filter all incoming Diameter messages to stop known Diameter-exploitation techniques?***

T-Mobile uses layered protective measures and network tools—including firewalls, robust inspection, and filtering—to address Diameter-exploitation techniques. The currently deployed SS7 firewall is designed to support Diameter specific messages as well. This feature will be production enabled in 2018.

6. ***Has your company implemented all of the SS7 security best practices as recommended in "SS7 Interconnect Security Monitoring and Firewall Guidelines" (FS.11), a document created by the GSM Association (GSMA) and distributed to its members? If not, what recommendations in this document have you not yet implemented, and by when do you expect to have implemented them?***

T-Mobile has implemented many of the SS7 security best practices as recommended in "SS7 Interconnect Security Monitoring Guidelines" (FS.11). The remaining monitoring guidelines will be implemented with the production launch of the SS7 specific firewall noted in response to Question 4 above.

****

T-Mobile aggressively protects against and responds to threats from nation-states, criminals and others to seek to exploit global communications networks. We use risk management tools like the NIST *Framework for Improving Critical Infrastructure Cybersecurity* as well as sophisticated technological solutions. We are building innovative security into next generation networks, products and services. The government and private sector must work in a spirit of trust to meet current and future security challenges. T-Mobile looks forward to continuing its effective collaboration with government to address wireless network security.

Sincerely,

Tony Russo

Anthony Russo
Vice President, Federal Legislative Affairs
T-Mobile US, Inc.