Vonya B. McCann
Senior Vice President
Government Affairs

Sprint Corporation
900 7th Street NW, Suite 700
Washington, DC 20001
Vonya.B.McCann@sprint.com

Sprint
works for me

October 13, 2017

The Honorable Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your September 14, 2017 letter to Marcelo Claure, President and Chief Executive Officer of Sprint Corporation ("Sprint"), inquiring about the steps Sprint has taken to secure its network from cyberattacks stemming from potential Signaling System No. 7 ("SS7") vulnerabilities.

SS7 security is a critical element of Sprint's overall network security program. Utilizing a "defense in depth" approach, Sprint has implemented multiple layers of security to protect its network, including its SS7 network, from malicious activity. Sprint's SS7 security framework is multi-faceted, taking advantage of CDMA technology, which manages SS7 signals differently than other technologies, and Sprint's unique network architecture and network security practices. Where Sprint identifies vulnerabilities, including those linked to SS7, it mitigates potential risks as feasible.

Sprint continues to review and enhance its SS7 security to keep pace with the evolving threat landscape. Sprint also continues to partner and collaborate with industry and the Department of Homeland Security to identify, assess, and address any new SS7 security vulnerabilities that may arise.

Sprint is pleased to answer your questions below.

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?**

   Yes, Sprint engaged a third party security firm to conduct SS7-focused penetration tests of its network, and Sprint has addressed the security issues that the firm 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.**

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

      DHS did not request permission to test Sprint's network's security against SS7-related attacks.

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

      DHS did not request copies of Sprint's 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?**

      In order to conduct valid external penetration testing, DHS must have highly specialized knowledge of each carrier's unique network architecture. Without this expertise, there is a high risk that DHS could inadvertently harm wireless carrier networks, garner inaccurate or incomplete test results, or interpret the results incorrectly. Accordingly, Sprint does not believe DHS should conduct such tests. Sprint, however, would consider allowing a third party expert to conduct such tests under appropriate circumstances.

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

   Yes, Sprint 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?**

   Sprint's current implementation of its CDMA SS7 design has similar functionality as an "SS7 firewall." Sprint screens all incoming SS7 messages from roaming partners and only permits messages essential to allow roaming functionality.

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?**

   Yes, Sprint uses Diameter edge devices to prevent unauthorized access to its network.

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?**

   Yes, where technically feasible, Sprint has implemented the SS7 best practices outlined in GSMA's FS.11 for relevant GSM traffic. Because Sprint is a CDMA carrier, not all GSMA SS7 best practices are applicable to Sprint. Sprint will continue to evaluate and adopt relevant industry best practices, as well as assess and deploy new security tools and enhancements as part of its ongoing security program review.

*****

Thank you for the opportunity to address your questions.

Sincerely,

Vonya B. McCann
Senior Vice President, Government Affairs