RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate

WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

September 14, 2017

Mr. Randall L. Stephenson
President and Chief Executive Officer
AT&T Inc.
208 S. Akard St.
Dallas, TX 75202

Dear Mr. Stephenson:

I write to you today to gain a better understanding of the steps your company has taken to secure your network from cyberattacks by hackers and foreign governments.

The Department of Homeland Security (DHS) concluded in a report published this summer "that all U.S. carriers are vulnerable to [Signaling System No. 7 (SS7)] exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions." As the DHS report notes, SS7 vulnerabilities can be exploited to "determine the physical location of cellular mobile devices, disrupt phone service from individual phones to entire networks, intercept or block SMS text messages, and redirect or eavesdrop on voice conversations." Moreover, in a June letter to Rep. Ted Lieu and myself, DHS also suggested that exploitation of SS7 vulnerabilities can threaten the reliability of the 911 emergency system.

According to the DHS report, these "vulnerabilities can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations."

The wireless industry has known that SS7 is vulnerable for nearly twenty years, security researchers have been publicly warning about SS7 vulnerabilities for more than a decade, and there are now a number of companies, located in countries around the world, who openly sell turn-key SS7 spying products. As such, the continued existence of these vulnerabilities and the ease with which they can be exploited by hackers and foreign governments poses a serious threat to U.S. national and economic security.

I understand that some wireless carriers are further along in the process of implementing protections against SS7 attacks than others. However, information about the progress that each carrier has made, and the extent to which their customers remain vulnerable to SS7 spying is not currently available to the general public, nor even to DHS. This means that the U.S. government and American consumers cannot currently vote with their wallets.

If wireless carriers were more transparent about the severity of SS7 vulnerabilities and their progress in defending against such attacks, the market could reward those companies who have

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

the most secure networks. Just as carriers openly compete on the speed and reach of their networks, they should also be competing on cybersecurity.

To that end, I would appreciate prompt, complete answers to each of the following questions by October 13, 2017. Please also provide my staff with copies of any written reports and threat assessments that your company has received from security firms that you have retained to conduct SS7 penetration tests against your network.

1. Has your company has 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?
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?
    b. Has your company refused a request by DHS for copies of SS7 penetration test reports? If so, why?
    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?
3. Has your company implemented "SMS Home Routing"? If not, do you have any plans to do so, and if so, by when?
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?
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?
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?

If you have any questions about this this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,

Ron Wyden
United States Senator