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

May 29, 2018

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street Southwest
Washington, DC 20554

Dear Chairman Pai:

One year ago I urged you to address serious cybersecurity vulnerabilities in U.S. telephone networks. To date, your Federal Communications Commission has done nothing but sit on its hands, leaving every American with a mobile phone at risk.

Mobile telephone networks connect to each other through Signaling System 7 (SS7), which is riddled with long-standing cybersecurity vulnerabilities that pose a major national security threat. SS7's flaws expose U.S. telephone networks to hacking by criminals and foreign governments. Hackers can exploit SS7 flaws to track Americans, intercept their calls and texts, and hack their phones to steal financial information, know when they are at home or away, and otherwise prey on unsuspecting consumers. Moreover, according to multiple news reports, SS7 spying products are widely available to both criminals and foreign governments.

Over the past year, my office has consulted with mobile security experts, the major wireless carriers, and the Department of Homeland Security (DHS) to discuss these vulnerabilities. These meetings have made clear that SS7 vulnerabilities pose a major threat that must be addressed immediately, a conclusion the DHS 2017 *Study on Mobile Device Security* shares.

This threat is not merely hypothetical—malicious attackers are already exploiting SS7 vulnerabilities. One of the major wireless carriers informed my office that it reported an SS7 breach, in which customer data was accessed, to law enforcement through the government's Customer Proprietary Network Information (CPNI) Reporting Portal. This is a legal requirement for wireless providers who believe that private consumer information has been illegally accessed. Submissions via the portal are automatically delivered to the FCC, the U.S. Secret Service, and the Federal Bureau of Investigation.

Although the security failures of SS7 have long been known to the FCC, the agency has failed to address this ongoing threat to national security and to the 95% of Americans who have wireless service. In 2016, the FCC created a new working group under the Communications Security, Reliability and Interoperability Council (CSRIC) to explore and address SS7 vulnerabilities. However, the working group was dominated by wireless industry insiders with serious conflicts of interest. CSRIC appointed a senior official from the wireless industry's trade association,

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

CTIA, to be lead editor of the group's report. Of the fifteen non-government members, twelve worked for telecommunications companies or industry associations. No academic experts or representatives from civil society were members of the working group. Likewise, although personnel from DHS's National Coordinating Center for Communications (NCC) participated, DHS has informed my office that the vast majority of the edits to the final report suggested by NCC's subject matter experts were rejected. DHS also informed my office that those same subject matter experts from the NCC were not invited back to participate in the subsequent CSRIC SS7 working group, created in late 2017.

The FCC deferred to the wireless industry to assess the same security vulnerabilities that the industry has long ignored. CSRIC's final report, published in March 2017 openly acknowledged that "the attack surface for a bad actor to potentially exploit... [SS7] has increased" and "there is reported evidence of attacks being launched against U.S. carriers." While some of the working group's technical recommendations were constructive, it let the wireless industry off the hook for ignoring these issues for decades and did not recommend that the FCC use its regulatory authority to force the industry to fix these and other long-standing security flaws. That the working group appointed by the FCC to study this issue did not recommend a more forceful response is, I believe, not a coincidence.

In a prior letter to me, you dismissed my request for the FCC to use its regulatory authority to force the wireless industry to address the SS7 vulnerabilities. You cited the work of the CSRIC as evidence that the FCC is addressing the threat. But neither CSRIC nor the FCC have taken meaningful action to protect hundreds of millions of Americans from potential surveillance by hackers and foreign governments. The FCC must now take swift action, using its regulatory authority over the wireless carriers, to address the market failure that has enabled the industry to ignore this and other serious cybersecurity issues for decades. I also ask that you provide me with answers to the following questions by July 9, 2018:

- The DHS's 2017 report *Study on Mobile Device Security* stated "all U.S. carriers are vulnerable… resulting in risk to national security." In response to one of my letters, then-Director of the NSA Admiral Michael Rogers agreed with me that "the security of mobile networks needs to improve and securing the vulnerabilities of SS7 must be part of that work." Do you agree with DHS and NSA that SS7 vulnerabilities pose a significant national security threat?
    - If you do not, please explain why your assessment differs.
- The CSRIC-V working group 10 was charged with the creation of a Risk Assessment Report, as noted in each of their presentations. The working group's publicly available final report only summarizes the findings of the Risk Assessment Report. Please provide me with a copy of the full Risk Assessment Report.
- In each of the past five calendar years, how many breaches have been reported to the FCC through the CPNI breach portal?
    - How many of these were breaches in which SS7 was used to access subscriber information?
- In each of the past five calendar years, how many breaches of customer location data have been reported to the FCC by wireless carriers.

    - How many of these were breaches in which SS7 was used to access subscriber information?
- For each SS7-related breach, please describe what steps, if any, the FCC took to investigate the breach.
- For each SS7-related breach, did the FCC notify the individuals whose information was stolen?
    - If not, please explain why the FCC did not notify these individuals.

If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

November 13, 2018

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Wyden:

I write in response to your letter regarding the importance of protecting our communications networks. I agree with you that our nation's networks must be robust and resilient. As you know, the Department of Homeland Security's Office of Cybersecurity and Communications is the designated agency responsible for overseeing cybersecurity preparedness of the communications sector. The Commission plays a supporting role, as a partner with DHS, in identifying vulnerabilities and working with stakeholders to increase security and resiliency in communications network infrastructure.

The Commission's efforts in this area primarily operate through the Communications Security, Reliability, and Interoperability Council (CSRIC). Last year, CSRIC V recommended best practices to prevent exploitation of Signaling System 7 (SS7). The Commission encouraged carriers to adopt those best practices in August 2017. Earlier this year, we sought comment from the public, industry, and other stakeholders on the implementation of those best practices, and our staff are reviewing the responses. We hope this additional information will help inform the Commission on their use and effectiveness. You also request in your letter a copy of the CSRIC V Working Group 10 Risk Assessment Report. We welcome you or your staff to come to the Commission to review that report *in camera*.

Further, CSRIC VI released its Final Report on recommendations to mitigate security risks on the Diameter protocol in March, and continues its work on assessing the risks and recommending best practices for 5G, including those risks associated with the Internet of Things devices. I appreciate the hard work of CSRIC, which includes the participation of DHS officials.

Regarding Customer Proprietary Network Information (CPNI) breaches, including SS7-specific breaches, I should note that carriers do not report this information to the FCC. Instead, as required by federal law and in line with the Commission's supporting role when it comes to cybersecurity matters, they report that information to the law enforcement agencies that may take action on it through the CPNI Breach Reporting Facility, managed by the U.S. Secret Service. For more than a decade, the Commission's rules have required electronic notification of CPNI breaches to the U.S. Secret Service and the Federal Bureau of Investigation so those entities can conduct criminal investigations as appropriate. The Commission has only indirect access to the CPNI Breach Reporting Facility and only for the purpose of ensuring compliance with our CPNI rules. If you would like additional data, you may wish to contact those agencies that oversee the

CPNI Breach Reporting Facility. Additionally, the Commission's rules require that carriers, rather than the Commission, notify individuals of any breaches that involve their CPNI.

I appreciate your interest in this matter. Please let me know if I can be of any further assistance.

Sincerely,

Ajit V. Pai