Congress of the United States
Washington, DC 20515

265

March 28, 2017

The Honorable Ajit Pai
Chairman
Federal Communications Commission
455 12th Street, S.W.
Washington, DC 20554

Dear Chairman Pai,

We are deeply concerned about the poor state of America's telecommunications cybersecurity. Our communications networks are far too vulnerable; the FCC has not, to date, prioritized cybersecurity; and the American people have largely been kept in the dark about the fact that their calls, texts, and movements are vulnerable to spying by foreign governments and hackers. This must change.

Cybersecurity researchers have issued repeated warnings about critical flaws in our communications infrastructure, including those in Signaling System 7 (SS7). However, cybersecurity has not traditionally been a regulatory priority for the FCC. Left, for the most part, to police itself, the cellular industry has neither adequately addressed these serious cybersecurity vulnerabilities nor warned its customers about the risks they face. Consequently, foreign governments and criminals can reach into U.S. cellular networks to track, surveil, and hack the phones of Americans.

The continued existence of these vulnerabilities—and the industry's lax approach to cybersecurity—does not just impact the liberty of Americans, it also poses a serious threat to our national and economic security. As such, the FCC must take swift action to address fundamental security threats to our mobile phones, which are no less dangerous than those cybersecurity threats that receive far more attention from other government agencies.

Last year, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) was tasked with looking into the SS7 cybersecurity issues that have been the subject of several media reports. On March 15, 2017, the CSRIC V working group 10 released a final report that includes a number of details that highlight the seriousness of this problem. In particular, the report:

- Recognizes that wireline and 5G networks may be as vulnerable as cellular networks.
- Notes that "complicit or compromised operators means that all telecommunications protocols used to interconnect networks are potentially at risk."

- Identifies U.S. critical infrastructure that is vulnerable to cyber attacks.
- States that signaling aggregators will provide a wider view of signaling traffic and will reduce risk.
- Recommends a layered approach to security that includes "methods to protect the content of messages and voice communications by using end to end encryption."
- Recommends improved firewalls to stop SS7 attacks.
- Notes that only a "handful of interconnection security experts in the world" focus on this issue.

Tasking the CSRIC with looking into this matter was a good first step, and the FCC should promptly implement the working group's recommendations. However, CSRIC V's charter ended on March 18, 2017, and, as the report notes, there are a number of related security issues that the group did not examine, as they were beyond the scope of the working group's mandate. We urge you to establish a new CSRIC working group and to expand its scope to examine the remaining issues that were not previously explored by the CSRIC V working group 10.

It is clear that industry self-regulation isn't working when it comes to telecommunications cybersecurity. We urge you to take swift action in this area in three ways. First, by forcing the cellular industry to address these serious cybersecurity vulnerabilities. Second, by warning the American public that their movements, communications, and devices may be vulnerable to foreign governments and hackers. And third, by promoting the use of end-to-end encryption apps, which, as the CSRIC working group stated, can be used to mitigate some of the SS7 risks.

Sincerely,

Ron Wyden
United States Senator

Ted W. Lieu
Member of Congress