RON WYDEN
OREGON

CHAIRMAN 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 THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

April 12, 2023

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, D.C. 20528-0075

The Honorable Paul M. Nakasone
Director
National Security Agency
9800 Savage Rd., Suite 6272
Fort Meade, MD 20755-6000

Dear Directors Easterly and Nakasone:

I write to request that the Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA) conduct or commission annual cybersecurity audits of FirstNet, the phone network for first responders and the military, operated by AT&T under contract with the U.S. government.

As you know, cybersecurity experts have long warned that phone networks are vulnerable to surveillance by hackers and foreign spies exploiting flaws in technologies used by telephone companies to exchange information with each other, known as SS7 and Diameter. As FCC Chairwoman Jessica Rosenworcel acknowledged in written answers she provided to Congress after a hearing on December 5, 2019, “criminals and foreign governments can exploit flaws in SS7 to track mobile users, intercept calls and texts, and even steal sensitive information available on devices.” Moreover, as the Department of Homeland Security described in an April 2017 report to Congress, "all U.S. carriers are vulnerable to these exploits, resulting in risks to national security, the economy, and the Federal Government’s ability to reliably execute national essential functions."

These phone network vulnerabilities are being actively exploited to conduct cross-border surveillance, according to cybersecurity researchers and several investigative reports by the press. As I revealed in a letter to the Federal Communications Commission (FCC) on March 28, 2018, one carrier told my staff that it has reported to the U.S government data breaches in which SS7-vulnerabilities were exploited to track people in the United States. Furthermore, as the press has documented, several surveillance technology companies sell point-and-click products that leverage these vulnerabilities to allow their customers to target phones anywhere in the world.

To date, the U.S. government has done little to force wireless carriers to fix these vulnerabilities, leaving Americans vulnerable to surveillance by hackers and foreign intelligence services. The FCC under the Trump Administration allowed the industry to invest as little as it wanted in cybersecurity. During the Trump Administration, then-FCC Commissioner Rosenworcel called for the Commission to “move beyond studies and voluntary recommendations.” Now under her

leadership, I hope that the FCC will address this market failure and protect Americans' privacy. The FCC should issue new regulations forcing the carriers to meet minimum cybersecurity standards, just as regulators in other countries have done.

These security flaws are also a national security issue, particularly if foreign governments can exploit these flaws to target U.S. government personnel. I am particularly concerned about FirstNet, the phone network for first responders and the military, which is operated by AT&T under contract with the U.S. government. In a briefing on February 11, 2022, focused on this issue, CISA's subject matter expert told my staff that they had no confidence in the security of FirstNet, in large part because they have not seen the results of any cybersecurity audits conducted against this government-only network.

My staff looked into the concerns raised by CISA and have spoken to officials at AT&T, the FirstNet Authority and the Department of Commerce's National Telecommunications and Information Administration (NTIA). These officials stated that while AT&T has obtained independent audits of FirstNet, AT&T is unwilling, and the Department of Commerce is unable to share the results with CISA, NSA, other government agencies, or Congress. According to NTIA, the Department of Commerce is bound by a non-disclosure provision in the contract it negotiated with AT&T. As a result, NTIA told my staff, NTIA and the FirstNet Authority are not allowed to reveal how frequently AT&T commissions these audits, how robust they are, what the audit results were, or whether all vulnerabilities discovered during the audits have been fixed.

Concealing vital cybersecurity reporting is simply unacceptable. As the lead agencies responsible for the government's cybersecurity, CISA and NSA need to have access to all relevant information regarding the cybersecurity of FirstNet, and Congress needs this information to conduct oversight. If the Department of Commerce is unable to share the results of the FirstNet audits commissioned by AT&T, CISA and NSA should conduct or commission their own annual audits and deliver the results to Congress and the FCC. If you lack the resources or authority to conduct such audits, please indicate as much, so that Congress can take the necessary steps to address this gap. I also request that CISA provide me with a copy of a report titled "U.S. telecommunications insecurity 2022," which CISA has acknowledged it commissioned while refusing multiple requests for a copy from my staff.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator

CC: Kemba Walden, Acting National Cyber Director
Jessica Rosenworcel, Chairwoman, Federal Communications Commission
Clare Martorana, Federal Chief Information Officer, Office of Management and Budget