

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

November 4, 2021

The Honorable Lloyd J. Austin III
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301-1000

The Honorable Antony Blinken
Secretary of State
2201 C Street NW
Washington, DC 20520

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane
Washington, D.C. 20528-0380

The Honorable Avril Haines
Director of National Intelligence
Washington, DC 20511

The Honorable Jessica Rosenworcel
Chairwoman
Federal Communications Commission
445 12th Street, SW
Washington DC 20554

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue Northwest
Washington, DC 20535

Dear Secretary Austin, Secretary Blinken, Director Easterly, Director Haines, Chairwoman Rosenworcel, and Director Wray:

I write with concern regarding the U.S. Government's abysmal failure to protect federal workers from the counterintelligence threat posed by cell phone surveillance technology.

It has been a matter of public record for decades that phones can be tracked and calls and text messages intercepted using a device called a cell site simulator, which exploits long-standing security vulnerabilities in phones by impersonating a legitimate phone company's cell towers. These surveillance devices have been available for sale since the late 1990s, and used by the government subject to rules outlined in Department of Justice guidance first published in 1997. But the U.S. does not and has never had a monopoly over this surveillance technology — cell site simulators are widely available on the global market, including to America's adversaries.

While the threat posed by this technology has been clear for years, the U.S. Government has yet to meaningfully address it. Both the Department of State and Department of Defense have confirmed to my office that they lack the technical capacity to detect cell site simulators in use near their facilities. Recognizing this threat, Congress in 2019 gave the Director of National Intelligence (DNI) and the Federal Bureau of Investigation (FBI) the authority to detect and deploy countermeasures against this technology, prioritizing the National Capital Region. It is imperative that the DNI and FBI exercise this authority.

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

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

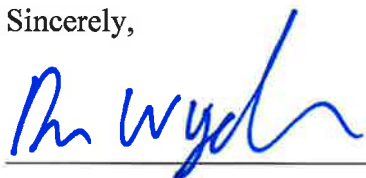
PRINTED ON RECYCLED PAPER

After consecutive administrations failed to address this counterintelligence threat, President Biden now has the opportunity to finally secure America's phone networks. However, doing so will require a whole-of-government effort, including: deploying counter-surveillance sensors near sensitive federal facilities, including overseas military bases and diplomatic facilities; requiring phone manufacturers and wireless carriers to make it easier for users of phones to turn off support for older, insecure 2G and 3G networks; and requiring that federal workers' voice and text communications be end-to-end encrypted. To that end, I ask that you provide me with an unclassified joint response by December 10, 2021, with a plan of action to address this national security threat, as well as answers to the following questions:

1. Which federal agency is responsible for ensuring that U.S. phone networks cannot be easily surveilled by foreign governments? If none, please explain why.
2. Which federal agency has the authority to require phone manufacturers and cellular network operators to fix the vulnerabilities exploited by cell site simulators? If none, please explain why.
3. Which federal agency has the authority to require that intra-executive branch unclassified voice calls be end-to-end encrypted? If none, please explain why.
4. Which federal agency is responsible for protecting U.S. Government facilities in the United States from cell site simulators? If none, please explain why.
5. Which federal agency is responsible for protecting U.S. Government facilities outside the United States from cell site simulators? If none, please explain why.

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