

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

June 30, 2025

The Honorable Kash Patel
Director
Federal Bureau of Investigation
935 Pennsylvania Ave. NW
Washington, DC 20535

Dear Director Patel:

I write with concern that the Federal Bureau of Investigation (FBI) is not taking seriously the counterintelligence threat posed by spyware and is not providing government officials with effective cybersecurity guidance to defend against that threat.

According to press reports, experts detected spyware targeting the phones of elected officials and their staff at the European Parliament and in the United Kingdom, France, Mexico, Poland, and Spain. The U.S. faces the same threats. Spyware has been discovered on the phones of a dozen U.S. diplomats serving overseas and, reportedly, those of White House officials. Members of Congress have also reportedly been targeted by foreign governments with commercial spyware. Yet in spite of the seriousness of the spyware threat, the FBI has yet to provide effective defensive guidance.

FBI guidance to the Senate, which presumably mirrors its guidance to Executive Branch officials, has thus far consisted of remedial advice such as not clicking on suspicious links or attachments, not using public Wi-Fi networks, turning off Bluetooth, keeping phone software up to date, and rebooting regularly. This is insufficient to protect Senate employees and other high-value targets against foreign spies using advanced cyber tools. Well-funded foreign intelligence agencies do not have to rely on phishing messages and malicious attachments to infect unsuspecting victims with spyware. Cyber mercenary companies sell their government customers advanced “zero-click” capabilities to deliver spyware that do not require any action by the victim.

Potential victims of spyware can still take straightforward steps to meaningfully raise their cyber defenses by making their phones harder to hack. These best practices are already recommended by the FBI and other government agencies, in obscure online resources, but not, seemingly, as part of the FBI’s guidance to U.S. officials. I therefore request that future briefings, for Congress and Executive Branch officials include current best practices against advanced cyber threats, such as:

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

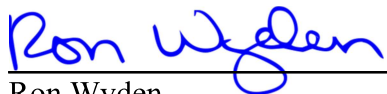
[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)
PRINTED ON RECYCLED PAPER

1. **Enable opt-in anti-spyware defenses in Apple's iOS and Google's Android phone software.** The FBI co-issued defensive cyber guidance in May 2024 to individuals in civil society likely to be targeted with spyware, along with the Cybersecurity and Infrastructure Security Agency (CISA) and the governments of Canada, Estonia, Japan and the United Kingdom. That advice recommends enabling Lockdown Mode in Apple's iPhone and iPad software, which is an opt-in security feature specifically designed to defend against advanced forms of spyware. CISA subsequently issued communications security advice to government officials in response to the Salt Typhoon hacks in 2024, which also recommended Lockdown Mode. A similar feature also exists for Android, called Advanced Protection Mode, which was recommended by the CISA cybersecurity advisory committee in 2023.
2. **Use ad blocking.** The FBI issued public guidance in 2022 recommending ad blocking software to protect against malicious advertisements, which can be used to deliver spyware. CISA and NSA both also recommend ad blocking.
3. **Disable ad tracking IDs.** CISA and the National Security Agency have both issued public guidance recommending disabling the unique advertising ID assigned to phones by Google and Apple via the phone's privacy settings, which can make it harder to target users with malicious ads and to collect and sell their location data.
4. **Opt-out of commercial data brokers,** to make it harder for adversaries to learn the cell phone numbers of potential targets. In public guidance issued in June 2024 to critical infrastructure personnel, CISA recommended that they "opt-out of the major data broker and people search sites or subscribe to a service to do that for you." This defense against doxing can also help to protect against spyware, because spyware often exploits vulnerabilities in widely used messaging apps such as iMessage and WhatsApp to infect the victim's phone, which requires the victim's phone number.

Our adversaries have upped their game, and we must up our defenses. Accordingly, I urge you to update the content of the FBI's counterintelligence and cyber briefings to include these and other high-impact cyber defenses against spyware.

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:

Jennifer A. Hemingway, Senate Sergeant at Arms
Nicolette Llewellyn, Director of Senate Security