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

March 3, 2023

The Honorable Karen Gibson
Sergeant at Arms and Doorkeeper
United States Senate
Washington, DC 20510

Dear Sergeant Gibson:

I write to commend you and your staff on their recent work to upgrade the Senate's cybersecurity by supporting phishing-resistant multi-factor authentication (MFA). But offering support for this cyber defense is just the first step. I urge you to take additional steps to ensure that this industry-standard cybersecurity technology is widely used in the Senate.

In 2017, I wrote to the chairman and ranking member of the Senate Rules Committee to urge an upgrade to the Senate's cybersecurity, to be consistent with industry and executive branch best practices. I urged the Committee to require physical MFA tokens to secure both remote and in-person access to Senate systems. In January of 2022, the Office of Management and Budget (OMB) issued a new policy requiring executive agencies to improve their cybersecurity and adopt phishing-resistant MFA. The OMB endorsement of and requirement to use phishing-resistant MFA has been echoed by both Cybersecurity and Infrastructure Security Agency and the National Security Agency, which have recommended the adoption of this technology in public education materials they have published online.

While OMB's mandate to use phishing-resistant MFA only applies to executive branch agencies, my staff has over the past year urged your Chief Information Officer and Chief Information Security Officer to upgrade the Senate's cybersecurity to be consistent with the OMB policy and industry best practices. In particular, my staff urged your team to support and offer at no cost to Senate offices FIDO tokens, a phishing-resistant industry standard for MFA. FIDO tokens are widely recommended by cybersecurity experts in government, industry, and academia, supported by the major operating systems and cloud computing providers, manufactured by several competing firms, and sold for about $30 each; less in bulk.

To their credit, your staff have been responsive to my request to add support for FIDO tokens. They have worked diligently over the past year to test and deploy support for this industry standard to protect remote users accessing the Senate's Virtual Private Network (VPN). This is an excellent first step. But offering support for more-secure FIDO technology on an opt-in basis isn't enough. Thousands of Senate employees who currently use less-secure forms of MFA must be re-issued new, phishing-resistant FIDO tokens and the Senate must stop supporting methods

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

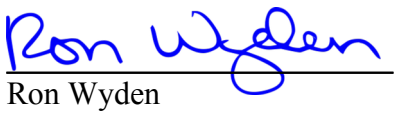
707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589–4555

HTTPS://WYDEN.SENATE.GOV

of MFA that are vulnerable to phishing. I also reiterate my request from 2017 that you require the use of FIDO tokens to login to Senate-issued and Sergeant at Arms-administered desktop and laptop computers, not just for remote users accessing the Senate's VPN.

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