

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

June 28, 2018

COMMITTEES:

COMMITTEE ON FINANCE

COMMITTEE ON BUDGET

COMMITTEE ON ENERGY & NATURAL RESOURCES

SELECT COMMITTEE ON INTELLIGENCE

JOINT COMMITTEE ON TAXATION

The Honorable Walter G. Copan
Director
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Dear Director Copan:

I write to ask that the National Institute of Standards and Technology (NIST) evaluate and then encourage government use of modern encryption technology to secure remote network communications.

Virtual private networks (VPNs) protect the confidentiality and integrity of data as it travels across the internet by authenticating and encrypting traffic. Data generated and stored by government agencies is increasingly valuable. As such, VPNs are an essential tool for protecting data.

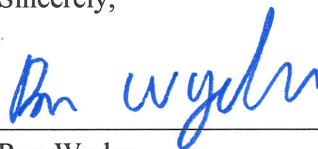
Two aging technologies, IPsec and OpenVPN, are currently used for most government VPNs. Cybersecurity researchers now know that the complexity of these old technologies can completely undermine their security. In the twenty years since the development of these two widely-used VPN technologies, the software engineering and cryptography communities have learned valuable lessons about the importance of simplicity and conservative design. Experts now recognize that encryption technologies should be secure by default, should not include unnecessary options, and should make it impossible for developers and system administrators to proverbially shoot themselves in the foot by choosing the wrong configuration.

Recently, a new open-source VPN technology called Wireguard has gained prominence. To ensure security, its design emphasizes simple setup and minimizes the number of available options. Notably, Wireguard is now being incorporated into the Linux operating system, a clear signal of its widespread support in the technology and security industries.

In light of the serious cybersecurity issues with the two most widely-used VPN technologies, I urge NIST to work with stakeholders to evaluate appropriate replacements, including Wireguard, for government use. I also ask that once NIST finds an appropriate replacement, existing VPN guidelines and support should quickly be discarded in favor of the newer alternative.

If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator

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

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER