

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

COMMITTEES:

COMMITTEE ON FINANCE

COMMITTEE ON BUDGET

COMMITTEE ON ENERGY & NATURAL RESOURCES

SELECT COMMITTEE ON INTELLIGENCE

JOINT COMMITTEE ON TAXATION

October 24, 2018

The Honorable Christopher C. Krebs
Under Secretary for National Protection and Programs
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Krebs:

I write to urge the Department of Homeland Security (DHS) to protect web browsing information about Americans, including U.S. government employees. Metadata revealing specific website visits is currently transmitted over the internet without encryption, leaving it vulnerable to interception and tampering by foreign hackers and cyber criminals.

Data sent over the web is now increasingly encrypted by default. According to Google, U.S. users of the Chrome browser now access 85 percent of web pages over an encrypted connection. Thanks to DHS' strong cybersecurity leadership, roughly 70 percent of federal government websites now use encryption best practices, protecting the contents of web pages from prying eyes and third-party tampering. However, some metadata is still transmitted in the open, revealing the domain name of the website the user is visiting. Hackers can intercept or hijack the unprotected metadata, tricking users into visiting a malicious site or spying on their activities.

Two new technologies can help remedy this situation. The first method of protection applies to the DNS (Domain Name System) and uses one of two forms of encryption (DNS-over-HTTPS or DNS-over-TLS) to protect metadata which reveals the name of websites as users visit them. In order to protect DNS information revealing which websites federal workers are accessing from interception, DHS should require, where possible, that federal agencies encrypt employees' DNS queries. Federal agencies could protect DNS data either by operating their own encrypted DNS servers, or using private encrypted DNS services, provided that they meet rigorous cybersecurity and privacy standards.

A second promising new cybersecurity technology, Encrypted Server Name Indication (ESNI), protects the name of a website that the user is attempting to visit as it is transmitted to the site that the user wishes to visit. This technology is particularly useful when it is used by major content distribution networks (CDN), which provide internet connectivity to tens or hundreds of thousands of different websites. When ESNI is used by a CDN, any hacker intercepting a user's internet browsing data will only learn that the user is visiting a website delivered by a particular CDN and not which particular site the user is visiting.

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

Consider the following two practical examples:

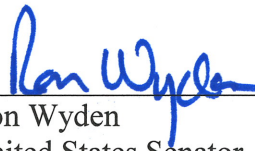
- The Department of Defense (DoD) operates an online sexual assault hotline at www.safehelpline.org. Amazon Web Services hosts the website and while the website already uses encryption to protect content delivered to visitors, metadata about the visit itself is not currently protected because Amazon does not currently support ESNI. This means that third parties could potentially identify specific Americans accessing the DoD Safe Helpline even if those third parties can't see the encrypted content.
- The Federal Bureau of Investigation operates an online tip line at tips.fbi.gov. The FBI's website is hosted by a company that supports ESNI. As such, when this FBI website is visited by Americans that are using a web browser that supports ESNI, the name of the particular website being visited will not be revealed to a hacker or foreign government that is intercepting the website data.

Although only one major CDN and one major web browser currently support ESNI, this is likely to change in the coming months, particularly with encouragement and support from the U.S. government. In order to promote broad industry adoption of this important cybersecurity technology and therefore protect sensitive metadata about Americans' visits to all U.S. government websites, I urge DHS to work with the General Services Administration to require companies to enable ESNI as a condition of selling CDN service to the U.S. government.

In 2014, Congress gave DHS the power to require federal agencies to adopt cybersecurity technologies and DHS has repeatedly used this authority to improve the government's security posture. Indeed, you recently issued Binding Operational Directive 18-01, which, among other things, instructed federal agencies to encrypt their websites. Requiring agencies to protect metadata with encrypted DNS and ESNI is the next logical step.

I appreciate all that you do on behalf of America's cyber defenses and look forward to your affirmative response within the next 60 days. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator

CC:

Dr. Walter G. Copan, Under Secretary of Commerce for Standards and Technology & Director, National Institution of Standards and Technology
Emily W. Murphy, Administrator of the U.S. General Services Administration
Dana Deasy, Chief Information Officer, Department of Defense.