

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

May 22, 2018

Dana Deasy
Chief Information Officer
U.S. Department of Defense
1300 Defense Pentagon
Washington, DC 20301-1300

Dear Mr. Deasy:

I write to ask that you take immediate action to require the adoption of cybersecurity best practices on all publicly accessible Department of Defense (DoD) web services.

In 2015, the Office of Management and Budget (OMB) issued memo M-15-13, requiring all federal agencies take steps to secure their websites and other web services—including interfaces for automated, programmatic interaction (APIs)—from cyberattacks. The OMB memo gave agencies until the end of 2016 to enable HTTPS encryption and to enforce its use with HTTP Strict Transport Security (HSTS), which ensures web browsers will not use insecure protocols when connecting to HSTS-enabled websites. In 2017, the Department of Homeland Security (DHS) issued Binding Operational Directive (BOD) 18-01, reiterating the OMB requirements and requiring civilian agencies to adopt additional forms of basic cyber hygiene.

A small number of DoD websites including the Army, Air Force, and the National Security Agency homepages currently implement HTTPS by default and use certificates trusted by major web browsers. Unfortunately, many other sites, including the Navy, Marines, and your own office's website at dodcio.defense.gov, either do not secure connections with encryption or only prove their authenticity using a certificate issued by the DoD Root Certificate Authority. Many mainstream web browsers do not consider these DoD certificates trustworthy and issue scary security warnings that users are forced to navigate before accessing the website's information. These challenges do not only impact civilians; servicemembers accessing DoD pages from home regularly encounter security warnings and must click through such errors when accessing public DoD resources.

The DoD cannot continue these insecure practices. Starting in July, the Google Chrome browser will begin warning visitors to non-HTTPS sites that the requested site is not secure. These warnings will erode the public's trust in the Department and its ability to defend against sophisticated cyber threats. Moreover, the DoD's refusal to implement cybersecurity best practices actively degrades the public's security by teaching users to treat critical security warnings as irrelevant. Normalizing these warnings increases the risk of cybercrime and foreign-government hacking, as users, both military and civilian, incorporate these dangerous practices reinforced by the DoD into their daily habits.

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)

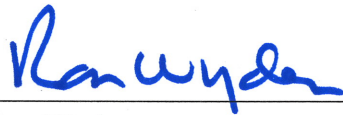
PRINTED ON RECYCLED PAPER

DoD has prided itself on cybersecurity leadership and now is the time to again demonstrate that leadership. I urge you to direct all DoD agencies and offices to take the following three concrete steps to improve the cybersecurity of their publicly accessible web services:

- Adhere to all the guidelines specified in OMB memo M-15-13 and DHS Binding Operational Directive 18-01, including:
 - Enable HTTPS with HSTS on all public web services;
 - Facilitate the adoption of HSTS by delivering a list of all public DoD domains, including .mil addresses, to DHS, as required by DHS Binding Operational Directive 18-01;
- Obtain and deploy certificates trusted by major web browsers for all web services accessible to the general public; and
- Evaluate the use of shorter-lived, machine-generated certificates, such as those available at no cost from organizations like Let's Encrypt.

Please provide me an action plan by July 20, 2018, describing your progress implementing these steps and detailing an estimated date by which all publicly accessible DoD web services will implement these cybersecurity best practices. If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator