

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

December 12, 2017

The Honorable Lt. Gen. H.R. McMaster, Jr.,
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear General McMaster:

I write to ask that you take immediate action to secure federal elections from hacking by foreign governments.

The hacking efforts by the Russian government during the 2016 election should serve as a wake-up call to the U.S. government. Moving forward, foreign governments will continue to exploit cybersecurity weaknesses in our election infrastructure. While some states have taken the threats seriously, others are seriously lagging behind and remain woefully vulnerable to foreign government cyberattacks. As such, the federal government must take action: leaving federal election cybersecurity to the states is irresponsible and a total abdication of the federal government's primary role in matters of national security.

Cybersecurity experts have complained for decades about the risks associated with insecure electronic voting machines and the need for paper audit trails. Their warnings have largely gone unheeded. Fourteen states still use Direct Recording Electronic voting machines that record votes directly into the machines' digital memory. These voting machines do not produce a paper trail and cannot be subsequently audited if voting officials have any reason to doubt the validity of the electronic vote tally. Moreover, according to the *New York Times*, Georgia conducted November's elections on voting machines running Windows 2000; parts of Pennsylvania relied on machines running Windows XP. These two operating systems are decades old and no longer receive critical security updates, which leaves them especially vulnerable to cyberattacks.

At a Senate hearing in October, Attorney General Jeff Sessions conceded that the U.S. government is not doing enough to prevent future election interference by Russia and other foreign adversaries. When asked if the government is taking adequate action to prevent meddling in elections, Attorney General Sessions stated that "we're not," and that "the matter is so complex that for most of us we're not able to fully grasp the technical dangers that are out there." Attorney General Sessions' testimony suggests that the Administration is not taking this issue seriously enough or dedicating sufficient resources to fixing it. That must change.

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

I will soon be introducing legislation to bolster the cybersecurity of federal elections by requiring common-sense measures widely recommended by experts. In particular, my bill will require that all election bodies conduct “risk-limiting audits” of federal election results, regardless of how close the elections are. These statistically rigorous audits, already required by state law in Colorado and Rhode Island, provide a high degree of confidence in election results and thus determine whether the electronic tallies have been tampered with or hacked, without the cost and labor that would otherwise be required to hand-count every single paper ballot.

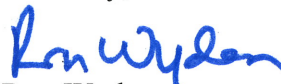
Unfortunately, even with clear evidence that states are not addressing their vulnerable election infrastructures, Congressional leadership has been unwilling to schedule legislative efforts that either provide oversight or require states to adopt common-sense election-cybersecurity measures. Congressional leadership conveniently chooses to believe that this is a states’ rights issue, even if it means leaving our national elections vulnerable to cyberattacks by foreign governments.

Without bipartisan support, Congress cannot address this critical national-security threat. As such, the executive branch must shoulder the burden of protecting federal elections from foreign cyberattacks. To that end, I ask that you take the following concrete steps:

1. Designate a senior White House official to “own” the issue of election cybersecurity and require that official to brief Congress regularly on cybersecurity threats, mitigation efforts underway, and key barriers to implementation.
2. Direct the National Institute of Standards and Technology and the Department of Homeland Security (DHS) to create an objective framework to grade states on their election cybersecurity and publish annual “scorecards” giving each state a letter grade and describing the areas in which each needs to improve.
3. Direct DHS to designate political campaigns as part of our nation’s critical infrastructure so that campaigns can receive cybersecurity assistance if they request it.
4. Direct the Secret Service to expand Presidential candidate security to include cybersecurity. At the very least, the Secret Service should help candidates and their campaigns secure email, voice, and text communications.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,



Ron Wyden
United States Senator