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

June 11, 2018

Commissioner Thomas Hicks, Chair
Commissioner Christy McCormick, Vice Chair
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Dear Commissioners Hicks and McCormick:

I write to inquire about the Election Assistance Commission's (EAC) efforts to help states improve the cybersecurity of elections.

In 2005, the EAC published the Voluntary Voting System Guidelines (VVSG)–recommendations designed to ensure state voting systems guarantee "basic functionality, accessibility, and security." These guidelines serve as suggestions to the states and producers of voting technology–several of which cite compliance with the VVSG as evidence that their products are secure.

In 2007, the National Institute of Standards and Technology (NIST) compiled a set of suggested changes to the VVSG, including recommending the use of voter-verifiable paper ballots. The EAC subsequently rejected these recommendations. Although the EAC has made revisions to the VVSG since, the guidelines still encourage states to adopt policies–including certifying machines that make auditing difficult and permitting voting systems to be connected to the internet–that are wildly inconsistent with modern cybersecurity best practices.

Given the well-resourced, organized, and persistent threat posed by foreign governments to the integrity of our elections, it is more important than ever that the EAC promote the use of secure voting technologies and practices. Indeed, earlier this year, congress recognized the importance of election security by appropriating $380 million for the EAC to distribute to states for election technology and security upgrades.

Absent guidance from the EAC, some states may opt to spend these new funds on insecure voting technology. Election security experts have worked tirelessly to understand and articulate the vulnerabilities certain types of machines can introduce into elections. For instance, paperless 'direct-recording electronic' (DRE) machines cannot be meaningfully audited and leave voters unsure whether their vote will be properly

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
PRINTED ON RECYCLED PAPER

tabulated. Newer voting technologies, including 'voter verified paper audit trails' (VVPAT) voting machines and 'ballot marking devices' (BMD) that generate non-human readable printouts like barcodes, theoretically allow voters to verify their ballots. Security experts agree, however, that in practice these machines do not substantially increase election security and in fact enable cyberattacks through malware and system failure. Failing to clearly impart this knowledge to the states would be a tremendous wasted opportunity.

Beyond voter verification, it is important that voting machines employ basic cyber hygiene. Specifically, voting machines and the computers used to program them should never be connected to the internet, nor should remote administration software ever be installed on them.

The EAC must act to secure our elections from advanced cyber threats. In particular, the EAC should issue up-to-date guidelines that incorporate the recommendations of cybersecurity experts. The EAC should also promptly advise states against using EAC-distributed federal funds to purchase insecure voting technologies–described above–which violate cybersecurity best practices. I would also appreciate responses to the following questions by July 15, 2018:

1. Does the EAC currently employ any full-time technical staff with demonstrated expertise in cybersecurity?
    a. If yes, please describe their roles and responsibilities.
    b. If not, please explain why.
2. What are the EAC's processes for ensuring that EAC-certified voting systems used by states are properly maintained by manufacturers and administrators such that they adhere to cybersecurity best practices?
3. Has the EAC ever revoked the certification of a voting system because of a cybersecurity issue?
    a. If yes, please provide a record of any such instances.
    b. If no, does this mean that the EAC believes that all previously certified voting machines are still secure?
4. How will the EAC ensure that the cybersecurity concerns outlined by cybersecurity experts, including those at NIST, are properly conveyed to states as the states determine how to spend their share of the $380 million dollars recently appropriated by Congress?
5. Does the EAC support the common-sense requirement for open-ended investigation of potential vulnerabilities, such as penetration testing, red teaming, or open-ended vulnerability testing, in voting systems by an independent body of experts before certification?
    a. If not, please explain why.
    b. If yes, please describe what steps, if any, the EAC has taken to facilitate or encourage these robust cybersecurity-testing practices.

6. In a public letter on January 7, 2017, Commissioner McCormick dismissed the intelligence community's assessment that Russia engaged in election interference in 2016. In support of this claim, Commissioner McCormick cited statements made by John McAfee during a TV appearance on Russia Today on January 6, 2017. In her letter, Commissioner McCormick described Mr. McAfee as a "cyber security expert." Please identify all of the other cybersecurity experts the EAC has relied upon for advice since January 2016.

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

Sincerely,

Ron Wyden

Ron Wyden
United States Senator