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

March 6, 2018

Mr. Tom Burt
President and Chief Executive Officer
Election Systems & Software, LLC
11208 John Galt Boulevard
Omaha, NE 68137

Dear Mr. Burt:

I write to you, for a second time, to seek answers to basic questions about your firm's cybersecurity practices in order to better understand the threat posed by foreign government hackers to our election infrastructure.

The U.S. Intelligence Community has assessed with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. The intelligence community has also assessed that the 2018 U.S. midterm elections are a potential target for Russian influence operations. Given the real threat that our democracy now faces from hostile foreign governments, it is of paramount importance that our election infrastructure be secure against cyberattacks. As the largest U.S. manufacturer of voting machines and election technology, your firm is an obvious target for hackers and foreign nation states.

The American public has been repeatedly assured that voting machines are not connected to the internet, and thus, cannot be remotely compromised by hackers. However, according to a recent article in the *New York Times Magazine*, election systems sold by your company frequently include pre-installed remote-access software, which exposes elections systems to remote attack and compromise. In other cases, where the software isn't pre-installed, ES&S officials have apparently advised state and local governments to install the software to allow ES&S technicians to remotely access the election systems. The default installation or subsequent use of remote-access software on sensitive election systems runs contrary to cybersecurity best practices and needlessly exposes our election infrastructure to cyberattacks.

In order to help me understand the scope of this alleged practice, I would appreciate responses to the following questions by March 30, 2018. In addition, please also provide me with complete answers to the questions I asked in my October 3, 2017 letter. Although I received a written response from your company on October 26, 2017, that response did not include answers to my questions.

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

1. Has ES&S sold any products on which remote-access software was pre-installed? If yes, please:
    a. Describe each product that included such software and identify all of the state and local governments that purchased it.
    b. Describe the security settings used for the remote-access software, including whether or not it was configured to use default or hard-coded passwords.
    c. Describe whether or not the remote-access software and the configuration settings used by ES&S were subjected to a security audit prior to shipping to state and local government customers. Please provide me with copies of all security audit reports related to this software.

2. Have ES&S officials or technical support personnel ever recommended that customers install remote-access software on voting machines or other election systems?
    a. If yes, how many state or local governments were advised to do so?

Sincerely,

Ron Wyden

Ron Wyden
United States Senator