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 3, 2017

Mr. John Poulos
President & Chief Executive Officer
Dominion Voting Systems
215 Spadina Avenue, Suite 200
Toronto, ON M5T 2C7
Canada

Dear Mr. Poulos:

I write to seek public answers about cybersecurity threats to our election infrastructure and whether the election technology industry has taken steps to defend against hackers, including those working for foreign governments.

As our election systems have come under unprecedented scrutiny, public faith in the security of our electoral process at every level is more important than ever before. Ensuring that Americans can trust that election systems and infrastructure are secure is necessary to protecting confidence in our electoral process and democratic government.

In order for Congress and the American people to better understand the threats that your company faces and the steps you have taken to protect against them, I would appreciate complete answers to the following questions by October 31, 2017.

1. Does your company employ a Chief Information Security Officer? If yes, to whom do they directly report? If not, why not?
2. How many employees work solely on corporate or product information security?
3. In the last five years, how many times has your company utilized an outside cybersecurity firm to audit the security of your products and conduct penetration tests of your corporate information technology infrastructure?
4. Has your company addressed all of the issues discovered by these cybersecurity experts and implemented all of their recommendations? If not, why not?
5. Do you have a process in place to receive and respond to unsolicited vulnerability reports from cybersecurity researchers and other third parties? How many times in the past five years has your company received such reports?
6. Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data? If your company has suffered one or more data breaches or other cybersecurity incidents, have you reported these incidents to federal, state and local authorities? If not, why not?

7. Has your company implemented the best practices described in the National Institute of Standards and Technology (NIST) 2015 Voluntary Voting Systems Guidelines 1.1? If not, why not?
8. Has your firm implemented the best practices described in the NIST Cybersecurity Framework 1.0? If not, why not?

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