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. Jack Cobb
President
Pro V&V
700 Boulevard South
Suite 102
Huntsville, AL 35802

Dear Mr. Cobb:

I write to seek public answers about cybersecurity threats to our election infrastructure and whether the election technology and election technology testing industries have 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. This effort must include not only the manufacturers and government consumers of election systems but also the Voting System Test Laboratories accredited by the U.S. Election Assistance Commission.

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 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 testing equipment and systems and to 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. What is the process for when your laboratory determines that a product undergoing testing has potential security vulnerabilities? Do all security vulnerabilities result in non-certification of a product undergoing testing? Are all product security vulnerabilities reported to the manufacturer and to the Election Assistance Commission?
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

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

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 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

Ron Wyden
United States Senator