Five Cedars Group, Inc.

October 25, 2017

Senator Ron Wyden
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden,

We are responding to your letter regarding election security issues dated October 3, 2017.

While we are thrilled to get your letter to election technology companies, as it validates our small role in the election process, we have to report that most of your questions don't apply to our company or product.

Five Cedars produces accessible HTML and large print ballots for use by voters with disabilities. We do this for all 36 counties in Oregon, and have since 2008. This form of ballot delivery is called "remote accessible vote-by-mail" or RAVBM. Because of the way the Oregon Secretary of State office designed the process back in 2007, at no time are ballots posted on a Five Cedars server. We also never receive any voter registration data, marked ballots or any other document that would of interest to a hacker.

Before every election, the counties, using a login and password, upload their ballot definition files to our Citrix ShareFile account. We download the definition files, run them through our ballot generator program and upload the HTML ballots, again using a login and password, to the Citrix ShareFile server. The counties then download the ballots, visually verify they are correct and post them to the Secretary of State's server for voter's to access. Five Cedars role in the chain of ballot custody ends with us uploading the files to Citrix ShareFile.

Answers to your questions:

1. We are a small company and don't have a security officer. Our development environment resides behind two firewalls. All our machines have virus and firewall software installed. We don't host any live ballots or election files.
2. We have a network contractor that set up and periodically modifies our network passwords.
3. We have never utilized an outside cybersecurity firm. Again, we don't host any election data or ballots.
4. N/A.
5. We have never received any unsolicited vulnerability reports.
6. We are not aware of any data breaches or other cybersecurity incidents.
7. To our knowledge, we have not implemented any of the best practices of the VVSG 1.1, as none of them apply to our product, a remote Ballot Marking Device. We do meet the practices defined in the NIST report *"Principles and Guidelines for Remote Ballot Marking Systems."* We are also on the NIST working committees for Human Factors and Interoperability.
8. We have reviewed the NIST Cybersecurity Framework 1.1 (draft report) and believe we are meeting its suggested security protocols.

As another data point, our remote accessible ballots and process has just been certified by the California Secretary of State. As part of that process, California hired a Voting Systems Testing Lab (VSTL) to test the security of our code, ballot delivery, and accessibility of our ballots. We passed their scrutiny and are actively marketing our services in California, Ohio and Hawaii.

Senator, we are pleased that you are working to make our election equipment and voting processes secure and safe. We wholeheartedly endorse your efforts.

Five Cedars would be pleased to give you a demonstration of our accessible ballots next time you are back in Oregon.

Sincerely,

John Schmitt
President