United States Senate

WASHINGTON, DC 20510

August 22, 2018

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

Dear Mr. Burt:

As members of the United States Senate Select Committee on Intelligence, we agree with the conclusion of the Intelligence Community: America's elections are the target of unprecedented attacks by foreign adversaries. Free, fair, and trusted elections are the bedrock of our democracy, and safeguarding our elections is an urgent national security priority. We are concerned that ES&S and other election system providers may not be prepared for the growing threats to our elections.

The reality of these unprecedented security risks was on full display at the DEF CON cybersecurity conference, where researchers at the "Voting Village" successfully probed a variety of electronic equipment used to administer elections. We are disheartened that ES&S chose to dismiss these demonstrations as unrealistic and that your company is not supportive of independent testing. We believe that independent testing is one of the most effective ways to understand and address potential cybersecurity risks.

Election agencies must be able to make informed decisions about what election equipment will help them conduct secure elections, and independent testing helps both election agencies and vendors. Many industries have found that a critical element of security testing involves embracing the work of the independent security research community. Many of the world's leading electronics and software companies have opened their arms to the research community, maintaining active presences at the largest security research conferences and inviting "white hat" hackers to probe their products to identify how they can improve product security.

Currently, there are significant barriers that prevent states from working with independent, qualified, good faith researchers to conduct cybersecurity testing on election systems. States are often unable to procure systems at a reasonable cost before entering long-term contracts with vendors. Most researchers are unable to procure systems from vendors for testing, no matter how trustworthy and well-resourced they are. In addition, legal ambiguities about contracts and software licensing chill this valuable practice. Furthermore, we believe that urging the Copyright Office to limit good faith cybersecurity testing on election systems under the Digital Millennium Copyright Act[1] is harmful to this effort.

---

[1] U.S. Copyright Office, Long Comment Regarding a Proposed Exemption under 17 U.S. Code § 1201. (https://www.copyright.gov/1201/2018/comments-021218/class10/Class_10_Opp'n_Election_System_Providers.pdf)

We ask for your attention in this very important matter and request responses to the following questions:

1. Will ES&S commit to allowing election agencies to arrange independent, qualified, good faith cybersecurity tests of ES&S election systems and share results with the public? Further, will ES&S work with agencies to conduct these tests? If not, why not?

2. Will ES&S commit to providing election agencies with ES&S election systems at a reasonable cost, before entering into a long-term contract with ES&S, so that they can arrange independent cybersecurity testing? If not, why not?

3. Will ES&S commit to providing independent, qualified, good faith cybersecurity researchers with ES&S election systems at a reasonable cost so that the researchers can conduct cybersecurity testing and share their results with the public? If not, why not?

Our elections remain vulnerable to attack and taking steps to secure them cannot wait. As a result, we ask for a response by Wednesday, August 29, 2018.

Sincerely,

Kamala D. Harris
United States Senator

Mark R. Warner
United States Senator

Susan M. Collins
United States Senator

James Lankford
United States Senator