Election Systems & Software
11208 John Galt Blvd · Omaha, NE 68137
P: 402.938.1437 · TF: 1.877.377.8683
teburt@essvote.com · www.essvote.com

August 24, 2018

By Email & UPS Overnight

The Honorable Kamala D. Harris
112 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mark. R. Warner
703 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Susan M. Collins
413 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable James Lankford
316 Hart Senate Office Building
Washington, D.C. 20510

Dear Senators Harris, Collins, Warner and Lankford,

Thank you for your letter of August 22, 2018, and for the opportunity to discuss how Election Systems & Software (ES&S) is working with many stakeholders, including the U.S. government, to secure our democracy through free and fair elections.

Below please find our answers to your questions, as well as our invitation for you to join us in a discussion on election integrity.

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?*

Our answer to your question is yes.

ES&S enlists election agencies to conduct independent, qualified, good-faith cybersecurity tests of ES&S election systems. ES&S products are certified by the U.S. government, which conducts independent testing. In addition, our products are tested by several third-party experts, including those being arranged by the Department of Homeland Security (DHS). As you may know, certification via the federal Election Assistance Commission (EAC) is an extremely thorough process that requires thousands of hours for testing of each product and often each product variant. Additionally, many states, including California, require a separate, extensive testing and certification process. Any assertion that our products are not thoroughly and independently tested, or that we do not allow election agencies to arrange testing, is erroneous.

ES&S will continue to share significant findings with the EAC, Voting System Test Labs, and the State and Local Election Officials we partner with and support. We will not, however, provide or submit any hardware, software, source code or other intellectual property to unvetted, anonymous security researchers, nor would we make public any assessments of vulnerability findings, because providing or making available secure information to individuals or groups whose interests may counter the United States' interests would be irresponsible and may in fact, jeopardize the integrity of elections.

ES&S tests, independent tests, and third-party tests are conducted under both extreme laboratory conditions, as well as realistic conditions that replicate a typical polling place or elections office to take into account what kind of hacking is and isn't possible during an actual election. That way, time and resources are directed to vulnerabilities that are actually capable of being exploited. We believe there is real value in the ethical "white hat" hackers. We agree security researchers or ethical hackers often provide significant and measurable insight into the vulnerabilities associated with technology of all kinds. Whether it is hardware, software, personnel, or facilities, security researchers help technology manufacturers be more aware of the cyber threats that may affect the devices

we use in our daily lives. Security researchers also assist government and businesses in protecting vital information and critical infrastructure assets important to our national security and democracy.

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?*

Our answer to your question is yes.

ES&S makes its systems available for review at no cost before an election jurisdiction makes a financial commitment to acquire the system. First, we provide system review through the above-mentioned EAC federal testing program which makes available the complete test reports of our systems for public review. Second, each state election authority requires its own level of testing of voting systems before a jurisdiction can acquire a voting system. Many of these states use independent third-party researchers, academics, and laboratories – all of whom we most willingly work with. The results of the tests determine whether a system is allowed to be used within a jurisdiction.

All of this information and access ensures election agencies make informed decisions about which election equipment will help them conduct secure elections.

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 answer to your question is yes.

We will commit to this and, as stated above, ES&S already uses independent qualified, good-faith cybersecurity testing and researchers and shares information and coordinates with appropriate government and elections agencies to ensure we provide the best protection possible for this vital element of our nation's infrastructure. We actively meet and work with academics, researchers, all levels of government, and other outside experts to ensure we provide the best protection possible for this vital element of our nation's infrastructure.

Senators, we respect your positions and share your interests in election security. We are an American company that dedicates each and every day to the security of elections, as well as every other aspect of this cornerstone of our nation's democracy. Independent, robust, and ethical testing is just one example of the steps we take—as a matter of course—to ensure election integrity. It is to our benefit to do so—any compromise of our products or technology would be harmful to our business, to our personal integrity, and to the trusted relationships we have built over the last 40 years.

Elections are our sole business. Our dedicated employees spend all their waking hours on research, development, security, and ongoing support of our products and processes for our nation's elections. We support many of the

bills currently in Congress, and welcome optical scan, precinct-based, balloted voting with risk limiting audits, as many experts have endorsed.

We completely understand that today's environment presents risks to our democracy that are unprecedented. All informed observers and participants in protecting America agree that our nation's critical infrastructure is under attack by nation-states, cybercriminals, and professional and amateur hackers. That's why forums open to anonymous hackers must be viewed with caution, as they may be a green light for foreign intelligence operatives who attend for purposes of corporate and international espionage. We believe that exposing technology in these kinds of environments makes hacking elections easier, not harder, and we suspect that our adversaries are paying very close attention. We strongly urge you to, in your capacity as members of the Select Committee, reach out to your contacts in the Intelligence Committee and make your own assessment regarding the presence of foreign adversaries in these anonymous forums. We note that most defense firms and other critical infrastructure suppliers also do not display national security technology in unsecured environments. This prudent approach doesn't mean there is a lack of cybersecurity testing—to the contrary. Security is at the forefront of everything we do.

We agree that it is only through preparation, constant vigilance, secure technology, post-election audits, and strong, continuing partnerships between state and local election officials, the EAC, DHS, law enforcement and voting system manufacturers that we will keep the elections infrastructure secure, and ES&S is at the forefront of that preparation, vigilance, expertise, and coordination.

Thank you for the opportunity to share our approach. We invite each of you, as well as your security experts, to a discussion to learn more about all of the protective, proactive steps our customers and we have taken and continue to take to ensure the integrity of America's democracy.

Yours truly,

Tom Burt, President & CEO, Election Systems & Software

cc: Ms. Kathy Rogers (kathy.rogers@essvote.com)
Mr. Zach Lewis (zach_lewis@warner.senate.gov)
Ms. Darci Greenacre (scheduling@collins.senate.gov)
Ms. Sarah Seitz (sarah_seitz@lankford.senate.gov)
Senator Kamala D. Harris (kamala_harrissac@harris.senate.gov)