PUBLICCITIZEN

To: Tom Burt, President & Chris Wlaschin, Vice President, Systems Security
Election Systems & Software (ES&S)

CC: Secretaries of State, State Election Officials & Local Election Official Associations

From: Public Citizen

Re: Modems in vote tabulating machines

Dear Mr. Burt and Mr. Wlaschin,

We call on you to stop the marketing and sale of cellular modems with the DS200 paper ballot scanner, central tabulators and any other vote tabulating systems you sell.

We call on you to disclose to election officials and the public that vote tabulating systems with modems are not U.S. Election Assistance Commission certified.

Further, we call on you to quickly comply with all election official requests to remove modems and any source code in the election management system that would permit external communication beyond the pre-election programming of the machines.

Following the 2016 election, when foreign actors took a documented interest in U.S. election systems, it is unconscionable that the largest voting machine vendor in the nation is pushing election officials in 2018 to buy machines that connect to the internet. No matter how brief the connection, the convenience of having vote totals communicated online does not outweigh the need of the American people to be assured their votes will be accurately counted.

Congress has designated funding for the purchase of voting systems that rely on a paper record in an effort make systems more secure. By marketing modems as part of one of your most popular paper ballot vote counting systems, ES&S is pushing for the use of taxpayer funds on systems that are less secure and more expensive than those without modems.

To the extent modems are offered it all, it should be clear in all marketing materials and communications that modems are an optional add-on to the DS200 at a distinct and significant additional cost, and that systems with modems lack federal certification.

Finally, in light of recent coverage regarding remote access software installed on voting systems, Public Citizen calls on ES&S to remove remote access software from every ES&S voting system still in use. If removing the software is not possible, the

company should compensate election officials who may need to purchase new machines without this security vulnerability.

Sincerely,

Aquene Freechild
Public Citizen's Democracy Is For People Campaign
1600 20th St. NW
Washington, DC 20009
afreechild@citizen.org
202-588-7752