United States Senate
WASHINGTON, DC 20510

March 26, 2019

Mr. Phillip Braithwaite
President and Chief Executive Officer
Hart InterCivic, Inc.
15500 Wells Port Dr.
Austin, TX 78728

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

Mr. John Poulos
President and Chief Executive Officer
Dominion Voting Systems
215 Spadina Ave., Suite 200
Toronto, ON M5T 2C7

Dear Mr. Braithwaite, Mr. Burt, and Mr. Poulos:

We write to request information about the security of the voting systems your companies manufacture and service.

The integrity of our elections remains under serious threat. Our nation's intelligence agencies continue to raise the alarm that foreign adversaries are actively trying to undermine our system of democracy, and will target the 2020 elections as they did the 2016 and 2018 elections.[1] Following the attack on our election systems in 2016, the Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure[2] in order to protect our democracy from future attacks and we have taken important steps to prioritize election security. We appreciate the work that your companies have done in helping to set up the Sector Coordinating Council (SCC) for the Election Infrastructure Subsector.

Despite the progress that has been made, election security experts and federal and state government officials continue to warn that more must be done to fortify our election systems.

---

[1] Dan Coats, "DNI Coats Opening Statement on the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community", January 29, 2019. https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf

[2] "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector", Department of Homeland Security, January 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

Of particular concern is the fact that many of the machines that Americans use to vote have not been meaningfully updated in nearly two decades. Although each of your companies has a combination of older legacy machines and newer systems, vulnerabilities in each present a problem for the security of our democracy and they must be addressed.

On February 15, the Election Assistance Commission's (EAC) Commissioners unanimously voted to publish the proposed Voluntary Voting System Guidelines 2.0 (VVSG) Principles and Guidelines in the Federal Register for a 90 day public comment period.[3] As you know, this begins the long-awaited process of updating the Principles and Guidelines that inform testing and certification associated with functionality, accessibility, accuracy, auditability, and security.[4] The VVSG have not been comprehensively updated since 2005 – before the iPhone was invented – and unfortunately, experts predict that updated guidelines will not be completed in time to have an impact on the 2020 elections. While the timeline for completing VVSG 2.0 is frustrating, these guidelines are voluntary and they establish a baseline – not a ceiling – for voting equipment. Furthermore, VVSG 1.1 has been available for testing since 2015.

In other words, the fact that VVSG 2.0 remains a work in progress is not an excuse for the fact that our voting equipment has not kept pace both with technological innovation and mounting cyber threats.[5] There is a consensus among cybersecurity experts regarding the fact that voter-verifiable paper ballots and the ability to conduct a reliable audit are basic necessities for a reliable voting system. Despite this, each of your companies continues to produce some machines without paper ballots. The fact that you continue to manufacture and sell outdated products is a sign that the marketplace for election equipment is broken. These issues combined with the technical vulnerabilities facing our election machines explain why the Department of Defense's Defense Advanced Research Projects Agency (DARPA) is reportedly working to develop an open source voting machine that would be secure and allow people to ensure their votes were tallied correctly.

As the three largest election equipment vendors, your companies provide voting machines and software used by 92 percent of the eligible voting population in the U.S.[6] This market concentration is one factor among many that could be contributing to the lack of innovation in election equipment. The integrity of our elections is directly tied to the machines we vote on – the products that you make. Despite shouldering such a massive responsibility, there has been a lack of meaningful innovation in the election vendor industry and our democracy is paying the price.

---

[3] "EAC Commissioners Unanimously Vote to Publish VVSG 2.0 Principles and Guidelines for Public Comment ", February 15, 2019. https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/

[4] https://www.eac.gov/news/2017/09/12/committee-approves-next-generation-of-voting-system-guidelines/

[5] "Voting Machine Vendors Under Pressure," Politico, July 12, 2018, https://www.politico.com/newsletters/morning-cybersecurity/2018/07/12/voting-machine-vendors-under-pressure-277054

[6] "The Business of Voting." University of Pennsylvania Public Policy Initiative. https://trustthevote.org/wp-content/uploads/2017/03/2017-whartonoset_industryreport.pdf

In order to help improve our understanding of your businesses and the integrity of our election systems, we respectfully request answers to the following questions by April 9, 2019:

1. What specific steps are you taking to strengthen election security ahead of 2020? How can Congress and the federal government support these actions?

2. What additional information is necessary regarding VVSG 2.0 in order for your companies to begin developing systems that comply with the new guidelines?

3. Do you anticipate producing systems that will be tested for compliance with VVSG 1.1? Why or why not?

4. What steps, if any, are you taking to enhance the security of your oldest legacy systems in the field, many of which have not been meaningfully updated (if at all) in over a decade?

5. How do EAC certification requirements and the certification process affect your ability to create new election systems and to regularly update your election systems?

6. Do you support federal efforts to require the use of hand-marked paper ballots for most voters in federal elections? Why or why not?

7. How are you working to ensure that your voting systems are compatible with the EAC's ballot design guidelines (i.e. "*Effective Designs for the Administration of Federal Elections*")?

8. Experts have raised significant concerns about the risks of ballot marking machines that store voter choice information in non-transparent forms that cannot be reviewed by voters (i.e. such as barcodes or QR codes), noting that errors in the printed vote record could potentially evade detection by voters. Do you currently sell any machines whose paper records do not permit voters to review the same information that the voting system uses for tabulation? If so, do you believe this practice is secure enough to be used in the 2020 election cycle?

9. Do you make voting systems with Cast Vote Records (CVRs) that can be reliably connected to specific unique ballots, while also maintaining voter privacy? If not, why not? Does your company make voting systems that allow for a machine-readable data export of these CVRs in a format that is presentation-agnostic (such as JSON) and can be reliably parsed without substantial technical effort? If not, why not?

10. Would you support federal legislation requiring expanded use of routine post-election audits, such as risk-limiting audits, in federal elections? Why or why not?

11. What portion of your revenue is invested into research and development to produce better and more cost effective voting equipment?

12. Congress is currently working on legislation to establish information sharing procedures for vendors regarding security threats. How does your company currently define a reportable cyber-incident and what protocols are in place to report incidents to government officials?

13. What steps are you taking to improve supply chain security? To the extent your machines operate using custom, non-commodity hardware, what measures are you taking to ensure that the supply chains for your custom hardware components are monitored and secure?

14. Do you employ a full-time cybersecurity expert whose role is fully dedicated to improving the security of your systems? If so, how long have they been on staff, and what title and authority do they have within your company? Do you conduct background checks on potential employees who would be involved in building and servicing election systems?

15. Does your company operate, or plan to operate, a vulnerability disclosure program that authorizes good-faith security research and testing of your systems, and provides a clear reporting mechanism when vulnerabilities are discovered? If not, what makes it difficult for your company to do so, and how can Congress and the federal government help make it less difficult?

16. How will DARPA's work impact how your company develops and manufactures voting machines?

We look forward to your answers to these questions, and thank you for your efforts to work with us and with state election officials around the country to improve the security of our nation's elections.

Sincerely,

Amy Klobuchar
United States Senator

Gary C. Peters
United States Senator

Jack Reed
United States Senator

Mark R. Warner
United States Senator