ELECTION
Systems & Software

Election Systems & Software
11208 John Galt Blvd · Omaha, NE 68137
P: 402.970.1100 · TF: 877.377.8683
teburt@essvote.com · www.essvote.com

April 9, 2019

<u>By Email & Hand Delivery</u>

The Honorable Amy Klobuchar
425 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Gary C. Peters
724 Hart Senate Office Building
Washington, DC 20510

The Honorable Jack Reed
728 Hart Senate Office Building
Washington, DC 20510

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

Dear Senators Klobuchar, Peters, Reed, and Warner:

Thank you for your letter of March 26, 2019, and for the opportunity to discuss how Election Systems & Software (ES&S) is working with many stakeholders, including the U.S. government, to secure and ensure faith in our system of democracy.

Please find below the answers to your questions.

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

We appreciate the question regarding the role of ES&S, Congress, and the federal government in supporting and strengthening the integrity of elections. At the outset, we want to be clear that *ES&S fully supports the use of paper ballots and post-election audits as a way to ensure accuracy and increase confidence in our country's election process.*

In regard to ES&S' work to strengthen election security ahead of 2020:

1. Testing: As standard procedure, our internal security team conducts thorough and pervasive penetration testing of our hardware and software using the same modern security tools that hackers might use to make sure our equipment is secure before it ever reaches the customer. After the 2016 election, to complement our own testing, we submitted our current hardware to third-party security research firms to independently verify the security of our devices. In addition, ES&S recently submitted its full end-to-end voting configuration of software and hardware for testing by the Idaho National Laboratory (INL), the nation's leading center for research and development in energy, national security, science and environment, to perform third-party independent testing of both our hardware and software to ensure the resilience and security of our voting systems.

2. Coordination: In strategic partnerships, ES&S met with the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) leadership frequently over the past year, and we signed up for DHS weekly cyber-hygiene scans of our external web presence. ES&S has joined both the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and the Information Technology Information Sharing and Analysis Center (IT-ISAC) to take advantage of the significant cyber threat sharing channels these groups support, and we have requested and installed Albert sensors in our hosted voter registration environments in order to detect and thwart any potential indicators of compromise. Albert is a unique network security monitoring solution that provides continuous remote monitoring and delivery of automated alerts on both traditional and advanced network threats for state and local jurisdictions, allowing election jurisdictions and ES&S to respond quickly when data may be at risk. Combined with an in-depth review conducted by expert analysts through the Center for Internet Security's (CIS) 24/7 Security Operations Center, Albert is a fully monitored and managed service which complements ES&S' existing, robust suite of cybersecurity controls.
3. Education: ES&S has conducted numerous election security training sessions, presentations, and discussions for state and local election officials who use our equipment to continue to educate and inform them of best practices for securing election equipment and processes.
4. Additional security: ES&S has implemented additional security controls protecting our corporate network environment, including independent vulnerability assessments and DMARC email security to further strengthen our corporate network from cyber threats. All ES&S personnel (employees, contractors, temps, and interns) are required to carry a security badge that limits access to only the areas required to perform their specific job function. All building entrances, elevators, and sensitive internal areas of ES&S facilities are covered by electronic door badge access and security cameras. Our physical security posture has been reviewed by the local office of the DHS Critical Infrastructure Physical Security Specialist for this area of the nation. ES&S conducts on-site reviews of our vendor partners' physical and information security programs to ensure they are also following industry best practices to secure their facilities and environments.

Regarding Congressional support, we support Congress adopting legislation to establish a program mandating that all voting machine suppliers submit their systems to stronger, programmatic security testing conducted by vetted and approved researchers. We also believe Congress should mandate physical paper records of votes to enable an effective, meaningful audit of each voter's selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid post-election audits. As noted above, *ES&S fully supports the use of paper ballots and post-election audits as a way to ensure accuracy and increase confidence in our country's election process.*

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?*

ES&S looks forward to the approval of the VVSG 2.0, so that we can work to ensure our solutions meet or exceed these guidelines. ES&S has been an active participant in the working groups focused on developing these guidelines. We are eager to see the underlying test requirements and associated test assertions that will accompany these guidelines as it is these test requirements and assertions that will provide the specific information needed to fully guide our efforts to comply with VVSG 2.0. As an example, VVSG 2.0 guideline 9.4 states that “The voting system shall support efficient audits.” ES&S systems currently support audits, and we are actively enhancing these systems to enable even more robust audit support. We are keen to understand the test requirements, assertions, and details related to “efficient audits” so we can ensure our solutions comply with these new standards. We will continue to be active participants in the VVSG 2.0 working groups and look forward to the availability of the test requirements and assertions that will guide our systems development efforts.

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

The jurisdictions we serve have been requesting systems focused on security improvements and robust support for election audits that are above and beyond the VVSG 1.1. These requests, combined with our recognition that the elections ecosystem must stay ahead of security threats, have resulted in stronger security and auditing advancements. Consequently, ES&S has shifted its focus to compliance with the newer VVSG 2.0 to allow ES&S systems to advance to the higher standards of increased security and auditing.

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?*

ES&S is continually developing new products and conducting research to further security. In fact, the equipment ES&S sells today contains some of the most secure voting technology available.

ES&S takes an active approach to do everything we can with customers who operate legacy systems to help ensure that such systems are as secure as possible, offering regular hardware maintenance and federally-certified software and firmware updates as allowed.

To help deliver accurate election results and maintain the security of legacy systems, we provide support and guidance to election authorities on best practices in conducting pre-election logic and accuracy (L&A) testing, election day operations and post-election audits. We work closely with local jurisdictions to implement physical security controls and proper chain-of-custody procedures for all aspects of the election management and voting systems.

ES&S has conducted “Secure the Vote” seminars around the country to help election administrators ensure their elections are secure, regardless of which systems they are operating. The seminars cover not only the security of the election systems, but also aim to educate election administrators about general best practices in cybersecurity.

Recognizing the challenges that come with a rapidly advancing technology environment, ES&S has worked to architect its current, purpose-built systems to sustain a long useful life, beyond what is expected with typical consumer electronics. As a result, some of our current products have been fielded for well over a decade, yet continue to receive regular security updates and feature enhancements.

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?*

The certification process under the EAC Testing and Certification Program varies depending upon the scope and magnitude of the changes to the voting system. A new voting system could potentially take 18 months or more to get through full testing and certification. Modifications to previously certified voting systems generally require 5-7 months, again depending on the scope of changes. Very minor modifications such as a small software revision or a minor hardware modification can potentially complete the EAC process in approximately six weeks.

While the current certification process has served the nation well for over a decade, it is currently in need of modernization. Specifically, the process needs to be streamlined, while maintaining rigor, to better allow for modifications (especially as it relates to COTS) to more quickly address vulnerabilities that may be identified. This is an area where Congress can help.

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?*

ES&S fully supports the use of paper ballots for all elections.

ES&S provides both hand-marked and machine-marked (ballot marking device) paper-based tabulation systems. Jurisdictions decide which system and configuration best fit their needs. All paper-based voting machines currently sold by ES&S allow the voter to review and verify their ballot information in the form of human-readable text that is presented to them on a piece of paper.

Using only hand-marked paper ballots is a concern for the disability community as it would separate and segregate certain voters, prohibiting them from participating in a fully universal voting experience. Fully ADA-compliant, ballot marking devices offer the same experience for all voters, regardless of ability, while also utilizing a variety of functions to ensure election data and cast vote records are secure. Ballot marking devices allow voters to review their selections and verify that their vote selections were recorded accurately before submitting for tabulation. Ballot marking devices also eliminate the need for human interpretation of voters' intent when ballots contain marginal or ambiguous marks. To be clear, election systems that process hand-marked paper ballots and election systems that process machine-marked paper ballots are both very secure. We actively sell and support both types of systems, and we do not believe that the federal government should mandate one of those systems over the other. That choice should be left to individual jurisdictions.

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")?*

ES&S has fully embraced the EAC's ballot design guidelines and uses these as standards within its products. ES&S was intimately involved in the project that led to the development of the best practices prescribed in "Effective Designs for the Administration of Federal Elections." ES&S took part in early pilots, implementing and testing the ballot-design best practices in three counties. This opportunity allowed ES&S to understand the best practices better and adapt our products to enable usage of them. While the final layout and design of ballots is ultimately decided by our customers, we continue to conduct usability testing and consult with design experts to ensure our products are both highly usable and accessible.

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?*

Both hand-marked paper ballots and machine-marked paper ballots are highly secure methods of casting a vote. Post-election audits can fortify the security of the election under either voting scenario.

There are several important facts about how tabulators count hand-marked paper ballots and machine-marked paper ballots.

Barcodes exist on both hand-marked paper ballots and machine-marked paper ballots and those barcodes are used in the very same manner in both scenarios to count votes. Here is how tabulation devices read hand-marked paper ballots:

- On a hand-marked paper ballot there is a master barcode along the left edge of the ballot and the top and/or bottom of the ballot.
- When a voter hand marks the oval next to candidate Jane Doe, for example, and inserts that hand-marked paper ballot into a tabulation machine, that tabulation machine is not reading the name Jane Doe. In fact, the tabulation machine does not recognize the text, Jane Doe, at all. Rather, the tabulation machine first recognizes, through digital imaging technology, that an oval has been filled in. Then it uses the master barcode on the ballot to determine the grid coordinates of that filled-in oval.
- In this example, if the grid coordinates of the filled-in oval are “six down, four across,” the tabulation machine then queries the database that resides on the master media (typically a USB stick) that has been inserted into the tabulator. In essence, the tabulation machine asks the database on the master media, “what candidate’s name is associated with six down, four across?” The database, which has been pre-programmed and tested by the county/city election office, then tells the tabulation machine that “six down, four across” corresponds with Jane Doe. At that point, the tabulation machine creates a cast vote record that records a vote for the name Jane Doe.

Jurisdictions perform pre-election logic and accuracy tests and post-election audits to ensure the accuracy of the aforementioned process. During both the pre-election tests and the post-election audits, jurisdictions are asking whether the actual text next to the filled in oval on the hand-marked paper ballot corresponds exactly to the vote that was registered by the tabulation machine. This verification can only be done if the jurisdiction has access to the paper ballot *and* the cast vote record from the tabulation machine. As noted above, pre-election testing and post-election auditing provide a testable and auditable method to verify that ballots are programmed and counted as intended.

Machine-marked paper ballots behave in the exact same way, only the voter marks their ballot with a machine instead of a pen. Here's how:

- When the voter chooses Jane Doe on the touch screen, the marking device prints out a paper record that shows the text Jane Doe along with a barcode that contains the ballot coordinates of "six down, four across." When that paper record is inserted into the tabulator, it performs the same routine as it does with the hand-marked paper ballot. It reads the barcode, which reveals the grid coordinates of "six down, four across" and then it queries the database on the tabulation machine (which is the same tabulation machine that counts the hand-marked paper ballot) asking which candidate name is associated with those grid coordinates. The database then reveals to the tabulation machine that "six down, four across" corresponds to Jane Doe. At that point, the tabulation machine creates a cast vote record for Jane Doe.

Just as is the case with hand-marked paper ballots, the tabulation machine is only looking for the grid coordinates, and the cast vote records from both examples are identical.

Even tabulation systems that utilize Optical Character Recognition (OCR) incorporate the use of a barcode to count the vote. Here's why: It is possible that there could be two separate and distinct candidates, both named Jane Doe, who are running for different offices on the same ballot. The system cannot use OCR to read "Jane Doe" and record a vote reliably because it would have to know for what race the vote for "Jane Doe" should be counted. Thus, the barcode is used to tell the tabulation machine for what race Jane Doe should receive a vote.

In sum, all tabulation machines that count paper ballots use a barcode to determine how to properly and accurately count the vote. The security of each method of voting is confirmed by election officials during pre-election tests and in post-election audits.

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?*

ES&S high-speed central scanners can imprint a ballot identification number on a ballot. This ballot identification number allows the paper ballot to be directly tied to a cast vote record while maintaining strict voter privacy. This capability is currently being added to our precinct scanner.

ES&S solutions do provide a cast vote record export in a flexible format. The imprinted ballots and the cast vote record exports have been used in multiple jurisdictions, most recently in the State of Rhode Island, to successfully complete post-election risk-limiting audits.

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?*

Yes, ES&S strongly supports legislation that would expand the use of routine post-election audits.

ES&S believes that successful post-election audits, including risk-limiting audits such as those which have recently occurred in several jurisdictions, will increase confidence in our country's election process.

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

Over the last four years, our research and development expenses have averaged approximately 19 percent of our revenue.

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?*

ES&S follows the 2018 Department of Homeland Security publication, "Incident Handling Overview for Election Officials," which instructs election entities how to inform DHS about cyber-related incidents. Also, ES&S has a mature, tested incident-response policy and process whereby potential cyber incidents are triaged by our internal team of subject matter experts. Where circumstances indicate the reporting of the incident to government officials, we follow DHS guidelines for alerting the National Cybersecurity and Communications Integration Center (NCCIC), Multi-State Information Sharing and Analysis Center (MS-ISAC), and EI-ISAC.

ES&S hosted a tabletop exercise at our headquarters just prior to the November 2018 General Election that was facilitated by the DHS National Cyber Exercise and Planning Program (NCEPP) team from the NCCIC. During this exercise, we reviewed and practiced our established protocols for analyzing and reporting incidents to the proper 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?*

Our purpose-built tabulation machines, which are produced in ISO-9001 manufacturing facilities, are made of many commercially available components configured to a custom design for a specific use. The entire voting system is managed by a secure engineering change order control process. This includes all component suppliers. Changes to the voting system follow a formal closed-loop process and must be internally and externally reviewed, verified, tested and approved before they can be incorporated into the voting system. Every unit is individually serialized for complete traceability.

ES&S also conducts thorough security reviews of our supply chain including supply-chain risk assessments and on-site visits to our suppliers to ensure that every component is trusted, tested and free of malware. All tabulation software is developed and compiled exclusively in the USA. All components of the hardware go through a formal incoming inspection and testing process. Final hardware configuration control and quality assurance are performed at our headquarters in Omaha, Nebraska.

As standard practice, each hardware and software release undergoes thousands of hours of performance testing and runs millions of test ballots along with extensive security testing after which ES&S provides a complete set of software components to the voting systems testing labs (VSTL) for review.

In addition, ES&S is participating in discussions with the Department of Homeland Security's National Risk Management Center (NRMC), the National Institute of Technology (NIST) and the Center for Internet Security (CIS) regarding the development of guidelines and best practices to ensure that we continue to manage new or emerging risks associated with supply chain components.

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?*

Yes, Mr. Chris Wlaschin is ES&S' Vice President of Systems Security and Chief Information Security Officer. Mr. Wlaschin reports directly to me. He has worked for ES&S for a year, and he has the authority to drive security improvements across hardware, software, and corporate operational and infrastructure security. Mr. Wlaschin is also the Chair of the Elections Infrastructure Subsector Coordinating Council (EI-SCC), a DHS sponsored organization to drive security improvements across the elections industry. Prior to joining ES&S, Mr. Wlaschin was the Chief Information Security Officer for the Department of Health and Human Services in Washington D.C., where he oversaw cybersecurity efforts for the Department. He has held other senior cybersecurity leadership positions in both the public and private sector including the Department of Defense, Department of Veterans Affairs, National Research Corporation, and the University of Nebraska.

ES&S conducts thorough background checks on all employees and we contractually require our vendor partners to do the same. Every employee at ES&S is expected to be accountable for security and all receive annual security training; it's an essential part of everyone's job.

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?*

ES&S is actively working with good-faith ethical researchers to test our systems. We also provide a security message and email address on our public website that states "If you have a comment about election security or would like to report an issue, potential vulnerability or bug to us, please contact us by using the following email address: security@essvote.com. Your comments will be kept confidential, and a member of our security team will follow up with you."

ES&S utilizes its internal corporate information security staff to receive, evaluate and act upon, as necessary, unsolicited vulnerability reports from cybersecurity researchers and other third parties. These unsolicited reports may be received by phone, verbal, mail or media reports.

Congress and the federal government can help the election sector by proposing legislation to create and support an Independent Coordinated Vulnerability Testing and Disclosure Process to improve election system security across all election vendors. This cybersecurity testing program would mandate that all voting machine vendors submit their systems to a programmatic cyber testing program conducted by vetted and approved researchers. Although voting machines are not connected to the internet, there are non-internet related types of cybersecurity testing that are necessary to protect elections. Machine penetration tests simulate attacks on election equipment by people who gain physical access to the voting machines or the components.

Congress could also pass legislation that requires a paper record for every voter. It is difficult to perform a meaningful audit without a paper record of each voter's selections. Mandating the use of a physical paper record sets the stage for all jurisdictions to perform statistically valid post-election audits.

ES&S believes if Congress can establish these standards, the general public's faith in the process of casting a ballot can be restored.

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

We are very interested in learning more about the DARPA effort and how we can potentially leverage the work that emerges from the DARPA effort into ES&S products to improve election security. We have established contact with individuals involved and are seeking to find ways to participate, learn, and contribute.

We know that improving the confidence of every voter requires a tight collaboration between federal, state and local election officials, the EAC, DHS, law enforcement, voting system manufacturers, and the election community at large. As an American company and the nation's leading election provider, ES&S is committed to delivering high security products and services to ensure the integrity of our nation's elections.

Thank you for allowing ES&S to share our approach and all of the proactive steps we and our customers have taken and continue to take to secure the cornerstone of our democracy.

Yours truly,

Tom Burt

Tom Burt, President & CEO
Election Systems & Software