Written Testimony of Mr. John Poulos, CEO

Dominion Voting Systems

before the Committee on House Administration

"2020 Election Security-Perspectives from Voting System Vendors and Experts"

January 9, 2020

Chair Lofgren, Ranking Member Davis, and Distinguished Members of the Committee, thank you for the opportunity to testify today.

My name is John Poulos, and I am the Chief Executive Officer and co-founder of Dominion Voting Systems. As a U.S.-owned company, we currently provide voting systems and services to jurisdictions across 30 states and Puerto Rico.

I co-founded the company in 2003 on three basic pillars: security, accessibility and transparency. We continue to be committed to these founding principles and delivering best-in-class solutions for secure, transparent, and accessible elections. The voting systems that we produce provide high assurance that election outcomes are accurately and reliably tallied. All Dominion systems fully-support independent, third-party audits, and reviews of election data.

Together with my industry counterparts, I am here today to help explain how we are working to keep voting systems secure and resilient in the wake of today's sophisticated, nation-state threats. I would like to focus on our core company values and how they impact our product innovations and the work that we do in collaboration with our federal, state, and local government partners.

Consistent with our founding tenants, Dominion works hard to promote a company culture of security. This includes annual, mandatory background checks and cybersecurity awareness training for all employees. Dominion is committed to investing in security and innovation efforts, tracking risk and threat information, developing new capabilities and successfully supporting our customers.

Dominion has also adopted advanced digital protections while employing a Defense-in-Depth approach to our internal infrastructure. Multiple layers of protection are in place spanning user endpoints, network and systems infrastructure and cloud systems, along with multi-factor

authentication. We conduct continuous vulnerability scanning on our company network and utilize third-party services for threat hunting and breach detection. Specifically, we have implemented email verification records for Sender Policy Framework ("SPF"), DomainKeys Identified Mail ("DKIM"), and Domain-based Message Authentication ("DMARC") to protect communications with associates and customers.

We actively engage with the U.S. Department of Homeland Security ("DHS") and other trusted, third-party advisors to enhance and maintain our physical and cyber security posture. Together with federal, state and local government partners – as well as our industry counterparts, we conduct coordinated emergency drills, tabletop exercises and routine information-sharing as a member of the DHS Sector Coordinating Council for Election Infrastructure. Through these efforts, Dominion has refined our company's situational awareness and strengthened our procedures for handling incidents and emergencies.[1] We have also conducted security briefings and training sessions with state and local election officials who use our systems to educate and inform them of best practices for securing their voting equipment and chain of custody process. In these ways, we have made great strides to support and enhance the nation's collective readiness posture for the 2020 presidential election.

Dominion also works closely with jurisdictions seeking to upgrade or replace older, end-of-life systems with federally-certified solutions capable of producing paper records for auditing and resilience. These offerings have rigorous security features, and we provide hardware maintenance service and certified software/firmware updates on a routine basis.

In keeping with company security practices, all of our products are submitted to the U.S. Election Assistance Commission ("EAC") and state election authorities for further review, testing and certification. Systems are tested using an independent, federally-accredited Voting Systems Test Laboratory ("VSTL") in order to meet certification standards promulgated by the EAC, in conjunction with experts at NIST. They must also meet specific requirements set forth by individual states, including source code reviews, penetration testing, and post-election auditing.[2] These certified software packages and systems are the only versions allowed by law.

We are constantly innovating and certifying enhancements and new features, per federal, state and local election requirements. Our product advancements reflect the values of our state and local customers, with a focus on providing secure, reliable, quality systems that offer cutting-

[1] See U.S. Dept. of Homeland Security, "Incident Handling for Election Officials," 2018.
[2] Help America Vote Act of 2002 (HAVA). https://www.eac.gov/assets/1/6/HAVA41.PDF

edge features, including encryption, multi-factor authentication and trusted-user protections, as well as a robust auditing module for election officials who want to share post-election ballot images and other data with the public.

Dominion is actively engaged with the EAC and other stakeholders in the ongoing work to finalize VVSG 2.0 guidelines for 2020 and beyond. Our development strategy has shifted towards the latest iteration of these standards to ensure that our voting systems advance to the next generation of security and resilience. In 2018, Dominion equipment was used in the State of Colorado's risk-limiting audit ("RLA"), the first of this kind ever conducted in the U.S. Today, other states are conducting RLAs to ensure that election tallies are accurate and reliable.

Voting systems must also ensure federal protections for privacy, equal voting rights and ballot-casting options for all - including disabled voters, U.S. military and overseas voters, and those with literacy or language challenges who require some form of assistance in casting their ballot.[3]

Additionally, we are working with other industry companies to establish a Coordinated Vulnerability Disclosure ("CVD") program designed to strengthen the security and resilience of voting systems. This work expands upon existing federal and state processes for certification, testing and reporting on risks and vulnerabilities regarding election infrastructure. Government partners at all levels can help by supporting and incentivizing rapid modernization of the framework that is used for the certification and testing of election equipment.

Right now, the complex pathway from lab to market impacts the pace at which new or updated solutions can be introduced. While much of the current effort around VVSG has understandably focused on establishing thorough and comprehensive testing criteria for voting systems, there must also be clear mechanisms for streamlined updates and security-focused patching. We are hopeful that VVSG 2.0 will provide a more effective process for introducing innovations and maintenance of deployed systems.

Dominion makes extensive disclosures to maintain our good standing as a registered federal and state voting systems manufacturer. Like other providers, we submit a detailed "bill of materials" to the EAC as part of required submissions for federally-certified systems, which includes all component manufacturer and sourcing information for hardware. In addition to mandatory state and local disclosures for confirmed or suspected breaches and incidents, we also adhere to the

[3] See Americans with Disabilities Act, UOCAVA, Help America Vote Act (HAVA) and MOVE Act for specifics.

EAC's mandatory requirement for reporting system issues in federal elections.[4]

Federal and state-level product testing and certification applications require voluminous amounts of manufacturer information, including but not limited to:

- Ownership information, business structure and credit rating
- Notifications to all U.S. customers of any business change of ownership
- Personnel oversight policies, including background checks
- Third-party vendor and manufacturing location information
- Proprietary software disclosures, third-party test reports, and documentation to verify reliable use of the system in other jurisdictions

Dominion has always maintained full federal and state compliance under law. Given the high headline risk and the public visibility of the support that Dominion provides to state and local governments, it would be difficult to thrive as a business without maintaining the highest standards as an elections industry provider. Notably, voting systems manufacturers remain the only technology providers in the election ecosystem subject to company disclosures and federal certification testing. Only a handful of states currently extend their requirements beyond voting systems to other types of technology.

In conclusion, Dominion Voting Systems is committed to ensuring that Americans are confident in the security and resilience of the nation's voting systems. We commend Congress for its most recent bipartisan efforts to increase federal investment in state and local government election security initiatives for 2020 by $425 million. We urge you to continuing work with election officials to help remove additional barriers that exist for modernizing their infrastructure.

We also seek continued assistance from our federal partners in evaluating cyber risks for voting technology, to include increased transparency around malign activity observed by intelligence agencies. This would go a long way towards enabling private sector election providers to better prioritize resource allocations in the same economic terms as other enterprise decisions.

Dominion continues to focus on being the best-in-class elections provider with a commitment to security, transparency, and accessibility. Thank you again for the opportunity to share the company's perspective on these very important issues.

[4] See "EAC Testing & Certification Program Manual Version 2.0," www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf