DOMINION VOTING

1201 18TH Street, Suite 210
DENVER, CO, 80202
1.866.654.8683
www.dominionvoting.com

October 27, 2017

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Bldg.
Washington, DC 201510

Dear Senator Wyden:

Thank you for reaching out to Dominion Voting. We are completely committed to your goal of ensuring that Americans are confident in the security and reliability of our nation's voting systems. As a member of the U.S. Senate Select Committee on Intelligence, you have undoubtedly heard the unanimous conclusion of our national intelligence agencies that foreign meddling in the 2016 election cycle did not involve any tampering with voting machines or changes in vote tallies, and that any attempts at "cyber manipulation of the U.S. election system designed to change the outcome of the U.S. election would be detected."[1] As we embark upon new efforts to keep U.S. election infrastructure protected as a matter of national security, our systems must remain secure from sophisticated attacks.

Per your question regarding company-focused cybersecurity incidents, Dominion Voting Systems is not aware of any incidents in which an attacker has gained unauthorized access to our internal systems, corporate data or customer data. Additionally, we have not received any information from the U.S. Department of Homeland Security (DHS) or the Federal Bureau of Investigation (FBI) pertaining to any successful cyber intrusions of our systems. If such an incident were to occur, company practices would prioritize notification of our government customers and law enforcement, as appropriate.

Dominion Voting recognizes that maintaining our company security posture – as well as our longstanding record of providing safe, reliable and transparent voting systems – requires constant vigilance and engagement. Our company is using in-house experts, third party private security providers and government partners at all levels to meet existing cybersecurity threats, and to bolster our companywide commitment to risk awareness and sound cyber hygiene practices.

Together with the jurisdictions that we serve, Dominion Voting regularly works with independent, third-party firms to review the security of our company's IT infrastructure. While we have many employees who play a role in company security, our Director of IT, EVP of Engineering and others currently lead our cybersecurity and risk mitigation efforts. In addition to the strict federal and state-level certification processes to which our systems are subjected, we conduct internal and external cybersecurity reviews and risk mitigations, including during the run-up to the 2016 election cycle, and we plan to continue these efforts throughout coming election cycles. We also actively work together with our Election Administrators in discussing concepts for new ways to conduct penetration testing and audits of both our systems and our products in order to build upon past efforts.

For the 2018 cycle and beyond, we are proactively working to enhance our information security program standards, policies and controls by utilizing the National Institute of Standards and Technology (NIST)

[1] (U) National Intelligence Council, ICA 2017-01, 5 January 2017, (U) Assessing Russian Activities and Intentions in Recent U.S. Elections. See also testimony of U.S. Homeland Security Infrastructure & Analysis Cyber Division Acting Director Dr. Samuel Liles before the U.S. Senate Select Committee on Intelligence, 21 June 2017.

Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework"). The EAC began promoting the voluntary application of this Framework to elections in February/March 2017, following the DHS critical infrastructure designation for election infrastructure. We are also reviewing the new NICE Framework (NIST Specialty Publication 800-101) and its corresponding Cybersecurity Workforce Development Toolkit as supporting resources for meeting our cybersecurity personnel goals and building upon the comprehensive operational and incident response plan that we developed for the 2016 cycle.

Given the evolving nature of election threats during each cycle, we are actively working with the Election Administrators who currently deploy our systems to enhance protocols for protecting security sensitive critical infrastructure information (CII) and assets from persistent threat actors. The first planned meeting between election industry representatives and DHS is tentatively scheduled for December 2017, and we are hopeful that this working group will be highly effective in furthering the ability of our Election Administrators in keeping our elections safe, transparent and accurate.

Regarding your questions about unsolicited vulnerability reports, access to voting machines in the U.S. is strictly limited and controlled by the Election Administrators who are entrusted with conducting elections, with violations subject to criminal prosecution under law. States govern this process and establish their policies for controlled access. We recommend that you consult with election officials for a thorough understanding of existing state and local processes for limiting unsolicited access to voting systems, and why such security protections exist. The National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED) can be helpful in this regard.

Additionally, since the U.S. Election Assistance Commission (EAC) and state governments play a significant oversight role in the testing and certification of voting systems, we recommend that you speak with these entities to understand how such processes work to identify vulnerabilities and address technical issues before voting systems can be used. Under the Help America Vote Act of 2002, the EAC is tasked with working with NIST to develop Voluntary Voting Systems Guidelines (VVSG) for voting systems. Dominion Voting continues to be an active participant in EAC working groups supporting the VVSG 2.0 effort to build on security-by-design principles for increased transparency and auditability in federal voting system standards. Specific to cybersecurity, industry standards already require election equipment to be used in a closed, private network, with multiple security layers across all components of such systems.

Again, Dominion Voting Systems is deeply committed to the security of our company and its products and we thank you for your efforts to promote public confidence in U.S. elections. Please feel free to reach out to Kay Stimson, our Vice President of Government Affairs, if you need further assistance. Your staff has been provided with her contact information.

Sincerely,

John Poulos
President & Chief Executive Officer
Dominion Voting Systems