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

August 8, 2018

Byte Back on Election Security: Three Major Ways that Dominion Voting is Working to Keep U.S. Voting Systems Secure

Dear Election Official:

This week, Dominion Voting is announcing its role in the founding and inaugural leadership of a new cross-partner group that brings together private industry election providers and one of the nation's leading IT forums to combat election threats and vulnerabilities.

We are proud to be partnering with the Internet Technology Information Sharing and Analysis Center (IT-ISAC) to launch the Elections Industry Special Interest Group (EI-SIG), a new information-sharing group for election industry providers to guard their networks and assets against cyber threats. The goal of the EI-SIG – or "the SIG" – is to scale up the sharing that is happening through our industry to help understand broader threats to election IT systems and engage in peer-to-peer learning across sectors of critical infrastructure with IT giants like AT&T, BAE Systems, Cisco, Intel Corporation, Hewlett Packard Enterprise, Oracle and others.

We look forward to keeping you informed about this effort, as well as some other exciting security-focused initiatives ahead. In the meantime, we have prepared this general overview to help you understand what we are doing as a company to safeguard our voting systems from cyber threats:

#1 - Dominion Voting is working with top cybersecurity professionals to enhance security.

In addition to our new collaboration with the EI-SIG, today's election systems are being designed, built, tested and audited for security and resilience. Our community of hackers currently includes federally-certified testing labs (VSTLs), state testing authorities, in-house experts and third-party security providers vetted by our company and our customers to produce responsible controlled disclosures that account for all types of existing risk. Public voting system test reports create an important level of transparency for those who wish to review the technical reports with feedback on design defects and unanticipated errors used to make continued improvements to our products. Plus, our in-house technical experts are part of U.S. Election Assistance Commission (EAC) working groups, which have brought together election officials, voting system manufacturers, accessibility and computer science experts, and other stakeholders to create the next VVSG (2.0) to ensure accessibility, security, accuracy and auditability of voting systems.

#2 – Dominion Voting is operationalizing cyber security risk on a companywide basis.

Dominion Voting takes extensive measures to safeguard our voting systems throughout their lifecycle. We are proactively working to enhance our company's information security program standards, policies and controls utilizing the voluntary National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity ("NIST Cybersecurity Framework"). The framework is also being used to collaborate across IT, engineering and operations to secure our supply chain assets (products, facilities, equipment, information and personnel) and close gaps in our vendor relationships.
Perhaps most importantly, we have actively developed and implemented staff cyber hygiene training and cyber security protocols that highlight key issues and concerns in today's threat environment.

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

#3 – Dominion Voting is working collaboratively with our customers to develop adaptive solutions to new security and technology challenges while bolstering our cyber intelligence.

Technological advances over the past decade have made voting systems more secure, reliable and resilient. However, as cyber security threats evolve and change, so do risks and vulnerabilities. Our company proudly serves as Chair of the U.S. Department of Homeland Security's Sector Coordinating Council (EI SCC). Election industry companies continue to collectively stress the findings of the U.S. national intelligence community regarding voting systems. While the risks of voting machine hacking have drawn a disproportionate amount of public attention, the experts have been clear that the closed network security around these systems makes hacking a highly difficult, improbable task – even for a nation-state. Nevertheless, in recognizing the threats that do exist, Dominion Voting continues to prioritize and enhance our incident detection, logging, monitoring and response capabilities to prevent compromises and sophisticated attacks. We are taking part in U.S. government events and exercises to inform our incident response planning and communications, and we welcome such invitations from our customers.

Last but certainly not least, we are working every day to educate stakeholders about the gap that exists between public awareness of a vulnerability in a voting system and the litany of procedural steps that election officials take that would protect their system from actual manipulation or attack, including: physical security, pre-election testing, audit processes and chain of custody standards.

A word about DEF CON

We hope this overview of company security efforts is helpful to you in preparing for this week's DEF CON hacking event in Las Vegas on August 9-11, 2018, which will once again aim to generate headlines about election security. According to the Voting Machine Hacking Village's web page, hackers from around the world will "have new models of voting machines, some of them never-before subjected to public or independent security review." The village expects visitors from Congress, the National Institute of Standards and Technology and the U.S. Department of Homeland Security.

Additional details:

- **EQUIPMENT/ATTENDEE INFORMATION:** We cannot confirm DEF CON's voting equipment inventory or attendee details. Attendees pay by cash and may remain anonymous.

- **LEGAL QUESTIONS:** The DEF CON Code of Conduct is self-enforced and "assumes people are acting in good faith and not creating intentionally elaborate, dishonest or disingenuous claims of harm." Organizers cite a Digital Millennium Copyright Act (DMCA) 2015 research exemption, but acknowledge their event is "not meant to be academic or professional."

- **REPORTING ISSUES:** DEF CON has a harassment reporting policy. We encourage election officials to document and report any harassment or threats that are generated by this event.

- **MEDIA INQUIRIES:** Please feel free to refer vendor-focused media questions to Kay Stimson, Vice President of Government Affairs | kay.stimson@dominionvoting.com.

Thank you for your support!