U.S. Election Infrastructure Sector Coordinating Council

Testimony to the
U.S. Senate Rules Committee
Wednesday, July 11, 2018
10:30 AM – 12:00 PM

Mr. Bryan Finney, CEO, Democracy Live, Inc.
Homeland Security Elections Coordinating Council Executive Committee

Mr. Chairman, Ranking Member Klobuchar and members of the Committee,

I am here today as the CEO of Democracy Live, a Seattle-based voting technology firm delivering electronic balloting technologies to members of our military, voters living abroad and the 35 million blind and disabled voters who cannot see, hold, or mark a ballot. I also have the honor of being nominated and selected as a founding member of the Homeland Security Elections Sector Executive Committee.

Having been working to help modernize elections technology in this country since the 2000 Gore/Bush election, I have had the opportunity to have spoken with and visited hundreds of local elections offices and polling places over the last two decades. My testimony today is a byproduct of that experience:

As a member of the newly established Elections Sector Coordinating Committee (or SCC), supported by Homeland Security, I would like to report that our Committee has been fully operational since our charter in February 2018. This DHS Sector Committee represents a broad and diverse coalition of more than two dozen companies and nonprofits developing, deploying and supporting elections and voting solutions to meet the needs of our nation's 200 million eligible voters and the thousands of hard working elections administrators across the U.S. In addition, our members are working collaboratively with the U.S. Election Assistance Commission, as well as state and local election offices to ensure secure, stable, scalable and protected elections and voting systems. The SCC, representing the greater elections and voting systems providers, absolutely support the increased focus and attention on the security of our nation's elections systems.

As we know, Foreign attempts to probe government voter information platforms during the presidential campaign were clearly aimed at undermining faith in America's democratic institutions. While the consensus among the intelligence community remains clear that no vote tallies were altered in any way, and there is no hard, proven evidence that any private sector provider was compromised, the existence of foreign threats means that we need to continue to be extremely diligent in protecting our nations critical voting infrastructure and instilling confidence in our U.S. electoral systems.

One key aspect of the SCC's role when it comes to developing secure and resilient technology, is to work with DHS and other government partners to ensure that industry expertise is available

to decision and policy makers at all levels. As the providers and innovators who are developing the tools that run our elections and voting systems, our SCC members routinely serve as trusted partners to State and local elections officials. We often are the "first responders," to incidents, issues and possible threats to our elections systems. This requires working closely with federal, state and local officials to identify, report and respond to incidents (both physical and cyber) that may be happening at any level of the electoral process.

SCC members are prepared to meet the threats and challenges that exist. However, with less than two dozen providers serving the needs of over 6,000 elections localities, representing nearly 200 million voters, expectations must also be aligned: First, existing levels of government investment must correspond and increase to meet the growing threats to the entire electoral system. We also request DHS support the existing public-private partnership model outlined in the National Infrastructure Protection Plan (NIPP). As the inventors, innovators, providers and partners to what is truly the engine of our democracy, it is critical we are engaged at the start of any strategic planning, testing, educating or other security initiatives relating to voting systems.

As this committee considers how to better secure our nation's elections infrastructure, I would encourage your members to remember that voting and tabulation machines, although they get the lion's share of the attention, is only the endpoint of a long process with potentially hundreds of voter touchpoints before that voter casts a ballot. These touchpoints must also be secured. They include voter registration, poll books, election night reporting, mail balloting, which is the fastest growing method of voting, and information about who and what is appearing on your ballot.

Laws and certifications exist that can and should be strengthened to better secure our voting and tabulation systems, but if the information systems are corrupted or manipulated than all the work and resources we put into hardening our voting systems may in the end be negated. In this era of voter bots and social misinformation, more and more voters are turning to their local elections officials for accurate objective information. As it was information systems that were manipulated in the recent Presidential election and not tabulation systems, I would encourage Congress to materially support elections officials to offer secure, objective and accessible voter information that voters can trust.

Finally, we need the help of Congress and other public officials in promoting greater public understanding of how elections technology is designed, tested, certified and secured. In the next few months American voters will head back to the polls. Each election is a test of the strength of our democracy. Voters could truly benefit knowing that no polling place svoting machines are connected to the Internet, the majority of systems produce a voter verified paper trail and almost all voting systems undergoes rigorous independent, 3rd party reviews by federal or state approved testing.

We look forward to being partnered with you on the work ahead, and we welcome your questions.

End of Oral Testimony

Extended Written testimony:

Risk assessments, third-party testing and voluntary blueprint models like the NIST Cybersecurity Framework are key priorities. We are also trying to address the need for increased company capabilities under the U.S. Government's Critical Infrastructure designation and how to meet the demand. Hiring additional IT and security personnel, adding resources and increasing training are key to this function. Companies are designating a qualified Chief Security Officer or Chief Information Security Officer to drive physical and cyber security initiatives, or using their existing CSO/CISO to take on new CI-related initiatives.

SCC members are talking to each other about best practices and ways to validate that they have the necessary resources (in-house or third-party) to fulfill changing expectations around security in the elections ecosystem, which is moving away from a static threat model to one of more dynamic threats. We are also working to ensure that our employees have the necessary levels of cyber hygiene training and awareness that are required to do business in the elections industry.

We are looking to provide guidance for state and local customers regarding sound cyber hygiene practices regarding operation and maintenance of our products, physical security and chain of custody policies. We are also working to make sure that customers understand the legal considerations around licensing agreements and use of third-party security services.

Situational Awareness & Communication

Beyond risk management, SCC members are focusing on situational awareness and communication.

At the federal level, SCC Executive Committee members are in the process of applying for government clearances and gaining access to the Homeland Security Information Network (HSIN) in order to receive and share classified and unclassified information with our government partners. The goal is for our full membership to receive this level of access.

Last week, this Committee also heard about how the Elections Infrastructure Subsector is working to develop an enhanced information-sharing framework for security-related communications. In addition to playing a supporting member role in the newly-formed Elections Infrastructure ISAC, which is designed to serve state and local governments, the SCC has proactively engaged the help of the IT-ISAC to form a trusted information-sharing group for the elections industry.

The goal of the Special Industry Group, or "SIG," is to scale up the sharing that's happening through our companies within the private sector to support what the Center for Cyber and Homeland Security at George Washington University has dubbed a "Super-ISAC" capability. This proactive move helps us not only see elections-specific threats, but also broader IT-focused threats towards critical infrastructure.

Working and learning from peer companies in the IT-ISAC has also allowed our members to better understand the Critical Infrastructure Ecosystem, and how it applies to the private sector. Our

goal is to strengthen the dialogue between government and industry regarding the challenges and benefits of two-way information-sharing, particularly with respect to cyber security incidents and gaps.

Response, Recovery & Resilience

Our final area of focus is response, recover and resilience. New and updated election technology is being built with resilience and auditability in mind. The election solutions that are offered by voting system manufacturers are already certified by an independent, federally-accredited Voting Systems Test Laboratory (VSTL) in order to meet standards promulgated by the U.S. Election Assistance Commission (EAC) in conjunction with the National Institute of Standards and Technology (NIST), as well as specific requirements set forth by individual States. These certified software packages and systems are the only versions allowed to be deployed for voting.

One additional and important aspect of the SCC's role when it comes to developing secure and resilient technology, is to work with DHS and other government partners to ensure that SCC industry expertise is available to policy makers. If we are going to move from election hacking events as PR stunts to true initiatives that public and private representatives of the elections community can support and learn from, such efforts need to account for real-world conditions, including business and legal risks, in addition to technical risk. A number of states have strong models for security testing, and vendors know where and how this work is possible.

The last and final point to make is that security is important, but it's just one of many criteria that exist in the elections industry. Turning ideals like "secure" and "accessible" and "anonymous" into affordable, concrete outcomes at scale is a daunting challenge. This work entails third-party dependencies, legacy requirements, competing priorities, political pressures, conflicting incentives, budget shortfalls and rigorous input and scrutiny from government, media and the public. Companies will need to prioritize security fixes and features against other requirements, and meet customer expectations on tight timelines and even tighter budgets.

Thank you.

Bryan D. Finney, CEO
Democracy Live, Inc.
bryan@democracylive.com
206.465.5636

www.democracylive.com