Statement for the Record

Julie Mathis
President and Chief Executive Officer
Hart InterCivic, Inc.

For a hearing on
2020 Election Security:
Perspectives From Voting System Vendors And Experts

Before the
U.S. Committee on House Administration

January 9, 2020

Chairperson Lofgren, Ranking Member Davis, and members of the Committee, thank you for the invitation and for the opportunity to speak with you this morning about recent steps the election industry has made to better secure the integrity of the American election system. My name is Julie Mathis and I am the CEO of Hart InterCivic.

Hart InterCivic is based in Austin, Texas where we have been located since our inception over 100 years ago. Hart began as a paper ballot printer and, over the past 20 years, we've grown organically – one new customer at a time – to become one of the top three voting system providers in the country, with customers across 20 states. Hart's voting systems are designed, engineered, and built in the United States. In fact, our manufacturing plant is only a few short miles from our headquarters in Austin, allowing us to carefully monitor the entire build and testing process end-to-end. Because we value transparency, we have invited state and local election officials from around the country, as well as officials from the Department of Homeland Security (DHS) and the Election Assistance Commission (EAC) to tour our manufacturing plant to see where and how our devices are manufactured.

At Hart, we build the voting systems that local election officials use to create ballots, capture voter choices, and tabulate and audit results. And because the elections industry is broad, it's also important to note what elements of the election process we do not provide: Hart does not manufacture any products or provide services that manage voter registration, voter check-in at the polling place, the public reporting of election night results, or any other aspect of election or data administration.

I traveled to Washington DC to participate in this hearing because Hart strongly believes that voting system companies are one of the many critical players that ensure that American elections are accessible, transparent, and secure.

I will provide perspective on a few key aspects of how the election industry has adapted to meet new challenges and threats. I'm excited to discuss how Hart as an individual company has continued our focus on security, as well as how our engagement in the larger election community has made the entire industry more secure. Much has been done by members of this community, and we are committed to continue to evolve and adapt to the changing landscape.

- The national election system is far more secure and the officials responsible for managing it are better prepared to thwart cyber security attacks today than ever before, thanks in large part to the designation of the American election system as "Critical Infrastructure" by DHS.
- Hart and the other companies present today – along with many companies not represented at this hearing – are proactive in our approach to security. We're constantly learning and improving our protocols through our engagements with federal security agencies and security experts. We're not waiting around to make our products, our company, and our customers, local election officials, more secure – we do that every day.
- Strong leadership from organizations like DHS, the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED) has delivered needed attention and resources to election offices across the country.

Critical Infrastructure

The election industry is better informed, better supported, and more agile when it comes to cyber security threats as a direct result of DHS' designation of the American election system as Critical Infrastructure after the 2016 Presidential Election.

We saw the value in engaging with DHS immediately and so became a founding member of its Sector Coordinating Council (SCC), a group of diverse elections-related vendors that have come together under DHS's stewardship to address sector-specific resilience policies and practices, as well as to share threat information across the industry. Similarly, we are a founding and engaged member of the IT-ISAC (EI-SIG)[1], as well as an active, non-voting member of the EI-ISAC [2] (full, voting membership in the EI-ISAC is reserved for state and local election officials only).

The SCC and the ISACs, both available to the industry only because of the designation of Critical Infrastructure, enable election officials and industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. Though both offer a range of valuable programs and educational materials, the biggest impact has been to our ability to communicate and coordinate around cyber threat information. Prior to the designation of Critical Infrastructure, the election community had little guidance and no direct portal to report and share information on potential vulnerabilities or discovered cyber security threats.

Today, our ability to share information across the industry has drastically improved. Both DHS and the ISACs provide dedicated lines of communication for the reporting of any new threat information up to the national intelligence agencies and then across the entire industry in a matter of hours. Typically, the information shared is related to suspicious IP addresses and phishing campaigns, but the industry stands ready to act on more serious attacks. Additionally, both DHS and the ISACs offer free security-related programs and services such as briefings on foreign threat tactics and practices, cyber security assessments, and best practice guides and checklists on election security.

The effect these groups have had on our industry in just a few short years has been significant. Perhaps the best example of the real-world impact of the SCC and ISACs is the widespread adoption of coordinated vulnerability disclosure (CVD) programs across our industry. Through our participation in the IT-ISAC, we were able to meet and discuss CVDs with companies in other sectors of Critical Infrastructure and learn from their experiences. We then put that new knowledge to use immediately, calling on experts in the field to educate the industry on how CVD programs and "bug bounty" programs could be adapted to the field of voting system manufacturers. That discussion is on-going with the release of a white paper and a Request for Information (RFI) published by the IT-ISAC, but, in the meantime, we aren't waiting. Hart has implemented a dedicated line for ethical hackers to privately and securely report any perceived vulnerabilities in our products or our networks.[3]

[1]IT-ISAC (EI-SIG): Information Technology – Information Sharing and Analysis Center (Elections Industry – Special Interest Group)

[2] EI-ISAC: Election Infrastructure – Information Sharing and Analysis Center

[3] To date, Hart has not received any reports through our CVD program.

Standards and Certification

The election industry is sometimes described as "unregulated," but that label, at least as it applies to Hart and our Verity Voting system, is misleading. Every voting machine we produce is designed to meet or exceed federal and state certification requirements.[4] After thorough internal testing, our systems are rigorously tested by independent, federally approved test labs. Despite the name of the federal standard – the Voluntary Voting System Guidelines (VVSG) – at Hart, we consider the VVSG to be anything but *voluntary*.

We strongly support, and are very actively engaged in, the process to roll out updated national standards that better address modern security practices. We have submitted comments during the Public Comment period of the draft VVSG 2.0 and are in regular communication with the EAC to provide insight and information that may inform the drafting of the updated standard. We share Congress' and election officials' frustration over the slow adoption of the new standards, and Hart has proactively continued to enhance the security protocols of our products, to ensure that we are not stagnant on critical security enhancements while waiting on the final release of the standards.

Further, we encourage Congress and the EAC to continue exploring ways to apply federal oversight on all election technology, including areas of high vulnerability – such as voter registration, electronic pollbooks, and election night results reporting.

We are optimistic that your recent increase in funding to the EAC may allow additional resources to be dedicated to the on-going update of the VVSG. As vendors, we can support and inform the process, but ultimately it is the EAC and the National Institution on Standards and Technology (NIST) that drive the program. The more resources and funding that Congress can dedicate to the EAC and NIST, the sooner we will be able to submit innovative new systems built to a more modern standard.

Hart InterCivic and the Verity Voting System

The most important shift in institutional attitudes toward securing the integrity of election systems is that security is not a static process. At Hart, we recognize that cybersecurity threats will evolve and so we must continuously adjust and adapt to new technology and new adversaries.

In recent years, we have actively and repeatedly revisited our own corporate business policies to ensure they are compliant and fully mapped to relevant national security standards, such as the NIST Cybersecurity Framework and the Center for Internet Security's Controls. All Hart employees must pass background examinations, and all employees go through repeated cyber security trainings and receive regular cyber security updates.

We are proud that our Verity Voting system is one of the newest and, we believe, most secure line of election products on the market. Rather than patch updates on to older technology, Verity is a wholly new product designed from its core to meet modern security standards.

[4] Not all states have their own state-specific certification program. Some states rely exclusively on certification to the federal VVSG, while others have their own robust certification standard independent of the VVSG.

Verity Voting systems incorporate a well-defined, end-to-end, defense-in-depth (multi-layer) security strategy across all software and hardware elements:

- Verity software cannot be accessed remotely, by Hart or anyone else.
- Verity does not encode voter selections in bar codes.
- All election data is secured with National Institute of Standards and Technology (NIST)/Voluntary Voting System Guidelines (VVSG)-compliant Federal Information Processing Standards (FIPS) 140-2 cryptography.
- Verity devices apply "surface attack reduction" in both the hardware and software to eliminate unneeded components from the voting device. Only the minimally required operating software and hardware components are built into the devices.
- Multiple, redundant data backups protect against data loss and provide comparisons to test against attempted data manipulation.
- Verity systems run in "kiosk" mode, which limits users' access to only those elements of the system they are authorized to use. No user has access to operating system files, and no other programs or files can be loaded onto systems or devices running Verity software.
- Verity devices employ "secure boot" methods that provide strong tamper notification of changes to the operating system or systems software.
- Verity employs "whitelisting" security which is more secure than traditional anti-virus applications. Whitelisting prevents any and all unauthorized software from running on the voting system.
- Verity election management software requires two-factor user authentication.
- Verity devices are protected with physical locks and tamper-evident security seals. Voters cannot insert external cards, drives, devices or cables as all external ports are protected through hardware obfuscation (non-standard connections).
- Verity tracks every user action, including logins, data entry, ballot resolution steps and other system events, providing comprehensive, plain-language audit logs that make it easy for all stakeholders to monitor how the system is used.
- Verity supports the most thorough and sophisticated post-election auditing to provide complete transparency into the accuracy of election results.
- Hart systems are designed, engineered and manufactured in the United States of America, right in our hometown, Austin, Texas.

Even with all the security features listed above, we recognize that election security requires more than applying modern technology with the latest tools and protocols. It also requires properly trained election staff using well-defined processes. Hart assists our customers in conducting secure elections by providing thorough training on all aspects of the system and by sharing best practices for processes such as managing and documenting equipment chain-of-custody and using and logging physical security seals.

We also provide instructions and training in conducting tests to validate our customers' voting systems are operating properly throughout the ownership lifecycle. Tests include user acceptance testing, logic and accuracy testing prior to each election, and parallel testing to ensure the system performs as required, and post-election audits to assure stakeholders that results are accurate.

In the election industry, the relationship between vendor and election official is a long-term partnership. The initial point of sale of an election system is only the introduction to what are typically decade-long relationships. In addition to providing technology, Hart stays in constant contact with our customers through newsletters, calls, emails, regular visits, and webinars to help ensure we are sharing the latest intelligence and best practices regarding election security.

Supply Chain

Protecting the integrity of elections is at the core of everything we do and securing our supply chain is a responsibility we take seriously. Our efforts include protection of our manufacturing operations, assessment of points of origination of all components of our products, safe-handling protocols, tracking of inventory, secure container locks and tags for products in transit, and monitoring of both external and internal risks to technology and data. We use only trusted partners in our manufacturing supply chain, and ensure that our supply chain is fully mapped, controlled and monitored from design through final delivery of a device. We actively monitor and log all chains of custody. The supply chain is regularly reviewed for new risks and our policies are continuously updated or enhanced to address any new vulnerabilities.

Though responsibility for the physical storage and conservation of election equipment rests with the local election offices once delivered, at Hart, we know our role in safeguarding those devices continues. Hart routinely provides services and education to our customers to improve security practices even after the final delivery of our products. For example, Hart regularly releases best practice recommendations and even provides in-person training with our experts on how to securely and efficiently warehouse voting systems in their government facilities. Election security experts refer to the importance of cultivating secure election management through a combination of "people, processes, procedures and technology," and Hart provides specific guidance to customers regarding the necessary security protocols to maintain ongoing security at every one of their election sites.

Conclusion

Hart remains dedicated to supporting our customers as they conduct smooth, issue-free elections which translate into high levels of voter confidence. Our systems are:

- Fully accessible by all voters, including those with disabilities, without sacrificing security.
- Capable of supporting the most sophisticated audits for full transparency.
- Federally and state certified, including thorough, independent laboratory testing.

In my perspective much has improved over the last few years – not only are there innovative products on the market with enhanced security protocols, but the election community is much better informed, more coordinated, and more aware. But this enhanced awareness also highlights the clarity that

securing the American election system is a race with no finish line. It will take constant vigilance, funding, partnership, and coordination across all aspects of the election eco-system to ensure that elections are secure each and every year.

Your recent allotment of $425 million in funding was a good start, but election officials need a regular supply of funding to improve the resiliency of their systems and purchase newer, updated voting machines.

I encourage Congress to maintain your oversight and continue to fund DHS, the EAC, and all the programs and tools they make available to election officials and election manufacturers. As you've heard today, those resources and tools are vital to our national security, and they are being implemented across the nation.

At Hart, our goal is, and always has been, to provide election officials with accessible and secure technology. We listen when experts release new best practices on cyber security. We engage in the national dialogue on election security. We participate in disaster preparedness exercises hosted by DHS and state election offices. We dedicate significant time, energy, and resources to ensuring our products meet or exceed the latest security standards. And because of all of this, we are a trusted partner of the local officials who run elections in our country.

Thank you for the opportunity to address the Committee on these important issues.