HART INTERCIVIC RESPONSE
RANKING MEMBERS' LETTER

TOPIC: Security of Hart InterCivic's Voting Systems
REQUEST DATED: March 20, 2019
RESPONSE DATED: April 9, 2019

1. What specific steps are you taking to strengthen election security ahead of 2020? How can Congress and the Federal Government support these actions?

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

We are proud that our Verity Voting system is 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.

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

- No Verity device is capable of connecting to the internet.
- Verity software cannot be accessed remotely, by Hart or anyone else.
- 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 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 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.

Even with all the security features listed above, we recognize that election security requires more than applying modern technology with the latest 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 procedures 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 to ensure the system performs as required, and post-election audits to assure stakeholders that results are accurate. Hart stays in constant contact with our customers to ensure we are sharing the latest intelligence and best practices regarding election security.

Finally, Hart remains actively engaged in the national conversation on election security on an ongoing basis. We are connected with a broad community of stakeholders actively participating in knowledge sharing, best practice sharing and discussions on the latest election security technology and procedures. Some examples include:

- **Department of Homeland Security** – Hart is a founding member of the DHS Sector Coordinating Council, a formalized group of industry representatives who together act as a voice on election cybersecurity. In coordination with the DHS Government Coordinating Council, Hart participates in identifying potential security risks and implementing measures to eliminate those risks.

- **Center for Internet Security** – Hart contributed to CIS's recent publication, "A Handbook for Elections Infrastructure Security" and closely follows Best Practices and other guidance from CIS.
- **ISACs** – Hart proactively engages with several relevant Information Sharing & Analysis Centers (ISACs), including the IT-ISAC, the MS-ISAC (Multi-State), and the EI-ISAC (Election Infrastructure).
- **Election Assistance Commission** – Hart meets regularly with the EAC and actively participates in industry-wide initiatives.
- **National Academies of Science, Engineering, and Medicine** – As one of only two manufacturers to appear at the meeting of the NASEM Committee on Science, Technology and Law on the Future of Voting (Denver, Dec. 8, 2017), Hart actively participates in the conversation on technology innovation to safeguard elections.
- **Election Center** – Hart leadership serves on the Security Committee with the Election Center, participating in national conversations about cybersecurity at conferences that include a diverse array of election stakeholders (state and county officials; election administrators; technology and security experts) and at least a dozen of our Hart staff members are certified through the Election Center or are working on certification.
- **National Association of Secretaries of State** – Hart regularly exhibits our technology at NASS events, engages in conferences, attends substantive sessions on election topics – including security – and produces a bi-annual white paper submission.
- **National Association of State Election Directors** – Hart regularly exhibits our technology at NASED events and participates in election security sessions

In the wake of the 2016 election cycle, new federal funding and cyber security-related resources were released to election officials across the country. These resources had an immediate and significant impact on the security posture of state election offices.

In order to further bolster this progress leading into the 2020 election, the federal government should create a regular and reliable source of resources and funding dedicated to assisting election officials purchase new election technology. Threats to our national election system do not pop up once every ten years – neither should federal resources to help election officials maintain modern and secure voting systems. Further, the Election Assistance Commission (EAC) should be appropriately resourced to improve the speed and scope of the federal certification process. Without the personnel to process certification requests in a timely manner, system updates may lag as they wind through lengthy federal and then state certification processes.

2. What additional information is necessary regarding VVSG 2.0 in order for your companies to begin developing systems that comply with the new guidelines?

Hart is actively engaged with the EAC to help develop, improve and modernize the VVSG. We regularly participate in calls and meetings with the Technical Guidelines Development Committee (TGDC), and our team of election experts is now reviewing and drafting feedback on the VVSG 2.0 Principles and Guidelines currently out for public comment.

However, until the release of the regulations and test assertions that support the Principles and Guidelines and interpret and direct the technical specifications of system builds – an unknown date at this time – no companies will be able to build or test to the VVSG 2.0 standard.

3. Do you anticipate producing systems that will be tested for compliance with VVSG 1.1? Why or why not?

Yes, building to the latest standard is important to our customers and it is important to us. The local and county officials that run elections on Hart voting systems have made it clear that they expect new elections systems to comply with the newest standards. We've heard their call and look forward to being one of the first Election systems vendors to certify a voting device to the VVSG 1.1 standard.

4. What steps, if any, are you taking to enhance the security of your oldest legacy systems in the field, many of which have not been meaningfully updated (if at all) in over a decade?

To safeguard older election equipment still in the field, we maintain regular contact with our customers, routinely conducting webinars and releasing best practice reports on proper maintenance of Hart voting systems, chain-of-custody procedures, and the latest technical security guidelines and practices.

We believe it is our responsibility to alert and educate local election officials to the latest trends in elections security. A true defense-in-depth approach to securing our election system goes beyond technology; as described in previous answers, the people and processes in election administration are essential safeguards of our democracy. Through routine outreach and education across our customer base, we hope to mitigate potential threats before they can take root.

That trusted relationship we share with our customers also allows us to have honest conversations with local officials still on legacy systems who would be better served by a transition to newer, more secure, more advanced voting systems. For many local election offices, the optimum path to improved security is a full upgrade to our Verity Voting system which was designed to modern standards of security and usability.

5. How do EAC certification requirements and the certification process affect your ability to create new election systems and to regularly update your election systems?

The EAC's role in setting a single federal standard for the testing and certification of election devices and software is a considerable asset to both the vendors who manufacture election systems and the government officials who deploy them. The EAC's certification process is drastically more transparent and successful than previous iterations run through the FEC and the National Association of State Election Directors (NASED).

However, with reduced resources to support and manage the process, the speed and scope of what the EAC can accomplish is limited. According to the executive director of the EAC, in 2010, the agency had six positions dedicated to the certification of election technology. Today, the EAC has only three positions dedicated to certification; and with one position now open, a staff of two is currently overseeing the entire federal certification program.

As election system manufacturers, our ability to bring new, innovative products and timely upgrades to market is strained and slowed by a lengthy federal certification process. The single most direct and impactful way to improve the security of America's elections is to fully fund and staff the EAC.

6. Do you support federal efforts to require the use of hand-marked paper ballots for most voters in the federal elections? Why or why not?

How voters cast their ballot is a policy choice best decided by the elected officials that live, work, and interact with the citizens in their local communities.

Hart is committed to providing secure election technology across multiple voting styles, including hand-marked paper ballots. So long as election systems pass rigorous state and federal testing and certification and are accompanied by effective post-election audits, we stand ready to deliver voting solutions that meet the requirements and needs as determined by local officials.

7. How are you working to ensure that your voting systems are compatible with the EAC's ballot design guidelines (ie "Effective Designs for the Administration of Federal Elections)?

Thanks to the work of industry leaders in this field, such as the Design for Democracy program at the American Institute of Graphic Arts (AIGA), we know that poorly designed ballot layout can significantly impact voters' ability to have their vote selections counted as intended. With that in mind, Hart designed our new Verity Voting system specifically to adhere to the best practices established in the EAC's "Effective Designs for the Administration of Federal Elections."

Every Verity system and ballot we design is influenced by the standards and guidance from the experts at AIGA. In fact, Hart was the first Election system manufacturer to adopt and implement the AIGA's Design for Democracy

methodology across an entire product platform. Additionally, in 2015, the Verity UI (User Interface) was certified to the design standards established by the EAC in VVSG 1.0.

8. Experts have raised significant concerns about the risk of ballot marking machines that store voter choice information in non-transparent forms that cannot be reviewed by voters (ie such as barcodes or QR codes), noting that errors in the printed vote record could potentially evade detection by voters. Do you currently sell any machines whose paper records do not permit voters to review the same information that the voting system uses for tabulation? If so, do you believe this practice is secure enough to be used in the 2020 election cycle?

   Hart is one of the only election system manufacturers in the country with an EAC-certified ballot marking device (BMD) that does not place the vote selections in a barcode or QR code.

   Our device, Verity Duo, produces a printed ballot with a clear, legible summary of the voter's ballot choices, including the name of the contest, the full name of the selected candidate and the candidate's party. The ballot from Verity Duo is processed and tallied using Optical Character Recognition (OCR), which means the scanner reads the same printed words that the voter verified.

   Only Verity Duo combines the ease and accessibility of vote selection on a touchscreen interface with an assurance of vote capture that can be visually validated by the voter. Verity tallies the voter selections from the same printed words the voter verified. At Hart, we believe that words matter.

9. Do you make voting systems with Cast Vote Records (CVRs) that can be reliably connected to specific unique ballots, while also maintaining voter privacy? If not, why not? Does your company make voting systems that allow for machine-readable data export of these CVRs in a format that is presentation-agnostic (such as JSON) and can be reliably parsed without substantial technical effort? If not, why not?

   Yes, Hart's voting systems can reliably link CVRs back to a unique ballot without compromising the identity of the voter. Hart devices employ human and machine-readable exports in XML that can be parsed without substantial technical effort to assign a unique ID at the time the ballot is cast

10. Would you support federal legislation requiring expanded use of routine post-election audits, such as risk-limiting audits, in federal elections? Why or why not?

    Effective audit practices, such as risk-limiting audits, are an essential component to the integrity of every eligible American's vote. Audits not only increase the likelihood that any malicious tampering or malfunctioning machine in an election is detected and corrected, they provide the public with needed assurance that the outcome of an election contest was accurately determined and reported.

In late 2018, The National Academies noted in its report, Securing the Vote: Protecting American Democracy, that "…the most significant threat to the American elections system was coming, not from faulty or outdated technologies, but from efforts to undermine the credibility of election results. Unsubstantiated claims about election outcomes fanned by social and other media threaten civic stability."

Robust post-election audits are the most compelling response to this threat. Auditing is the most transparent and effective means to demonstrate that election outcomes accurately reflect the intention of voters. Hart unequivocally supports state efforts to strengthen auditing procedures.

11. What portion of your revenue is invested into research and development to produce better and more cost-effective voting equipment?

As described in responses to previous questions, Hart's Verity Voting system is an entirely new product, designed from the ground up to maximize usability, reliability, flexibility and security. Verity was first released and certified in 2015, with the most recent certification, for Verity Duo, coming as recently as March 2019. Over the course of Verity's conception, design, and initial development and build, significant resources were dedicated to research and development.

Hart continues to invest in designing and marshalling new products to market, along with enhancing our existing products through significant levels of investment in research and development and certification.

12. Congress is currently working on legislation to establish information sharing procedures for vendors regarding security threats. How does your company currently define a reportable cyber-incident and what protocols are in place to report incidents to government officials?

To ensure security events are quickly and concisely identified, eradicated, and reported, Hart's incident response methodology was developed to align with the best practices and guidelines established in NIST's Computer Security Incident Handling Guide (NIST SP 800-61) and the CIS Control 19: Incident Response and Management.

Broadly, any observable incident in which Hart networks or data is threatened triggers our response plan:

- **Detection and Analysis** – The first stage of our incident management policy includes the initial identification, assessment and triage of the security incident, including notification and analysis by the appropriate team member given the specifics of the incident.
- **Containment and Recovery** – Next, a detailed impact analysis is performed to ascertain the degree of the impact and prioritize any additional response activities that may be required for actual breaches. With the analysis information

in hand, containment activities kick in, and a tailored plan for recovery is executed.

- **Review and Report** – Finally, after the incident is appropriately managed, a draft report is developed detailing the origin and impact of the incident, along with instructions and guidance to prevent future incidents. The incident is then reported internally and externally, as appropriate.

We rely on the DHS' Sector Coordinating Council and the IT-ISAC Election Industry – Special Interest Group (EI-SIG) as the primary channels for communicating incidents up to appropriate government officials and out to other election system vendors who may similarly be affected. The emergence of both organizations over recent years has made incident reporting clear and direct.

13. What steps are you taking to improve supply chain security? To the extent your machines operating using custom, non-commodity hardware, what measures are you taking to ensure that the supply chains for your custom hardware components are monitored and secure?

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.

Security features of Hart's supply chain include:

- Hart is in direct control of the supply chain for Verity voting systems.
- All Hart voting devices are manufactured in the United States of America.
- Hart's manufacturing facility is within three miles of Hart's main office with restricted and controlled access to authorized personnel.
- As a voting solution that is relatively new in the market, Verity Voting was most recently certified by the EAC in March 2019. The supply chain is a newly scoped, closely managed element of Hart's direct approach, which protects the integrity of all parts of the system.
- Our return authorization process defines a strict step-by-step procedure for logging, securing and tracking chain of custody of product that requires technical attention that cannot otherwise be repaired in the field.
- When returning a product to a customer, Hart first follows specific state mandated policies for handling returned equipment per that state's guidelines. If there is a return to a state without prescribed return policies, Hart secures devices with custom tamper-evident seals specially designed for this purpose.

- Stringent security assurances are built into the agreements with our manufacturing partners.
- 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 trainings with our experts on how to securely and efficiently warehouse voting systems in 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 to ensure they meet the necessary security protocols to maintain ongoing supply chain security at every one of their election sites.

14. Do you employ a full-time cybersecurity expert whose role is fully dedicated to improving the security of your systems? If so, how long have they been on staff, and what title and authority do they have within your company? Do you conduct background checks on potential employees who would be involved in building and servicing election systems?

A core tenet at Hart is that security is a fundamental architectural and design requirement across all product development, quality, and regulatory requirements. Hart manages this focus on security through a rigorous, structured, documented phase gate process in which regular security audits and threat assessments are conducted and required before progressing through the phase gate process. This process is closely managed by Hart senior management and reviewed throughout the phase gate process.

To ensure that Hart's awareness and focus in the cyber security arena is relevant and in consideration of current known indicators, Hart also engages with multiple experts and credentialed consultants to supplement Hart's managers in specific areas of security standards and policies. In addition to our routine interactions with the Department of Homeland Security, the EAC, and the ISACs, as mentioned previously in this response, we have also directly engaged with trusted experts in the field of cyber security. We have brought in, and will continue to bring in, security consultants and firms that are nationally recognized experts in the field of security management to assess our policies against relevant federal standards – such as the NIST cyber security framework and CIS controls – and make recommendations on where our policies and practices could be improved.

Every Hart employee must pass background checks.

15. Does your company operate or plan to operate, a vulnerability disclosure program that authorizes good-faith security research and testing of your systems, and provides a clear reporting mechanism when vulnerabilities are discovered? If not, what makes it difficult for your company to do so, and how can Congress and the federal government help make it less difficult?

Earlier this year, Hart sat with several of our industry competitors in a day-long meeting hosted by the IT-ISAC (EI-SIG) in which representatives from the auto, aviation and medical device industries discussed their participation in a vulnerability disclosure program (VDP). Executives from the three industries highlighted their work with ethical, vetted, "white hat" security researchers to test for vulnerabilities among their various products. We heard them emphasize the importance of collaboration with reputable coordinated vulnerability disclosure service providers, and we listened.

Hart is committed to participating in a VDP and is working closely with the IT-ISAC (EI-SIG) and the EAC to develop a policy and build a secure channel for researchers to report security issues under a process that allows for the disclosure and mitigation of any discovered issues in an appropriate and timely manner.

However, Election system vendors can move only as quickly as the certification process allows. Once a vulnerability is identified, mitigated and a solution developed, it still may take months to deploy as the patch winds through lengthy federal and state certification programs.

The timing and process challenges inherent in testing and certification make an industry-wide VDP for election system manufacturers difficult to achieve without the direct assistance of the federal government through a properly resourced EAC. Looking to the future, the EAC should consider the feasibility of fast tracking or expedited review of issues that come through certification to address security vulnerabilities.

16. How will DARPA's work impact how your company develops and manufacturers voting machines?

Hart intends to pay close attention to any project that brings to bear the technical and security expertise housed within DARPA.

Though important questions remain as yet unanswered regarding whether and how the project will fit with the EAC's VVSG and certification process, should the project ultimately be successful, we look forward to leveraging any design features – hardware or software – that may improve the integrity and transparency of Hart's Verity Voting system.