# Appendix B

# FACT SHEET: The U.S. Election Assistance Commission's Voting System Testing and Certification Program

For more than a decade, the EAC's Testing and Certification Program has assisted state and local election officials by providing timely and accurate voting machine testing. This program is a requirement of the Help America Vote Act (HAVA) of 2002, legislation that created the EAC and mandated that the Commission provide certification, decertification, and recertification of voting systems, as well as the accreditation of voting system testing laboratories. This legislation marked the first time the federal government provided oversight for these activities, a step that allowed states to procure new certified voting systems without the added expense of independent testing and certification.

## What standards are used to test and certify election systems?

Election systems are tested for compliance to the Voluntary Voting System Guidelines (VVSG), which are a set of requirements that voting system hardware and software must meet to receive a certification. Some areas examined during testing include functionality, accessibility, accuracy, auditability and security capabilities. HAVA mandates that the EAC develop and maintain these requirements, as well as test and certify voting systems. On December 13, 2005, the EAC unanimously adopted the 2005 VVSG that significantly increased security requirements for voting systems and expanded access to voting, including opportunities for individuals with disabilities to vote privately and independently. The 2005 guidelines updated and augmented the 2002 Voting System Standards, as required by HAVA, to address advancements in election practices and computer technologies. These guidelines were again updated by the EAC and NIST and approved by EAC's Commissioners on March 31, 2015. The guidelines are voluntary, but it is of note that 47 states use EAC requirements, testing or voting system test laboratories to supplement or fulfill certification requirements in their state.

## How does the voting system certification process work?

The EAC accredits independent voting system test laboratories (VSTLs) that evaluate voting systems against the Voluntary Voting System Guidelines (VVSG) to determine conformance to the standard and test the basic functionality, accessibility, and security capabilities required of these systems. The test laboratory provides a recommendation to the EAC via a test report, the Testing and Certification Program Director accepts the test report and issues a recommendation to the EAC's Decision Authority (e.g. Executive Director), who makes the determination whether to issue a certification. After a decision is made on certification, the EAC posts the information on the Voting System Certification section of its website.

## How are the laboratories that test voting systems accredited?

HAVA requires that the National Institute of Standards and Technology (NIST) assist the EAC through its National Voluntary Laboratory Accreditation Program (NVLAP), which provides recommendations to the EAC regarding laboratory accreditation. After the EAC receives NVLAP's recommendations, the program conducts further review to address additional issues such as conflict of interest policies, organizational structure and recordkeeping protocols. After the EAC's final review is complete, the Commissioners vote regarding full accreditation.

## How many election systems has the EAC tested and certified?

The EAC has successfully completed 60 certification campaigns in coordination with 5 voting system vendors. Of the 60 voting systems submitted for certification, to date the EAC certified 38 voting systems or modifications to a voting system.

## How does this program help state and local election officials?

At least 47 states use the EAC's Testing and Certification program in some way when deciding which voting system to purchase, a decision which may save taxpayer dollars and can eliminate time lost to duplicative testing. In addition, State and local officials often request that the EAC provide assistance with editing and reviewing requests for proposals (RFPs) and other documents used in the election technology procurement process. These activities save jurisdictions time and money.

## When will the next set of testing and certification guidelines be released?

The EAC is working with the Technical Guidelines Development Committee (TGDC) – a diverse EAC advisory board comprised of representatives from the election community, public sector, private sector and interest groups – to develop the next iteration of the election system testing and certification guidelines, VVSG 2.0. A set of 17 core voting system functions that will guide the VVSG 2.0 were adopted by the TGDC. The VVSG 2.0 is a nimble high level set of principles and guidelines that will be supplemented by accompanying documents that detail specific requirements for how systems can be tested to meet the new guidelines. The supplemental documents will also detail assertions for how the accredited test laboratories will validate that the system complies with those requirements. The new system testing guidelines are expected to be released in 2018 and will become the most technically up-to-date standard against which voting systems can be tested in the United States.

**U. S. ELECTION ASSISTANCE COMMISSION**
**VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM**
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

Mr. Mark Skall
Chief, Software Diagnostics and Conformance
Testing Division
National Institute of Standards and Technology
100 Bureau Dr.
Gaithersburg, MD 20899-8970

Ms. Mary Saunders
Chief, Standards Services Division
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 2100
Gaithersburg, MD 20899

March 13, 2008

Dear Ms. Saunders and Mr. Skall:

The U.S. Election Assistance Commission (EAC) appreciates the work done by the National Voluntary Laboratory Accreditation Program (NVLAP) over the past two and one-half years to accredit Voting System Test Laboratories (VSTLs). We value our partnership established under Section 231 of the Help America Vote Act (HAVA) and continue to count on the expertise of NVLAP to assure the technical competency of the VSTLs. HAVA tasks NIST with the responsibility to "monitor and review, on an ongoing basis, the performance of the laboratories accredited by the Commission". As such, NVLAP recommendations are a pillar of the EAC laboratory accreditation process and a key component to a successful certification program.

Now that those VSTLs initially reviewed and accredited through the NVLAP program are approaching their second review pursuant to the renewal of their accreditation, the EAC believes this would be an appropriate time to discuss some observations and concerns gained from working with the VSTLs during recent EAC certification engagements.

Because the VSTLs have moved forward quickly to hire the staff necessary to take on a heavy workload of voting system test engagements, we would like your upcoming reviews to include an evaluation of the following staffing related issues:

- Please review the management process of each lab for assigning appropriately qualified staff to their EAC related voting system test engagements.
- Review the qualifications of all staff members directly involved in the testing of voting systems to assure that each has the appropriate qualifications and appropriate certifications in their relevant testing areas (for example a CISSP or similar certification for staff involved in security testing).
- Review how the VSTLs prioritize staffing for Federal testing engagements and other state or local voting system testing arrangements to ensure that testing is being conducted and managed by qualified personnel.

Furthermore, as you know, NIST is in the process of developing a standardized suite of test methods for voting systems. Because the VSTLs do not yet have such standardized methodology, each lab must currently develop and validate unique test methods appropriate for voting systems. The EAC recommends NVLAP review these test methods and their validation by the VSTL's to ensure that NIST remains confident of each VSTL's ability to test voting systems.

If NVLAP is unable for any reason to undertake any of the review items noted above, please inform the EAC at your earliest opportunity so that we may immediately pursue other avenues for laboratory review on these issues.

Thank you once again for your ongoing work in this extremely important field of accreditation. The EAC and the voting public is indebted to NVLAP for this invaluable service to our country.

Sincerely,

Brian J. Hancock
Director
Testing and Certification

**U. S. ELECTION ASSISTANCE COMMISSION**
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

Mary Saunders
Chief, Standards Services Division
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 2100
Gaithersburg, MD 20899

July 10, 2008

Dear Ms. Saunders,

Now that many of the Voting System Test Laboratories (VSTLs) have completed their 2nd NVLAP accreditation review, the EAC would like a status report from NVLAP on the items we noted as observations and concerns in our letter to you dated March 13, 2008. (Attached) Because these issues are so critical to the success of our certification program, we are requesting a response by August 8, 2008, or sooner if possible.

Specifically, we are interested in updates on how SysTest Labs LLC, iBeta Quality Assurance, and Wyle Laboratories:

- Assign appropriately qualified staff to EAC certification engagements.
- Assure that testers have certification in specific critical areas, particularly a CISSP or similar certification for staff involved in security testing.
- Prioritize EAC certification engagements in light of other State or local contractual responsibilities.
- Use their quality management process to develop and validate test methods to ensure test-to-test and case-to-case repeatability.

As you know, the credibility of the EAC Testing and Certification Program depends largely on having competent VSTLs to thoroughly test voting systems to the applicable Federal Standards. NVLAP review of the technical competency of these laboratories is a critical prerequisite to EAC accreditation of the VSTLs and provides assurance that the labs will function in accordance with internationally accepted standards for testing bodies.

Thanks to you and the NVLAP staff for your continued great work and support.

Sincerely,

Brian J. Hancock
Director, Testing and Certification

RON WYDEN
OREGON

COMMITTEES

# United States Senate

WASHINGTON, DC 20510-3703

October 3, 2017

Ms. Traci Mapps
Director of Operations
SLI Compliance
4720 Independence Street
Wheat Ridge, CO 80033

Dear Ms. Mapps:

I write to seek public answers about cybersecurity threats to our election infrastructure and whether the election technology and election technology testing industries have taken steps to defend against hackers, including those working for foreign governments.

As our election systems have come under unprecedented scrutiny, public faith in the security of our electoral process at every level is more important than ever before. Ensuring that Americans can trust that election systems and infrastructure are secure is necessary to protecting confidence in our electoral process and democratic government. This effort must include not only the manufacturers and government consumers of election systems but also the Voting System Test Laboratories accredited by the U.S. Election Assistance Commission.

In order for Congress and the American people to better understand the threats that your company faces and the steps you have taken to protect against them, I would appreciate complete answers to the following questions by October 31, 2017.

1. Does your company employ a Chief Information Security Officer? If yes, to whom do they directly report? If not, why not?
2. How many employees work solely on information security?
3. In the last five years, how many times has your company utilized an outside cybersecurity firm to audit the security of your testing equipment and systems and to conduct penetration tests of your corporate information technology infrastructure?
4. Has your company addressed all of the issues discovered by these cybersecurity experts and implemented all of their recommendations? If not, why not?
5. What is the process for when your laboratory determines that a product undergoing testing has potential security vulnerabilities? Do all security vulnerabilities result in non-certification of a product undergoing testing? Are all product security vulnerabilities reported to the manufacturer and to the Election Assistance Commission?
6. Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data? If your company has suffered one or more data breaches or other cybersecurity incidents, have you reported these incidents to federal, state and local authorities? If not, why not?
7. Has your firm implemented the best practices described in the NIST Cybersecurity Framework 1.0? If not, why not?

If you have any questions about this request, please contact Chris Soghoian on my staff at (202) 224-5244.

Sincerely,

Ron Wyden
Ron Wyden
United States Senator

SLI COMPLIANCE
4720 INDEPENDENCE ST • WHEAT RIDGE, COLORADO 80033 • 844-754-8683 • 303-422-1566
slicompliance.com SLI Compliance, a Division of GLI®

October 30, 2017

Honorable Ron Wyden
United States Senator
221 Dirksen Senate Office Building
Washington, DC 20510

**Re: Response to Letter Pertaining to Cybersecurity**

Dear Senator Wyden,

SLI Compliance (SLI), a Division of Gaming Laboratories International LLC. (GLI), received an email from Mr. Chris Soghoian, TechCongress Innovation Fellow, on October 2, 2017 seeking public information regarding election security and asked that we respond by October 31, 2017. Some of the information requested may more appropriately be obtained from the U.S. Election Assistance Commission (EAC).

As an accredited Voting System Test Laboratory (VSTL) under the National Voluntary Accreditation Program (NVLAP) of the National Institute of Standards and Technology (NIST) (NVLAP Lab Code 200733-0: TESTING) and the EAC, SLI conforms to the ISO 17025 and ISO 9001:2008 standards including the NIST Handbook 150 and 150-22. In addition, SLI adheres to all mandatory procedural requirements under the EAC as written in the EAC Voting System Test Laboratory Accreditation Program Manual and EAC's Voting System Testing and Certification Program Manual.

SLI and GLI as a company would like to assure you that our organization takes cybersecurity and the protection of our systems very seriously. We have taken stringent measures to identify, mitigate and contain threats to our company's digital infrastructure, including but not limited to companywide security awareness training, ongoing vulnerability assessments and continuous system monitoring and auditing. SLI is subject to regular audits, compliance disclosures and other regulatory and certification requirements as part of its ongoing obligation to remain accredited by the aforementioned oversight bodies.

We would like to encourage you, and/or Mr. Chris Soghoian, to contact the EAC directly for any further questions in regards to the accreditation and requirements of a VSTL under the EAC's Testing and Certification program.

Sincerely,

Traci Mapps
Director of Operations
SLI Compliance, a Division of GLI LLC

**U. S. ELECTION ASSISTANCE COMMISSION**
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

August 14, 2019

**Sent via email**

Pam Geppert
Hart InterCivic
15500 Wells Port Drive
Austin, TX 78728

**Approval of Voting System Testing Application Package**

Dear Pam Geppert,

The U.S. Election Assistance Commission (EAC) completed the review of the application package for the Hart Verity Voting 2.4 voting system. The application was accepted and assigned the following unique application number: HRT-Verity-2.4.

Hart InterCivic selected SLI Compliance as the lead VSTL for this testing engagement and testing will be conducted to the VVSG 1.0. If the system meets the criteria for a grant of certification, the system will be assigned the number "**HRT-Verity-2.4**" per your request on the application form (EAC-002C).

The Certification Program assigned Jessica Bowers as Project Manager to oversee this testing engagement. The goal of the Project Manager is to facilitate the communication between EAC staff (including Technical Reviewers), manufacturer, and VSTL to optimize the efficiency of the certification process. The Project Manager will monitor the voting system throughout its life cycle in the Certification Program, and ensure the process meets the requirements of the Certification Program's manuals. The contact information for this Project Manager is:

- Name and Title: Jessica Bowers, Senior Election Technology Specialist
- E-mail: jbowers@eac.gov
- Telephone: (202) 459-7861

The EAC may at any time utilize additional technical reviewers to assist in the review of test plans, test cases, and test reports. All communications with the technical reviewers shall be facilitated through the Project Manager.

Finally, we strongly encourage you to regularly visit the EAC's Web site (www.eac.gov) for the latest Notices of Interpretation and Clarification, news, program manuals, and updates. The exact location of this information is: https://www.eac.gov/voting-equipment/system-certification-process-s/. The information contained in the Notices of Interpretation and Clarification is critical to understanding testing standards and program requirements. It is a manufacturer's responsibility to ensure they adhere to all procedural requirements of the program.

If you have any questions or need further information about this matter, please do not hesitate to contact us at your earliest convenience. We thank you in advance for your cooperation in this matter.

Sincerely,

Jerome C Lovato

Jerome Lovato
Director, Voting System Testing and Certification

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.

**What happens if something changes or goes wrong?**

Hart has contingency plans in place to mitigate risks caused by supplier or subcontractor interruptions, as well as plans to cover any risks related to manufacturing interruptions. Additionally, we carry business interruption insurance coverage that provides customers with further assurance that we are positioned to provide continuous service and support.

In 19 years of manufacturing voting systems, Hart has managed numerous supply chain interruptions with no disruptions to our customer base. We maintain an adequate supply of inventory at Hart and at several secure offsite facilities as part of our business continuity plan. We have managed several major weather events both at Hart and at several of our key suppliers with no issues. We have managed through tornadoes, hurricanes, floods, heat waves, and ice storms – as well as transitioning our top tier partners with no loss of supply and no interruption of service to customers. Our business continuity plan has been tested, and we continually update it.

# Certification

**Does Hart have to get it's voting technology approved?**

Yes.

Voting systems must pass rigorous, independent testing and receive certification at the federal and state levels.

Unlike many other elements of the election system, voting systems must pass rigorous, independent testing to specific requirements to receive certification at the federal and state levels prior to being used by local jurisdictions.

The U.S. Election Assistance Commission (EAC) oversees the definition of federal voting system certification requirements and the thorough, independent testing process which determines whether a voting system meets those requirements. Voting system vendors are well-acquainted with the rigors of testing at the federal level and must plan years in advance to stage product releases.

In addition to the federal certification process, many states maintain their own separate certification and testing procedures. Voting system vendors must ensure their systems meet or exceed both the federal and state-level requirements to do business in those states.

**Do federal and state certification officials look at security?**

To be awarded certification at the federal level, by the EAC, and to attain state certification, which is required in many states, voting systems must meet or exceed established security standards. Certified voting systems adhere to standards designed to ensure that systems accurately record votes the way they are cast. Security standards include protections against tampering or manipulation and cover requirements for physical security of the equipment and ballots, features that prevent connection to the internet or a network during the voting period, auditing capabilities and more.

**Are Hart systems independently validated beyond EAC and state certification officials?**

Yes.

The Help America Vote Act (HAVA) of 2002 set the requirement for voting systems to be tested by independent, non-federal laboratories, which are called Voting System Test Laboratories, or VSTLs. Voting system vendors are not at liberty to select a VSTL, rather the EAC maintains the authority to designate the VSTL that will perform certification tests and technical review.

**How do federal and state certification requirements keep our elections secure?**

The federal and state certification processes provide transparency into the security of voting system solutions as follows:

- Federal and state certification program manuals and guidelines are publicly available.
- Independent voting system test laboratories (VSTLs) that test voting systems are accredited through a public process.
- Information about each certification campaign, including reports from VSTLs attesting to compliance with applicable security requirements, are publicly available.
- Source code, along with thousands and thousands of pages of technical documentation, is securely disclosed to accredited, U.S.-based laboratories, as part of federal and state testing and certification processes.

# Company

**Is security important to Hart?**

Security and auditability are of paramount importance to Hart InterCivic. The Hart Voting System and the Verity Voting system are regulated, tested and certified at both the federal and state levels. They have both been proven to be secure and accurate, successfully capturing and reporting millions and millions of votes across nearly 800 jurisdictions representing over 26 thousand precincts and nearly 30 million registered voters.

Security comes not only from hardware/software technology features, but also from the people who use the systems and the procedures they follow. Hart provides training courses for system operators and election officials, which includes security topics, physical device configuration, and data transfer. Hart encourages jurisdictions to utilize best practices to mitigate risks. Some include:

- Employing a chain of custody processes throughout all pre/during/post-election activities, physical numbered and logged security seals on devices, and experienced trusted election workers on staff
- Conducting Acceptance Testing upon receipt of equipment
- Pre-Election Logic and Accuracy Testing (conduct as provided under your respective State law)
- Post- Election auditing by inspecting the precinct totals and comparing to the cumulative totals

recent purchase of a new voting system.

a. The federal and Texas state rules which govern voting system requirements, testing and certification do not prohibit the use of touch-screen voting systems.
b. The EAC, which oversees the federal certification requirements, as well as the testing and certification processes, is made up of a bipartisan group of commissioners.
c. The system purchased in San Jacinto County, Texas has undergone rigorous testing and examination at both the federal and state levels. The federal certification process is an open inspection process, whereby Hart provides all source code for every component of the voting system, and it undergoes careful review by test laboratories that must be accredited by both the EAC and the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP). The EAC and the voting system test lab also have full access to a detailed Technical Data Package (TDP) describing the architecture and technical details of the entire voting system. There is nothing secretive about this process, and it includes common sense protections by the EAC and state authorities to prevent the release of sensitive information that could impact the integrity of the vote.
d. The EAC federal certification body publishes detailed information about certified voting systems and systems under test. Those documents are publicly available, at https://www.eac.gov/voting-equipment/system-certification-process-s/
e. The State of Texas Secretary of State publishes public, detailed information about certified voting systems. Those documents are publicly available, at https://www.sos.state.tx.us/elections/laws/votingsystems.shtml

**2) The story says,** *"Cyber experts, including a team from the nation's premier technology standards-setting lab, have warned since 2006 that hackers can plant vote-altering malware in electronic machines and some now say the cyberattacks could occur at plants where the machines are made...But an obscure federal agency charged with issuing election guidelines for state and local officials rejected the experts' finding in 2007, and 11 years went by before it recently took steps to reverse itself."* **This account of federal oversight and the experts that have been relied upon is inaccurate and misleading:**

a. As part of EAC certification, systems go through the "trusted build process," performed by accredited Voting System Testing Laboratories (VSTLs). During this process, secure workstation and device images are produced and securely stored with the EAC. Each set is uniquely tagged with a secure hash of the certified software components and is stored securely with the EAC. At any time, any jurisdiction can verify that the software they are running locally is consistent with the official source code on file with the EAC to ensure that the deployed configuration matches the system configuration certified by the EAC.

a. As part of EAC certification, systems go through the "trusted build process," performed by accredited Voting System Testing Laboratories (VSTLs). During this process, secure workstation and device images are produced and securely stored with the EAC. Each set is uniquely tagged with a secure hash of the certified software components and is stored securely with the EAC.
b. At any time, any jurisdiction can verify that the software they are running locally is consistent with the official source code on file with the EAC to ensure the deployed configuration matches the certified configuration.
c. The federal VVSG standards also have rigorous requirements for audit logging capabilities in all voting systems which produces a transparent record of all activity in the system. VVSG requirements for logging require voting systems to track, store and report each and every action associated with tasks such as creating an election/ballot, programming devices, reading captured vote data, adjudication of voter intent, tabulation of results, and reporting of results. Verity has extensive logging capabilities that exceed VVSG requirements. Verity's plain language logs and reporting provide complete transparency and are protected from tampering through encrypted digital signatures. Logging cannot be disabled through any means.
d. When new systems are purchased, the jurisdiction goes through a thorough User Acceptance Testing (UAT) protocol to ensure that all software installed on the new system matches the software version that has been certified by federal and/or state authorities, and the UAT ensures that the system performs as expected. User Acceptance Testing is administered by the receiving jurisdiction, and vendors serve only as a resource to answer questions or address any issues. Jurisdictions will not accept and use a new voting system until they are satisfied that it has passed all UAT requirements.
e. Separate from and in addition to UAT, before each and every election, jurisdictions put their voting system through public Logic and Accuracy Testing (LAT) to ensure the system is capturing and tabulating votes accurately. Vendors are not involved in any way with LAT. Once the systems pass the LAT, they are physically secured by the jurisdiction until they are to be used.

**4) The story continues to quote Mr. Scott,** *"...the next foreign attack on U.S. voting machinery will likely be initially directed at an equipment vendor's server before migrating to county systems and voting sites...He said the malware can poison vendors' update servers with a "decimalization feature" – a program to manipulate the vote outcome as desired...Then you add a second layer to the exploit that geo-targets that malware to hit swing regions of swing states...It embeds in the touch-screens and carries through to the central (vote-counting) tabulator at the state level before destroying itself upon final tabulation..."* **This quote reveals a serious lack of understanding about how modern, air-**

b. The EAC is not "obscure." It was created as a central part of the Help America Vote Act, which was a high-profile, national response to the 2000 federal presidential election.
c. The EAC did not "reject" any specific findings, and the "experts" cited in this article are completely unnamed.
d. The EAC relies on the expertise of a cross-functional body of experts that operate in association with the National Institute of Standards and Technology, and more specifically, the EAC's Technical Guidelines Development Committee (TGDC).
e. The TGDC is also not "obscure;" all its findings and work product are publicly available.
f. Detailed information about the TGDC is available at https://www.eac.gov/about/technical-guidelines-development-committee/
g. When new systems are purchased, the jurisdiction goes through a thorough User Acceptance Testing (UAT) protocol to ensure that all software installed on the new system matches the software version that has been certified by federal and/or state authorities, and the UAT ensures that the system performs as expected. User Acceptance Testing is administered by the receiving jurisdiction, and vendors serve only as a resource to answer questions or address any issues. Jurisdictions will not accept and use a new voting system until they are satisfied that it has passed all UAT requirements.
h. Separate from and in addition to UAT, before each and every election, jurisdictions put their voting system through public Logic and Accuracy Testing (LAT) to ensure the system is capturing and tabulating votes accurately. Vendors are not involved in any way with LAT. Once the systems pass the LAT, they are physically secured by the jurisdiction until they are to be used.
i. At any time, any jurisdiction can verify that the software they are running locally is consistent with the official source code on file with the EAC to ensure the deployed configuration matches the certified configuration.
j. While there are many security features built in to the voting system (significant detail below), every jurisdiction is responsible for ensuring that no unauthorized access to the software or devices occurs before, during or after an election. Physical security measures and thorough procedures in accordance with best practices are essential (e.g. personnel security policies, strong chain of custody, numbered and logged security seals, post-election reconciliation and audits, to name just a few).

**3) The story says, referring to certification testing,** *"Such assurances offer little consolation, because such "certification" tests cannot trace malware that deletes itself after tampering with vote totals, and because the vendors' computer coding is proprietary and unavailable for public examination, said James Scott, a cyber security whiz who is advising U.S. intelligence agencies and Congress about voting security..."* **This reflects a lack of understanding of how the federal certification process works.**

https://nda.ie/Publications/Attitudes/Appropriate-Terms-to-Use-about-Disability/

**7) The story says,** *"On March 21, U.S. Homeland Security Secretary Kirsten Nielsen ended years of federal equivocation about paperless touch-screen machines."*

a. There has been no "federal equivocation" about touch-screen machines; on the contrary, they have been repeatedly accepted for use and regulated for decades.
b. Functional standards for electronic voting devices, without prohibitions on the use of Direct Record Electronic systems (DREs), include:
   i. Federal Election Commission (FEC) Voting System Standards of 1990;
   ii. FEC Voting System Standards of 2002 (VSS 2002);
   iii. The federal Voluntary Voting System Guidelines (VVSG) v. 1.0 (2005);
   iv. The VVSG v. 1.1 (2015);
c. In addition, the EAC has recently accepted the TGDC's recommendation of VVSG 2.0 Guidelines, and although those Guidelines have not yet been formally adopted, they also include standards for both paper-based and electronic devices.

**8) The story states,** *"In December 2006, a team of as many as 20 computer experts at the National Institute of Standards and Technology reported, after exhaustive testing, that they could find no way to verify the accuracy of votes cast on paperless touch-screens...In a recommendation to the Election Assistance Commission...NIST's team wrote that the machines' vulnerability 'is one of the main reasons behind continued questions about voting system security and diminished public confidence in elections.' By then, however, most of the federal grant money had been spent, much of it on tens of thousands of touch-screens."* **This is not an accurate representation of what NIST actually said.**

a. On the heels of misleading efforts by some media sources to misconstrue what NIST said, NIST issued this statement in 2006:
   i. "Recent news accounts discussing the vulnerabilities of electronic voting systems contained in the report titled Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC said NIST on its Voting Technology page, "have raised the question of whether the report's recommendations represent the official position of NIST. This draft report was prepared by staff at the National Institute of Standards and Technology (NIST) at the request of the Technical Guidelines Development Committee (TGDC) to serve as a point of discussion at its Dec. 4-5, 2006, meeting. Prepared in conjunction with the Security and Transparency Subcommittee (STS) of the TGDC, **the report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC."**

**[emphasis added]**

ii. Source: http://www.govtech.com/security/NIST-Clarifies-Import-of-Voting-Machine.html

9) **Incredibly, the story continues,** *"In 2007, rather than addressing NIST's recommendation, the Election Assistance Commission shelved it."*

a. As pointed out already, the NIST comment in question was simply a discussion point and not a recommendation. Because of prior misleading reporting, NIST had to issue a specific statement pointing that out.
b. Actual 2007 NIST recommendations are available to anyone who searches for them here: https://www.nist.gov/document-7110
c. Note that the document above is stored on a NIST website and they contain the recommended standards for all types of voting devices.

10) **The story goes on to quote an unnamed government official,** *"It was knowingly wrong for Congress to appropriate funds for new systems before better standards could be written and reckless on the part of the EAC to then vote down NIST's update to the standards."* **Once again, this is misleading and incorrect.**

a. New standards were written and adopted in conjunction with the Help America Vote Act's appropriation of federal funds. Those standards were the VVSG 1.0 (2005) guidelines.
b. Around 35 states found them sufficiently valuable and rigorous to make compliance with VVSG a pre-requisite for state certification examinations.
c. As explained already, the EAC did not "vote down" NIST's "update to the standards".

11) **The story quotes Susan Greenhalgh, policy director for the National Election Defense Coalition who called it,** *"...'scandalous' that EAC ignored NIST's warnings all those years."* **This statement does not reflect the reality of how the EAC and NIST continue to collaborate closely.**

a. NIST continues to work regularly and closely with the EAC's Technical Guidelines Development Committee, and indeed, both NIST and the EAC recently celebrated the EAC's acceptance of the TGDC's recommendation for VVSG 2.0 Principles and Guidelines: https://www.eac.gov/news/2017/05/01/eac-standards-board-unanimously-approves-the-17-core-voting-system-principles/
b. Mary Brady, Voting Program Manager at NIST, provides regular updates on the cooperative work being done between the EAC and NIST. An example is here: (note that Slide 4 is titled "Together ..Making it Happen" and refers to the partnership between several groups, including NIST and EAC).

**How can people help secure elections beyond technology?**

Election security requires people, processes, procedures and technology.

Voting system technology is an important aspect of security; however, true election security requires thoroughly trained election officials and staff upholding state-defined processes by implementing well-defined election management procedures. Election experts refer to the importance of cultivating secure election management through a combination of "people, processes, procedures and technology."

Even if a voting system uses the very latest security technology, a successful, secure election depends on people, processes and procedures as well.

Jurisdictions' election managers own responsibility for the "people" aspect of election security. These election leaders must ensure staff members and volunteers are carefully selected and properly vetted with reference and background checks. Election personnel require training (including cross-training) in the procedures and technology used to ensure accurate vote capture and tabulation. Team members should be assigned unique usernames, passwords and permissions to access only the appropriate functions within the voting system. Two people should be present for certain types of functions.

Each state establishes the "processes" aspect of election security in the form of election laws, code, rules and advisories. Local jurisdictions within each state must stay informed of these processes and adhere to them.

Responsibility for the "procedures" aspect of election security resides with jurisdictions' election managers. Local procedures document how to apply state election law, rules and advisories based on the jurisdiction's election technology. Procedures include the frequency and steps for testing the voting system's logic and accuracy for every election, chain-of-custody protocols for voting equipment, rules for who can access voting system software when, reconciliation of election results with the voter count for every election, post-election audit steps and more. The voting system vendor should assist with system-related procedures by providing effective training and comprehensive documentation.

The voting system provider holds primary responsibility for the "technology" aspect of election security – for meeting or exceeding standards the U.S. Election Assistance Commission (EAC) and other bodies maintain. The election solution provider should assist the jurisdiction's election team in optimizing the use of the system's security features, providing in-depth training and documentation.

**Is Hart involved with any election security initiatives?**

Hart is an active participant in the national conversation regarding election security and holds leadership positions in key stakeholder groups.

Voting system vendors are key stakeholders in ensuring that elections are conducted securely in the U.S. For example, major voting system vendors are engaged in a series of coordination meetings with the Department of Homeland Security (DHS) to discuss cybersecurity for the nation's election infrastructure.

Leading voting system vendors are part of a broad community of stakeholders actively participating in knowledge sharing, best practice sharing and relevant discourse on the foremost election security processes, procedures and technology.

At the federal level and within local jurisdictions, voting system vendors are engaged in learning, educating and identifying risks with the larger community on the topic of protecting the elections system.

**What organizations work with Hart and other election technology vendors to keep our elections safe?**

The resources listed below all welcome participation of the voting system community:

- **Department of Homeland Security** – voting system vendors make up the membership of a new (2018) DHS Sector Coordinating Council composed of industry representatives regularly come together with the DHS Government Coordinating Council and act as a voice on election cybersecurity. Together, these groups partner in identifying potential security risks and implementing the measures to eliminate those risks. DHS has identified elections as critical infrastructure for the U.S.
- **U.S. Election Assistance Commission** – The EAC welcomes active participation of voting system vendors in industry-wide initiatives. In addition, the EAC is the governing body that defines and regulates federal certification of voting systems.
- **National Academies of Science, Engineering, and Medicine** – NASEM welcomes active participation of voting system vendors in its meeting of the NASEM Committee on Science, Technology and Law on the Future of Voting (last held in Denver, Colorado, Dec. 8, 2017).
- **Election Center** – Election Center welcomes active participation of voting system vendors in its meetings and advisory councils. Election Center serves elections officials and elections administrators nationwide and sponsors professional education programs, including the Certified Elections/Registration Administrator (CERA) continuing education program from Auburn University.
- **National Association of Secretaries of State** –NASS welcomes active participation of voting system vendors in its events, conferences, and learning sessions on election topics – including security.
- **National Association of State Election Directors** – NASED welcomes active participation of voting system vendors in its events and conversations on elections security.

## Have questions?

CONNECT WITH US

and accurate elections for all voters.

**Is Hart technology a voting system or an election system?**

Hart makes technology that is part of the "voting system", but not the whole "election system".

"Voting system" is a term that is not interchangeable with the term "election system."

The voting system – the hardware and software used for election preparation, vote capture, results tabulation and reporting and post-election audits – is a subset of the election system. The election system encompasses a broader spectrum of election activities, including voter registration, election night reporting and more.

The full "election system" is a broad lineup of systems managed by a diverse group of election professionals from a variety of vendors, agencies, departments and functions. These elements work together to facilitate

# Supply Chain

**Where are Hart products made?**

Hart products are designed, developed, and built in the United States. All Hart products are assembled exclusively by U.S. based contract manufacturers. Hart has developed a stable, long standing network of partnerships. These partners understand the elections community and the unique requirements specific to our market. This network has been very responsive to the changes that have been occurring over the past few years.

Our primary contract manufacturer is located approximately 5 miles from Hart's headquarters in Austin and restricts access to the Hart production line to authorized personnel only. The proximity of our manufacturing