ERIC V. CALDWELL
CHIEF INFORMATION OFFICER
Brazos County Maxwell Building
205 East 27th Street
Bryan, TX 77803
ecaldwell@brazoscountytx.gov

PHONE: (979) 361-4310
FAX: (979) 361-4408

MEMORANDUM

TO: Commissioners Court
FROM: Eric V. Caldwell, Chief Information Officer
DATE: October 11, 2024
SUBJECT: Future Agenda Requests – Elections Security

On October 8, 2024, Dr. Walter Daugherity made a request to Commissioners Court asking that six items be added to a future Court agenda. The items were intended to address improvements believed to be needed in Brazos County election systems.

The Information Technology Department, Elections Administration, and Legal Counsel have considered these requests, discussed them at length internally, and have consulted with Hart InterCivic, Inc., the manufacturer of the voting system solution used by Brazos County. Below, we have listed the requests made by Dr. Daugherity and have provided our thoughts so that Commissioners Court can make informed decisions concerning these requests.

The first two requests for future agenda items read:

> *1. Direct the Elections Administrator to install monthly Microsoft antivirus definition updates on Verity Count and Verity Central computers, as required by federal regulations. (Voluntary Voting System Guidelines Version 1.0, § 7.4.2)*
>
> *2. Direct the Elections Administrator to patch known vulnerabilities in Microsoft SQL Server on Verity Count and Verity Central computers, as required by state law. (Texas Election Code§ 122.001)*

In making these two requests, it is asserted that our Hart voting system is insecure because certain updates haven't been applied. It has also been implied that this makes our voting equipment illegal.

This is our response to those assertions:

The entire premise of the argument is that our elections systems are unsafe because we haven't applied the latest Microsoft updates on our voting equipment. The Texas Election Code says in Section 122.001 "… that a voting system may not be used in an election unless the system" ...

"(3) operates safely, efficiently, and accurately and complies with the voting system standards adopted by the Election Assistance Commission."[1]

There are two volumes of voting systems standards available from the U. S. Election Assistance Commission (EAC). In Volume I, Section 2.2.1 titled Security states:

> *System security is achieved through a combination of technical capabilities and sound administrative practices. To ensure security, all systems shall:*
>
> *a. Provide security access controls that limit or detect access to critical system components to guard against loss of system integrity, availability, confidentiality, and accountability.*
> *b. Provide system functions that are executable only in the intended manner and order, and only under the intended conditions.*
> *c. Use the system's control logic to prevent a system function from executing if any preconditions to the function have not been met.*
> *d. Provide safeguards to protect against tampering during system repair, or interventions in system operations, in response to system failure.*
> *e. Provide security provisions that are compatible with the procedures and administrative tasks involved in equipment preparation, testing, and operation.*
> *f. If access to a system function is to be restricted or controlled, the system shall incorporate a means of implementing this capability.*
> *g. Provide documentation of mandatory administrative procedures for effective system security.*[2]

We meet this requirement for system security using the sound administrative practice of "Air-gapping."

The EAC and the National Institute of Standards and Technology (NIST), part of the US Department of Commerce, define an air gap as *"An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)."*[3]

The NIST standard 800-39, titled "Managing Information Security Risk: Organization, Mission, and Information System View," lists air-gaps as a form of Risk Avoidance:

[1] https://statutes.capitol.texas.gov/Docs/SDocs/ELECTIONCODE.pdf - Chapter 122. State Supervision Over Voting Systems Subchapter A. Voting System Standards, pg. 505

[2] https://www.eac.gov/sites/default/files/eac_assets/1/28/Voting_System_Standards_Volume_I.pdf - Section 2.2 Overall System Capabilities, 2.2.1 Security, pg. 2-20

https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf - Section 2.1 Overall System Capabilities, 2.1.1 Security, pg. 15

[3] https://csrc.nist.gov/glossary/term/air_gap#:~:text=air%20gap%20Definitions%3A%20An%20interface%20between%20two%20systems,through%20the%20interface%20only%20manually%2C%20under%20human%20control%29.

https://www.eac.gov/documents/2017/09/21/common-cybersecurity-terminology

> *Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk tolerance. Organizations may conduct certain types of activities or employ certain types of information technologies that result in risk that is unacceptable. In such situations, risk avoidance involves taking specific actions to* ***eliminate*** *the activities or technologies that are the* ***basis for the risk*** *or to revise or reposition these activities or technologies in the organizational mission/business processes to avoid the potential for unacceptable risk. For example, organizations planning to employ networked connections between two domains, may determine through risk assessments that there is unacceptable risk in establishing such connections. Organizations may also determine that implementing effective safeguards and countermeasures (e.g., cross-domain solutions) is not practical in the given circumstances. Thus, the organizations decide to* ***avoid the risk*** *by* ***eliminating*** *the electronic or networked connections and employing an* ***"air gap"*** *with a manual connection processes (e.g., data transfers by secondary storage devices).* [emphasis added][4]

The network connections to our voting systems are eliminated in compliance with state law and federal guidance. We also have the voting systems housed in a controlled-access location to prevent direct interaction from unauthorized personnel. The location is under video surveillance twenty-four hours a day, seven days a week.

These controls, in conjunction with our current election security plan, puts us in compliance with the EAC guidance on Voting System Security Measures – Section 1:

> *Best practices election officials use to secure the computer include:*
>
> - *Keeping it in a location with restricted access (locks with documented entry, key card systems) and video surveillance*
> - *Never connecting it to the internet or other external network*
> - *Providing users unique logins, strong passwords, and access to the minimum functions needed to perform their duties*
> - *Routinely reviewing audit logs of all users who log onto the computer and actions they perform*
> - *Validating the computer's software has not been modified*[5]

The third request made to Commissioners Court for a future agenda item - to engage an independent CPA to investigate the discrepancy in election results from November 2020 - will be addressed separately.

The fourth request made to Commissioners Court for a future agenda item reads *"Direct the Elections Administrator to stop using computers for Verity Count and Verity Central which the Texas Secretary of State website says are uncertifiable since they possess the capability to connect to a network, namely, an integrated Network Interface Controller with an RJ-45 network jack plainly visible on the back of these computers, similar to the one circled in [an attached] picture."*

[4] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf - "Managing Information Security Risk: Organization, Mission, and Information System View, Risk Response, page 42

[5] https://www.eac.gov/sites/default/files/electionofficials/security/Voting_System_Security_Measures_508_EAC.pdf

This request asserts that our Hart systems are 'uncertifiable' because they possess an integrated Network Interface Controller with an RJ45 port on the back of the device.

It is correct that the Verity Count and Verity Central devices have an RJ45 port. However, the existence of this port does not mean that they are 'uncertifiable' by the Texas Secretary of State. The Secretary of State (SoS) website states that **Hart InterCivic** is certified by the EAC and approved by the SoS. Therefore, the system cannot be 'uncertifiable' because the system is explicitly listed as certified. See the below section taken directly from the SoS page on voting equipment.

1. Certification of Voting Systems

- *All voting systems must be certified by the U.S. Election Assistance Commission (EAC), created by the Help America Vote Act (HAVA) in 2002.*
- *The Texas Election Code requires all voting systems to be approved by the Secretary of State before they may be used in any Texas election.*
- *Currently, only two voting system vendors are certified by the Texas SOS:*
    - ***Hart Intercivic** - Austin, TX*
    - ***Election Systems & Software (ES&S)** - Omaha, NE*[6]

The point of contention is a section on that same page, again taken directly from the website:

2. Key Facts on Security of Voting Machines

1. ***Voting machines in Texas are not connected to the internet.** In order to be certified in Texas, the machines cannot even have the capability of connecting to the internet. Electronic pollbooks certified by the Texas SOS are connected to the internet, but they are never connected to any device that casts or tabulates votes.*
2. ***Only software certified by the Texas SOS can be loaded on voting equipment.** As an added security measure, Texas law requires software to go through a hash validation process to verify that the source code of any voting software was not altered in any way.*
3. ***All voting machines are required to be tested for logic and accuracy three times**-twice before each election, and once immediately after.*[7]

The relevant section to this discussion is item 2, subitem 1 *"… the machines **cannot even have the capability of connection to the internet**."* [emphasis added].

The existence of an RJ45 port doesn't mean that a device can connect to the internet. That requires hardware, software, and network protocols to work together to make that connection possible. While the hardware exists on the device, the necessary software and network protocols

[6] https://www.sos.state.tx.us/about/newsreleases/2022/092322.shtml

[7] Ibid.

are disabled, mitigated and/or removed per the vendor, the SoS office, and the EAC certification process.

The following is a statement from the vendor regarding protections to prevent access to the internet. This is in compliance with the EAC certification process and meets the standards for the Texas SoS.

1. *For all standalone products, there are no active network ports. All ports are disabled during manufacturing.*
   a. *Additionally, the workstation's firewall is configured to block all network activity.*
2. *For client/server configurations, Verity workstations are connected to a dedicated, isolated network switch. With only Verity workstations connected to this stand-alone network, internet access is impossible.*
   a. *Furthermore, these workstations are explicitly configured to operate only on isolated, internet-inaccessible networks.*
   b. *Each workstation's firewall is configured to block all unnecessary protocols and ports.*
   c. *For necessary communication, certificate-based authentication is required to establish an encrypted channel.*
3. *All configurations on each workstation are protected by full-disk encryption, which denies access to operating system configurations and features.*
4. *All configurations on each workstation are protected by kiosk mode, which further denies access to operating system configurations and features.*[8]

A link to the Verity system's certification by the EAC is included below. The verification process was completed by a third party (SLI Compliance in 2020):
https://www.eac.gov/voting-equipment/verity-voting-25

The fifth request made to Commissioners Court for a future agenda item reads *"Authorize an independent hash validation which does not use Hart software to check Hart software."*

We agree that the validation should use tools that are not produced by Hart, but do not believe action is required by the Court. We do NOT use Hart provided software to perform hash validation. The county uses a third-party tool, Hash Compare 3.0, made by SecurityXploded. This tool was tested and meets the county's needs for doing hash comparisons.

The sixth request made to Commissioners Court for a future agenda item reads *"Authorize an independent cybersecurity inspection of all voting equipment, including checking for network logins. For example, who is the actual person who logged in as cdr12312? Who is the actual person who logged in as harttech?"*

[8] Email dated Thursday, October 10, 2024 4:17 PM, From: Peter Lichtenheld (Hart), To: Trudy R. Hancock (Elections Administrtor)

An independent third-party review was conducted in 2019 by AT&T. However, they did not review the equipment used to cast or count votes, because a review of the equipment would have led to changes to the system thereby making the equipment illegal to use in an election according to state law and the SoS. Lastly, to address the two accounts mentioned: Cdr12312 is a former employee of the Brazos County Information Technology Department. One of their many job responsibilities was to administer the Hart systems in support of the Elections Administrator. They no longer work for Brazos County and their account was disabled after they left employment. Actions taken by this account are in line with proper election processes and procedures. Harttech was an account used for initial setup. It is also disabled, and there is no evidence of any actions taken by this account once the system was setup.

In conclusion, we appreciate the concerns of Dr. Daugherity regarding the security of elections in Brazos County, and we hope that this information will help to allay those concerns. We also hope that this information will help the Court to make informed decisions regarding elections security, infrastructure, and processes in Brazos County.