COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

ELECTRONIC POLL BOOK EVALUATION

CIVIX EPOLLTAB 1.2

Issued By:

Leigh M. Chapman

Leigh M. Chapman
Acting Secretary of the Commonwealth
January 13, 2023

1 INTRODUCTION

Pennsylvania's voter registration law, Act 3 of 2002 (Act 3), 25 Pa.C.S. §§ 1101, et seq., requires that the poll book or district register "shall be in a form prescribed and approved by the Secretary" for both paper and electronic poll books, (25 Pa. C.S. §1402(b)(2)). Pursuant to the request of Civix, the Department of State (Department) evaluated the ePollTAB 1.2, Electronic Poll Book (EPB) to ensure that the system complies with all the applicable requirements of Act 3, including the regulations implementing Act 3 of 2002, 4 Pa. Code §§ 183.1 et seq., and the Pennsylvania Election Code, 25 P.S. §§ 2601, et seq., and therefore can be used in Pennsylvania elections. The evaluation consisted of a system demonstration via video conference conducted by Mike Brown, Operations Director representing Civix, followed by in-person demonstration at Commonwealth Department of State Office, email communications and conference calls with Civix personnel, and documentation review. Benjamin Ohana, DevOps and Solutions Architect, John Alexander, Director of Development, and John Morrison, Product Director, also attended the offsite demonstration representing Civix. The system demonstration video conference occurred on July 22, 2022, and the in-person demonstration was conducted on August 16, 2022. Sindhu Ramachandran, Voting Systems Analyst; Matt Ruch, Voting Systems Analyst, representing the Bureau of Elections; Bryan Reed, Division Chief, Kerry TenHuisen, Portfolio Manager, representing the Office of Information Technology; and Gregory Darr, Assistant Counsel, Office of Chief Counsel attended the demonstration representing the Secretary. The initial demonstration was completed via video conference to enable an opportunity to demonstrate the system to Department staff and thus gather any specific requirements that needs configuration before the in-person demonstration.

2 ELECTRONIC POLL BOOK OVERVIEW

The ePollTAB 1.2 EPB demonstrated for use in Pennsylvania included the following components:

ePollTAB 1.2 – The ePollTAB 1.2 is a software application installed on a customer chosen hardware device that allows poll workers to perform the polling

place activities typically performed using a printed paper poll book. Refer to *Attachment A* for a list of compatible hardware devices represented in the application for approval.

CenterPoint 1.2 – CenterPoint is a platform that supports the management functions of the EPB system. CenterPoint allows the county election officials to prepare the voter and precinct data for use on Poll Pads. The system allows the user to configure an election, import data extract from a voter registration (VR) system, build the package to be deployed to polling place devices, deploy the election, manage post-election activities like reconciliation reports and vote history files, and serves as the platform for managing user access and roles. Jurisdictions can create templates for elections identifying the layouts of the polling place devices and data is uploaded and election is deployed each polling placing device.

Merlin – Manages encryption and network communications. ePollTab devices and CenterPoint communicates to Merlin and thus Merlin provides a security hub sync point to enable precinct and vote center connections for multiple poll books from a single location to a managed web service sync point. Merlin receives the changes in an audit log format which it applies to its internal database and then tunnels it to either the Local Area Network connected devices or Wide Area Network devices depending on the connectivity configuration. The use of only transmitting the required data to identify the changes keeps the transmission payload to only the required items and also reduces the data in motion.

Refer to *Attachment D* for a list of all the items in the ePollTAB EPB system case.

Deployment of ePollTAB and CenterPoint software systems are handled, managed and controlled using Meraki MDM to ensure that only permitted actions are allowed on the devices and only tested combinations of operating system and software can be run on EPB devices and CenterPoint.

3 EVALUATION APPROACH

To evaluate whether ePollTAB 1.2 EPB can be successfully used for elections in the Commonwealth of Pennsylvania and meets all the requirements mandated by Act 3 and the Pennsylvania Election Code, the following approach was used: (1) System Demonstration; and (2) Documentation Review.

The Department requires a System Demonstration to examine and confirm on a field-ready system that the EPB satisfies all the statutory requirements. The demonstration also allows the Department to gain a broad understanding of the system capabilities. The documentation review consisted of analyzing the system specifications, user manuals, state certification and third-party test reports pertaining to the Civix system.

Electronic poll books are heavily configurable distributed systems, typically consisting of networked tablets or laptops used at polling places to check-in voters. They work in conjunction with a central server performing the management functions, which include preparing the election data, performing voter history updates, and monitoring deployed devices at polling places. The documentation review was conducted to confirm that the system can be efficiently used for elections in the Commonwealth of Pennsylvania and to aid in deciding the EPB connectivity configuration to be approved for use in Pennsylvania.

4 EVALUATION PROCEDURES

4.1 System Demonstration Review

A Civix representative demonstrated the ePollTAB 1.2 system on July 22, 2022, via a teleconference, followed by an in-person demonstration on August 16,2022. The demonstration included a polling place capability walkthrough of the ePollTAB 1.2 application used at the polling place, a discussion of preparing and loading the data to the Poll Pads, and an explanation of the system security features. Civix used the test data supplied by the Department for the in-person demonstration.

The purposes of the demonstrations were to (a) validate that the system complies with Pennsylvania's statutory requirements for poll books; (b) discuss the overall capabilities of the system; and (c) to evaluate the system security posture and level of

compliance with the Commonwealth Information Technology Policies (ITPs) outlined in *Attachment C* of this report.

4.2 Documentation Review

The Department requested and completed a thorough review of the following documentation from Civix:

1. System Specifications
2. Hardware/Software/Peripherals/Additional Equipment Requirements
3. Technical Data Sheet
4. User Manual
5. Usability Reports
6. Security and Penetration Testing Reports
7. Test Reports from other states using the system

5 EVALUATION RESULTS

5.1 System Demonstration Review Results

1. Conformance to statutory requirements - The vendor successfully demonstrated that the ePollTAB 1.2 EPB system conforms to the statutory requirements outlined in Pennsylvania law. The demonstration proved that the system can be configured to meet the statutory requirements. See *Attachment A* for the list of statutory requirements discussed and validated during the demonstration.
2. Review of system capabilities - The Department reviewed the overall system capabilities during the demonstration and documentation review. See *Attachment B* for a summary of the demonstration discussion points.
3. Level of Compliance with Commonwealth IT policies and system security posture – The Department provided Civix with a copy of the Commonwealth of Pennsylvania IT policies relating to the security of distributed systems and network connectivity. The Department also provided Civix with a

questionnaire to evaluate the system security posture, which was completed and submitted as part of the evaluation request. The written response to the questionnaire and the security discussion with the Civix team during the demonstration allowed Department staff and election security partners to understand the security features of the system. See *Attachment C* for a summary of the answers submitted by Civix.

5.2 Documentation Review Results

Department staff analyzed the documentation provided by Civix to understand the system capabilities in detail. The review of the documentation allowed the Department to understand in depth the functionality of the system and further assess the security and accessibility properties of the EPB system.

The demonstration and documentation review determined that ePollTAB 1.2 consists of devices installed with ePollTAB 1.2 application configured as polling place devices to perform voter check-in activity at the polling place, and CenterPoint hosted on a physical computer located at the county to perform administrative functions. The system can allow the following modes of configuration, but these can also be deactivated where not permitted:

1. A Wide Area Network mode where data flows continuously between polling place devices across the county, with CenterPoint and Merlins implemented at different polling places.
2. A peer-to-peer on Local Area Network communication mode where the devices at a polling place communicate to each other via Merlin. This configuration allows voter check-in data to sync up in a polling place, thus allowing the use of multiple Poll Pads at a polling place.

The Department staff analyzed the connectivity configurations discussed during the demonstration in conjunction with the documentation provided and existing Department test protocols for Electronic Poll Books to determine the connectivity approved for use in Commonwealth of Pennsylvania, which minimizes the security

risks and maximizes the benefits in moving to an EPB solution.

5.3 Observations

Department staff noted the following as part of the demonstration and documentation review:

1. EPollTAB 1.2 uses software configuration features to determine the final functional behavior of the system. In addition to the demonstration and subsequent analysis and evaluation performed demonstrating that the system can be configured to satisfy all the statutory requirements, the Department also requires documentation after purchase confirming that the system setup complies with the approved configuration.
2. EPollTAB 1.2 includes configurable functionalities added to be system executables to satisfy certain jurisdictional specific requests.
3. The deployed system security posture will depend on the parameters selected during setup. This will necessitate validating the configuration during and after setup to ensure that the system is configured in a secure manner.
4. EPollTAB 1.2 when deployed in live Wide Area Network mode can communicate with the server located outside of the polling place and transmit transactional and operational data throughout Election Day to the CenterPoint server. The Wide Area Network mode maintain a communication channel between the polling place and the server for the entire time the polls are open on Election Day. These can be disconnected, which is the only approved setting during polling hours in Pennsylvania.
5. The data from Statewide Uniform Registry of Electors (SURE) system is prepared for loading on polling place devices using the CenterPoint system. The data preparation process is reconciled via a high-level onscreen summary of the records processed on CenterPoint, but the prepared data will need to be validated for accuracy and completeness after loading to the polling place devices to avoid any data inconsistencies on Election Day.

6 CONDITIONS FOR APPROVAL

Based on the evaluation, the Secretary of the Commonwealth of Pennsylvania approves ePollTAB 1.2 subject to the following conditions:

A. The polling place devices in operation at a polling place **must not** be configured to communicate to the CenterPoint server during the polling hours on Election Day. The devices in operation at a polling place can communicate only to each other to synchronize voter check-in data between each other at the polling place during the polling hours. Any data transfer required between the CenterPoint system and polling place devices may only happen outside of polling hours. Therefore, the polling place devices must be configured to prevent communication with the CenterPoint server during polling hours.

B. The polling place devices at an individual polling place communicating with each other must be configured and managed in a secure manner and may never connect to a publicly accessible network. The network at the polling place must be a "closed network" allowing only components of the EPB system to connect, and encryption must be enabled. The security settings must prevent other devices from detecting and connecting to the network at the polling place.

C. Any components which are/were part of the EPB system, including removable media, must not be connected to the Electronic Voting system. This includes, but is not limited to: PEB encoders and Voter Access Cards encoded on the EPB systems; USBs; SD cards; printers; CDs; etc.

D. Jurisdictions implementing ePollTAB 1.2 EPB system **must not** use the driver's license or ID card bar code scanning capability to check in voters. This is to avoid voters being asked for presentation of identification when not required by law. Counties must implement the system with the bar code scanning option disabled. The system must not present poll workers the option of checking in voters by scanning an identification card with bar code.

E. Jurisdictions printing barcodes at check-in to activate ballot marking devices must ensure that the specific integration details are demonstrated and technical documentation

about the integration is submitted for evaluation to the Department of State. There was no demonstration of the bar code printing functionality.

F. Jurisdictions must ensure that the system does not capture the poll worker Social Security Number (SSN) as part of the add poll worker workflow.

G. Portable media used to transfer files between any components of the EPB system must be new, unmodified, and not refurbished. Alternatively, removable media that is being reused must be fully reformatted before each election. All removable media used for elections must be managed with proper chain of custody and administrative safeguards to protect against disclosure, theft, or damage.

H. Any unused ports in the polling place devices must be sealed with tamper-evident seals. The polling place device case also must be locked and sealed.

I. Counties purchasing the ePollTAB 1.2 EPB system must work with Civix and the Bureau of Elections to do the following:

    1. Implement ePollTAB 1.2 EPB system in a manner that satisfies all statutory requirements outlined in Act 3 of 2002 and the Pennsylvania Election Code. The parameter configurations and the text of informational messages must be approved by the Bureau of Elections.
    2. Implement ePollTAB 1.2 EPB system in a secure manner that complies with applicable county and Commonwealth IT policies and any directives or guidance published by Department of State Bureau of Elections. The system configuration, connectivity setup, password configurations and password management policies must be approved by the Bureau of Elections; and
    3. Implement ePollTAB 1.2 EPB system with sound administrative practices and proper chain of custody in the same manner as counties deploy Electronic Voting Systems.

J. Counties implementing ePollTAB 1.2 must change all default passwords during implementation. County election officials must implement processes to confirm and maintain records that default passwords were changed before fielding the system. The proof must be documented using export of the system log files whenever possible. A

screenshot of the password change action performed at the county elections office or otherwise documenting the password change during acceptance testing can meet this condition. County election officials with administrative access on CenterPoint host must take proper precautions for password management and protection. The passwords and permissions management must, at a minimum, comply with the password requirements outlined in NIST 800-63. This publication can be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html.

K. Counties must work with Civix to ensure that the polling place devices are configured in kiosk mode or Guided Access Mode. The devices must be hardened with only the required software for the EPB system. No additional software applications or utilities shall be installed on the devices being used at the polling place.

L. Jurisdictions implementing the ePollTAB 1.2 EPB system must keep an inventory of all the device identifiers deployed in the county. The systems must be audited at the beginning of the Election cycle for any required maintenance. Any devices decommissioned, returned, or otherwise disposed of at the end of a lease or end of useful life must be permanently erased of any software and voter data. Counties must implement processes to ensure that the "clean wipe" is validated, documented, and maintained for audit purposes. Best practices on equipment sanitization are documented in publication NIST SP 800-88r1 and can be accessed at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

M. Counties must have a contingency plan to ensure that an election will not be affected should any component (including connectivity and power supply) of the EPB system fail due to malfunction, cyber incident or other cause on Election Day. The contingency plan must ensure that no "check in" information is lost. The contingency plan must be reviewed and approved by the Bureau of Elections. At a minimum, the contingency plan must ensure the availability of a full voter list and a process for maintaining and reproducing a list of voters who have already checked in if the EPB fails during voting hours.

N. Counties purchasing the ePollTAB 1.2 must work with the Bureau of Elections to

decide what portion of the data from the Statewide Uniform Registry of Electors (SURE) system can be shared with the vendor. The counties shall not allow the vendor to run any data extraction utilities against the SURE database/system. Any data transfer must happen via a file extract and secure file transfer process and must be encrypted. The voter data extract must not contain any additional data elements than what was shared during the evaluation. The data elements and sharing mechanism must be approved by the Bureau of Elections. Counties must ensure the accuracy of data loaded to the EPB system and maintain appropriate reports as necessary for auditability.

O. Counties purchasing the ePollTAB 1.2 EPB must work with the Bureau of Elections to finalize the process of voter history updates. Civix must be able to adhere to the extract format and timing of the update suggested by SURE system administrators.

P. Civix must notify the Department of State in writing of any changes made to ePollTAB 1.2 EPB system, including software, hardware, or configuration and present the system for approval before use in elections. This includes any changes to the software of the EPB system and to the environment of the EPB system, including but not limited to Civix's development locations, cloud service vendors, or data center locations, for example.

Q. Civix must escrow a copy of the code, trusted build, any verification/identification software used and installation instructions for safekeeping to the Commonwealth of PA and add the Commonwealth as a beneficiary to any Escrow accounts they have for safekeeping of the ePollTAB 1.2 EPB code.

R. Civix must provide fully prepared and version-controlled user and system manuals for counties purchasing the EPB. The manuals must clearly identify each user-configurable parameter. Copies of the final user manuals and any subsequent updated user manuals must be submitted to the Department before sale of the product or any subsequently approved product upgrades in Pennsylvania.

S. Counties must perform a thorough evaluation and User Acceptance Test of the EPB system before purchase. This test should include demonstrations of all expected activities occurring as part of the election, including interactions with the SURE system.

This approval is based on a demonstration by the vendor and documentation reviews. Demonstration by the vendor cannot be considered equivalent to testing.

T. Counties implementing the ePollTAB 1.2 must work with Civix to define and implement policies on data retention and archiving of the EPB system, including external servers and any removable media. Any election data stored on devices outside of the county network must be deleted and/or archived to physical media with access control as soon as it is no longer required, or no later than ninety (90) days after Election Day. Voter data shared with the vendor must be tracked and deleted to avoid data breaches. Counties must retain, as required by law, archived copies of data sent and received from the vendor for audit purposes. Civix must keep audit logs of every data access event and make those audit logs available for inspection by the counties or the Bureau of Elections, upon request.

U. All jurisdictions implementing the ePollTAB 1.2 must carry out full Logic and Accuracy testing prior to every election on each device and maintain records of this testing. The Department recommends creating a county-specific plan for Logic and Accuracy testing that includes all peripherals and anticipated check-in scenarios on Election Day, including any integrations. The vendor-supplied Logic and Accuracy checklist should be used as a reference but must not be accepted in lieu of a county-specific plan.

V. Civix must provide audit log specification documentation to the Bureau of Elections and counties purchasing ePollTAB 1.2 system. The county election officials and IT personnel must work with Civix to fully utilize and optimize the system-logging capabilities. The county must be able to identify and gather logs that provide audit trails of the election data preparation and transactions at the polling place and logs that aid in identifying and managing security incidents, fraudulent activities and operational problems. Processes must be implemented to harvest and safekeep the logs after each election for future analysis and review. The log files must be extracted and saved in a manner that allows identifying the device from which the logs files were extracted. The EPB log files must be retained for five (5) years in accordance with the statutory

retention period for poll books.

W. Civix must ensure that future releases of the software with enhancedsecurity features are presented for approval to Department.

7 RECOMMENDATIONS

The Secretary makes the following recommendations to the counties purchasing the ePollTAB 1.2 EPB system:

1. Counties should consider using the EPB in pilot mode during its first use in an election, in conjunction with printed poll books. This allows the jurisdictions to ensure that all appropriate checks and balances are in place before using the EPB system in full production mode. For larger counties, the county should also consider phased implementation to mitigate any unforeseen issues that may arise during implementation.
2. The Secretary urges counties to ensure that all poll workers and election officials receive appropriate training and are comfortable using the EPB. The training activities should include, but not be limited to hands-on training on devices to perform election set up and operations at a polling place, and cyber hygiene practices and procedures for detecting cyber-attacks. The training should ensure that poll workers and election officials can detect any warnings that signal cyber-attacks and immediately respond to them. Involvement of poll workers during the implementation project from start to finish with onsite trainings at the polling place is also recommended. Civix must work with counties to ensure that all training materials are updated as required and maintained for training activity before each election.
3. Counties using EPBs should implement processes of reconciliation at the open and close of polls to avoid any data discrepancies. Checklists should be developed for poll workers to ensure compliance with all requirements and to reduce the chance of human error. Counties should also work with Civix to produce quick reference cards and/or help files for use at the polling place on Election Day.

4. The Secretary recommends that counties purchasing the ePollTAB 1.2 EPB system perform proof of concept testing onsite at all polling places to ensure peer-to-peer connectivity and power supply availability. The Secretary further recommends that the test is conducted with a test system using components of the same make, model, and configuration as that being used on Election Day.
5. Counties using the ePollTAB 1.2 EPB system should work with Civix to develop and implement a plan that recognizes the possibility of a data breach or cyber-attack on the EPB and prepares a mechanism for completing election activities. The plan should detail processes and procedures to be followed by poll workers and election officials in the event of a cyber-attack.

8 CONCLUSION

Based on the demonstration, documentation review, and consultation with the Department staff, the Secretary of the Commonwealth concludes that the Civix ePollTAB 1.2 EPB meets all the applicable requirements set forth in Act 3 of 2002, the Pennsylvania Election Code, the voter registration law, and related regulations, and can be used for checking in voters during elections, provided that all of the conditions listed in Section IV of this report are met.

Attachment A – Statutory Requirements

Requirement	Demonstrated
The computer list shall be in a form prescribed and approved by the Secretary. (25 Pa. C.S. §1402(b)(2)).	Yes
Form of the Electronic Poll Book:	
Each screen of the EPB shall contain the name of the county. (25 Pa.C.S. § 1402(b)(2)).	Yes
Each screen of the EPB shall contain the election district. (25 Pa.C.S. § 1402(b)(2)).	Yes
Each screen of the EPB shall contain the date of the election. (25 Pa.C.S. § 1402(b)(2)).	Yes
Each screen of the EPB shall contain the date and time the list was prepared. (25 Pa. C.S. § 1402(b)(2)).	Yes
Content of the List:	
For each election district, the EPB shall contain an accurate list of the names of the registered electors- alphabetically by last name. (25 Pa.C.S. §1402(b)(2) and 1402(c)).	Yes
Poll workers must have access to the list at all times so that voters can be checked in without interruption. The Electronic Poll Book should provide for the following relating to data recovery and adequate contingencies should one or more elements of the Electronic Poll Book fail: • Memory Redundancy • Data Preservation • If the contingency for Electronic Poll Book failure is the printing of paper poll books/precinct lists from the EPB, the EPB must provide for the printing of a paper poll book AND a copy of the list of registered voters within the precinct. **Demonstration Comments:** EPB system keeps the data during operation on the hard disk of the devices and also transmits the data to Merlin. Merlin also holds all data and applies the changes transmitted by devices or CenterPoint to its internal database. Data redundancy at a polling place can be maintained by having a Merlin or multiple devices in a polling place and having the check-in data synchronized between them. Reports can be configured, exported, and saved to preserve data at any point in time.	Yes

The EPB must prevent multiple "check-ins" by the same voter. **Demonstration Comments:** The system identifies an attempt to check in an already checked in voter. The polling place device displays an indication of the original check in. The system can be configured for the poll worker to take additional actions like cancelling the check in, reprinting the voter slip, etc. In an environment where there are multiple polling place devices are connected, data syncing between the devices must be functioning to ensure multiple "check ins" are prevented on different devices.	Yes
A legible digitized signature for each registered elector. (25 Pa.C.S. § 1402(b)(2)). The official digitized signature for each registered elector must be obtained from the Statewide Uniform Registry of Electors (SURE) and it must be displayed in such a manner as only the poll worker can see the official signature at the time a voter is signing the EPB.	Yes
Street address of each registered elector. (25 Pa.C.S. § 1402(b)(2)).	Yes
Political party designation of each registered elector. (25 Pa.C.S. § 1402(b)(2)).	Yes
Suitable space for insertion of the signature of the registered elector. (25 P.S. § 3050(a.3); 25 Pa.C.S. § 1402(b)(2)).	Yes
Suitable space for insertion by the proper election official of the number and letter of the stub of the ballot issued to the registered elector or the registered elector's number in the order of admission to the voting systems. (25 P.S. § 3050(a.3); 25 Pa.C.S. § 1402(b)(2)).	Yes
Suitable space for insertion of the initials of the election official who enters the record of voting in the district register. (25 P.S. § 3050(a.3); 25 Pa.C.S. § 1402(b)(2)). If the EPB is designed in such a manner as it provides for unique login credentials for each election official, this requirement can be satisfied by a system-generated audit report that identifies by unique election official ID which voters were checked in by that election official. **Demonstration comments:** The poll worker login captures and identifies the the poll worker performing the check in.	Yes
Indication of whether the elector needs assistance to vote and, if so, the nature of the disability. (25 Pa.C.S. § 1402(b)(2)).	Yes
The date of birth of the registrant. (4 Pa. Code § 183.11(b)(4)).	Yes
The SURE registration number of the registrant. (4 Pa. Code § 183.11(b)(5)).	Yes

The following elector's affirmation must appear above the signature area: "I hereby certify that I am qualified to vote in this election." (25 P.S. § 3043).	Yes
An identification of whether the registrant's status is active or inactive. (25 Pa.C.S. § 1901(c); 4 Pa. Code § 183.11(b)(6)).	Yes
Voter Status Flags required by the SURE system:	
For voters who are "Inactive," affirmation is required. (25 Pa.C.S. § 1901(c) and (d)(3); 4 Pa. Code § 183.11).	Yes
"ID Required" – identification of whether the voter needs to present voter identification. An elector who appears to vote in an election district for the first time must present valid voter identification. (25 P.S. § 3050(a)).	Yes
"Absentee or Mail-in Ballot" – An elector who voted an absentee or mail-in ballot is ineligible to vote in the municipality on Election Day, although he or she may vote by provisional ballot if the district register does not show that the elector voted the absentee or mail-in ballot and may vote by regular ballot if the ballot and envelope are remitted, and the voter signs the required declaration. (25 P.S. § 3146.6(b) and § 3150.16(b)).	Yes
"Must vote in person" – Identification of whether the voter needs to present voter identification if the elector votes for the first time by mail. (Federal: 52 U.S.C. § 21083(b)).	Yes

Attachment B – Functionalities

Specific “check in”/voter handling Scenarios demonstrated:

a) Provisional Ballot: The process for issue of a provisional ballot.
b) Voter who was issued an Absentee /Mail-in Ballot: The workflow configuration capabilities on the EPB when voter is issued an absentee/mail-in ballot using the test data supplied by Department.
c) Cancel Check in: The process for cancelling an incorrect check-in and the requirement for elevated access privileges for the function.
d) Reissue Ballot: The process of re-issue of a ballot for a spoiled ballot.
e) Inactive Voter Check in: The EPB system was configured with the appropriate workflow that allows the poll worker to identify an Inactive voter and handle the affirmation requirements.
f) Redirecting a voter to the correct polling place: The system capabilities for redirecting a voter to the correct polling place.
g) Search/Lookup voter Capabilities of the EPB: The EPB system voter lookup capabilities and usability.
h) Identifying a Duplicate check-in: The system prevented the same voter from checking in multiple times.

Usability/User Interface Discussion - The following capabilities/functions of the EPB system was demonstrated:

a) Set up and Procedures for setting up the Field System/Poll Pad.
b) Poll worker ability to access the system and login.
c) Screen navigation capabilities.
d) Languages Supported by the system.
e) System power up and shutdown procedures.
f) System help availability.

Security and Chain of Custody

a) Password configuration on tablet: The password configuration capabilities of the EPB system were discussed.
b) Voter Signature pad information: The information displayed to the voter on the signature pad for the voter to sign using the stylus was displayed and demonstrated. The demonstration showed that the voter will not be able to see the signature on file when signing on to the EPB.

Attachment C – Commonwealth of Pennsylvania IT Policy Evaluation

This attachment summarizes the IT policy evaluation submitted by Civix as part of the approval process. The Department provided Civix with a questionnaire that allows Department staff to understand the system security posture. Civix submitted answers to the questions and this attachment describes those answers at a high level. The Department also discussed system security during the demonstration events. The direct answers or a summary is documented in this section of the approval report.

Terminology used –

Field System – Part of the electronic poll book that is used in polling place to check in voters.

Management System - The component of the electronic poll book that performs the centralized configuration, deployment and upload/download of data. Any devices that are part of the electronic poll book system but are not located at the polling place performing check in functions must be considered here. Examples include data preparation servers, pass thru servers, etc.

ITP-SEC001. The intention of this policy is to ensure that any systems under the control of the agencies that have the potential for introducing a virus or other malicious program onto the commonwealth network are protected by the referenced security agent software.

Q: What Anti-Virus protection software do you use and/or recommend for Field System?

A: Windows Defender. No connection to the Internet only connections to CenterPoint through Merlin.

Q: What Anti-Virus protection software do you use and/or recommend for Management System?

A: Windows Defender.

Q: What Host Intrusion Prevention software do you use and/or recommend for Field System?

A: Windows Intrusion Prevention through Defender

Q: What Host Intrusion Prevention software do you use and/or recommend for Management System?

A: Windows Intrusion Prevention through Defender.

Q: Do you have any process to monitor systems for possible intrusion attempts and for indications of compromise?

A: Pollbooks are kept in an offline mode during most of their lives. When they are connected to the Merlin secure network for pollbook-to-pollbook communication the network is monitored.

Q: What support/escalations/processes do you have to inform and mitigate your clients about any detected intrusion?

A: Civix operate a tiered ticket management systems to facilitate support and escalation processes in an ITIL 4 manner. The support desk is operational 24/7/365 days a year and escalation processes are defined within the end user licensing agreement for the pollbook system.

ITP-SEC004. Web application firewalls address the needs of limiting Internet attacks and monitoring of Web applications located in the commonwealth. This Information Technology Policy (ITP) establishes the policy and enterprise-wide standards for web application firewalls.

Q. Address any relevant firewall configurations.

Civix provided the firewall restrictions in place.

ITP-NET001. The purpose of this Information Technology Policy (ITP) is to establish enterprise-wide standards for Wireless Local Area Network (LAN) Technology and their secure usage in a production environment.

Q: Explain the connectivity configurations allowed for the Electronic Poll Book. Provide any diagrams or documentation as applicable.

Civix provided the allowable configurations and represented the architecture as it relates to the networking functionality.

ITP SEC019. This Information Technology Policy (ITP) addresses the policies and procedures for the identification of, and safe transmittal, transport, and storage of, commonwealth electronic data. There are many forms of electronic records within the commonwealth which require special treatment and/or heightened protections. These types of electronic records, known as "C" classification records, are defined below. Commonwealth employees and contractors must identify these electronic records and protect this information from improper disclosure.

ITP SEC031. The purpose of this Information Technology Policy (ITP) is to improve the confidentiality and integrity of data in transit by prescribing the use of encryption.

Q: What encryption levels and protocols do you employ for any transfer of data?

A: AES-256 encryption is used for all data communications between tablets, Merlin and Centerpoint. EPollTAB-to-Merlin-to-ePollTAB communications is encrypted to 256 AES standard with a unique crypto key for every election generated by the Administration Console. All data is treated as sensitive and critical to the operation of the poll book.

Q: What steps do you take to track and delete any intermediate files created as part of the electronic data preparation process?

A: All temporary files used as part of the intermediate process for preparation created and used by ePollTAB suite are encrypted and are cleaned up at every an active pollbook is loaded or unloaded or when the application is launched.

ITP SEC016. This ITP establishes an enterprise-wide policy for the identification of an Information Security Officer.

Q: Who is your organizations formally appointed point of contact for security coordination? Please provide any policies you have describing the duties.

Civix provided the designation and name of the person who serves as point of contact for security incidents.

ITP SEC020. The purpose of this Information Technology Policy (ITP) is to improve the confidentiality and integrity of data at rest by requiring the use of encryption.

Q: What encryption methods do you use for data at rest in the Electronic Poll Book System?

A: All data is encrypted at rest to AES-256.

ITP-SEC024. This Information Technology Policy (ITP) establishes standard policies, procedures and standards related to the reporting and managing cyber security incidents.

Q: What procedures do you follow for reporting and managing cyber security incidents? Would you be able to provide with any support needed for complying to ITP-SEC024?

A: Yes, Civix have a fully operational Cyber Security Tower to provide security monitoring, configuration management including incident response management and monitoring.

Q: Do you have policies to continually perform security assessments of your software applications and facilities? Are these assessments available for review?

A: All major releases involve a software independent third party through a CREST approved penetration tester. All code is reviewed for pull requests.

Q: Have you ever had a data breach in your organization? If so, please provide a brief description of the steps that were taken upon identification of the breach?

A: No data breaches have been experienced at Civix.

ITP-SEC025. This policy provides guidelines for the exercise of agency discretion in creating policies and procedures on the proper electronic use and disclosure of Personally Identifiable Information (PII).

Q: What security measures does your organization regularly use to protect PII from clients? Do you comply with ITP-SEC025 policy attached? (Proper Use and Disclosure of Personally Identifiable Information (PII)? Is there a policy document that can be shared?

A: All data is encrypted and only held for the relevant amount of time and disposed of using NIST approved data erasure processes and tools. All data used in demonstrations, testing and support are generated and not using any customer data.

Q: Do you use any Threat Modeling/Threat identification exercise as part of the application design? If so, please provide details.

A: The ePollTAB suite is designed to mitigate risk from various threat actors performing actions against the application, its network, the Wi-Fi or wired networks with a number of threats scenarios investigated, modelled and mitigated.

ITP-SEC007. The purpose of this Information Technology Policy (ITP) is to establish minimum standards for the implementation and administration of user, system, network, device, application account IDs, passwords, and requirements around multi-factor authentication.

Q: Describe the username and password (configuration and management) policies in place on both the Field System and Management System?

A: Default password is NIST-63B compliant.

Q: Do you have any time out configuration due to inactivity that can be used on the Field System?

A: Yes, it is possible to have a field unit configured to be inactive after a set period of time.

Q: Questions related to the password policies of the system

Civix described the process of assigning and changing passwords and authentication mechanisms.

ITP-SEC029. The purpose of this policy is to establish an information security policy to ensure that commonwealth IT facilities and resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

Q: Please describe physical access safeguards in place at your organization to ensure security of the data.

Civix represented that all data is managed in a Datacenter that has all the physical security required for a SOC I/II/III accredited Datacenter.

Q: Describe procedures to protect documents, computer media (e.g., tapes, disks, CD-ROMs, etc.), from unauthorized disclosure, modification, removal, and destruction?

Civix described the secure storage and encryption used on the data in their organization's hands. They also described data transmission safeguards in place with each licensing jurisdiction.

Q: What measures, policies and procedures do you employ and or/recommend for the physical security of the electronic poll book components?

A: We employ tamper protection cases with tamper evident tags, locks on all cases, stored in a humidity-controlled environment. During deployment the pollbooks should never be left alone without oversight and should where possible be locked to desks during use in a vote center or precinct.

Q: Are there security procedures for the decommissioning (replacement) of IT equipment and IT storage devices which contain sensitive information?

A: All pollbooks decommissioned by Civix will be processed by our partner to ensure safe and secure destruction of all storage locations as primary and secondary storage.

General Security Assessment Questions

Q: What strategy do you employ for tracking/auditing any data movement within the Electronic Poll book ecosystem?

A: All changes within the data creates trackable audits that are tamper resistant, record who, when and where that change happened and are used to propagate across the network and provide validity to the updates. This provides a consistent but secure data flow.

Q: Does the system provide a kiosk mode for Election Day use and prevent users from accessing other applications?

A: *Civix represented that the system can be configured in Kiosk mode.*

Q: Describe how the network architecture will be configured, where the Management System can be hosted and who would maintain the network and equipment?

A: *Civix described the configuration options.*

# # #

Attachment D – Components

The attached PDF explains the components in the ePollTAB case deployed to polling places. This is taken as represented in the Poll worker guide submitted as part of the application for approval.

Components - ePollTab.pdf

2.1 EPOLLTAB SETUP

Your ePollTAB Case contains a complete Poll Book setup which includes everything you would need to setup and run your Poll Book on Eleciton Day.

2.1.1 EQUIPMENT CHECK LIST

TRANSPORT CASE

This is an example of the transport case you will have to transport your ePollTAB and other items needed to setup a voting location.

A complete item check list will be provided during training and specifically for your jurisdiction.

2.1.2 CASE CONTENT

EPOLLTAB

The ePollTAB device which will be used to Check Voters in durring the Election.

MERLIN SYNC POINT

The Merlin device enables your precinct to securely communicate between each of your Poll Books during the Election.

MERLIN SECURITY SEALS

Your Merlin Device will come with Tamper resistant seals that should not be removed during the Election.

UBIQUITY AC – WIFI

The Ubiquity Access Point is a Wi-Fi device which is connected to your ePollTAB carry case.

2.1.3 OPTIONAL EQUIPMENT

BAR CODE READER

The Bar Code Reader is used to quickly check in Voters who have ID's that can be scanned.

QSENCE PRINTER

The Brother Rugged Jet 2030 is used with the QSence app to manage your Voter Lines.

BROTHER RECIEPT PRINTER

The Brother reciept Printer is used to pring Voter Reciepts.

BROTHER FORMS PRINTER

The Brother Laser Jet Printer is used to Print any Forms the Voter would need to sign.

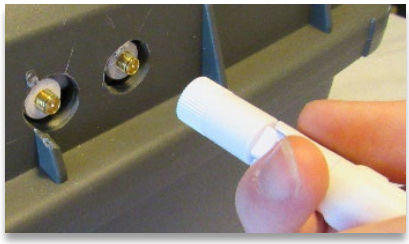
SECURITY LOCK

Your device might come with a Security lock.

TAMPER PROOF SEALS

Your device may come with Tamper proof Seals. These are installed by your Election Administrator.

2.1.4 SETTING UP



WIFI SETUP

When you arrive at the voting location, Open the ePollTAB carry case and remove the Access Points Antenna's.

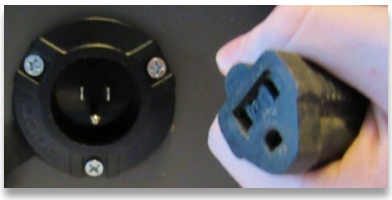
Attach them to the side of the ePollTAB case by screwing them into the extruding Antenna Points.

ELECTION SECURITY KEY

This USB Key contains the Election security Key and the Merlin Decrytion key and should be placed into the Merlin before you power on the Merlin and before you power on the first ePollTAB at the location.

USB BACKUP FOR MERLIN

This USB device is used to provide a Live Backup for audit logs and checkins and should be placed in the Merlin Device.



POWER TO THE MERLIN

TRANSPORT CASE

Once you have attached the Ubiquity Antennas, plug your Power cord into the Back of the case to provide power to your Merlin device.

POWER TO THE PRINTER

Unpack your printer and insert the Power cord into the back of the printer.

COMPLETE SETUP

Once you have everything plugged in, you are ready to power on the unit and start checking Voters in.

POWER UP YOUR ePollTAB unit

Press the Power button located on the side of the Samsung Galaxy device.

Printer Power ON

To Power on the Brother Printer, Press the Power button once.