COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

RESULTS OF VOTEC ELECTRONIC POLL BOOK VoteSafe (version PA-Cert) DEMONSTRATION

SECRETARY OF THE COMMONWEALTH
PENNSYLVANIA

Issued By:

Pedro A. Cortes

Pedro A. Cortes
Secretary of the Commonwealth
September 20, 2017

RESULTS OF THE VoteSafe (version PA-Cert) ELECTRONIC POLL BOOK DEMONSTRATION

I. 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 by VOTEC Corporation (VOTEC), the Department of State (Department) evaluated the VoteSafe (version PA-Cert) Electronic Poll Book (EPB) to ensure that the system complies with all the applicable requirements of Act 3, including the regulations implementing Act 3, 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 system demonstrations conducted by the Department with VOTEC Corporation on May 19, 2016 and April 26, 2017, in Hearing Room 5 of the Keystone Building located at 400 North Street, Harrisburg, Pennsylvania. Marian Schneider, then Deputy Secretary for Elections and Administration; Jonathan Marks, Commissioner of the Department's Bureau of Commissions, Elections and Legislation; and Kathleen Kotula the Department's Deputy Chief Counsel, represented the Secretary of the Commonwealth (Secretary) on May 19, 2016. Commissioner Marks and Deputy Chief Counsel Kotula represented the Secretary of the Commonwealth on April 26, 2017. Russ Dawson, National Sales Director/Legislative Liaison, and Keir Holeman, Elections Project Manager, represented VOTEC Corporation. Staff members of BCEL and the Department's Office of Chief Counsel also attended the demonstration. The Department videotaped the demonstrations on both days.

II. THE VOTEC VoteSafe (version PA-Cert) ELECTRONIC POLL BOOK

The VoteSafe (version PA-Cert) demonstrated for use in Pennsylvania included the following components: (1) WelcomeVoter Kiosk (Field System) – the hardware running

VoteSafe Pollbook Suite version: 8475 software at the polling place that allows poll workers to check in voters; and (2) PollPower Management System version: 8374M (Management system) – VOTEC supplied software that serves as VoteSafe command and control module that administers the Electronic Poll Book (EPB) system. The Field System consists of the laptop/tablet used by poll workers, the dedicated voter-facing tablet used for signature capture, and the printer used to print the check in activity. The system can be configured with additional Commercial Off the Shelf (COTS) peripheral devices. The following hardware components were represented in the documentation provided by VOTEC:

System & Hardware

Component Name	Details
Field System Laptop	PC running Windows 7, 8.1 or 10, Home or Pro, 32bit or 64bit with the latest Service Packs installed
Management System	PC/Server running Windows 7, 8.1 or 10 PC / Windows 2008 or 2012
Voter signature Capture Tablet	Windows Tablet
Printer/s (Optional)	Brother QL-700 label printer Star TSP 100 future print Any other printer
WEBCAM (Optional)	USB webcam (used for viewing DL while scanning barcode)
DL MAG SWIPER (Optional)	USB Magtek swiper

III. EVALUATION APPROACH, PROCEDURES AND RESULTS

A. Evaluation Approach

To evaluate whether VoteSafe (version PA-Cert) EPB can be successfully used in 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 evaluate and confirm on a field-ready system that the EPB satisfies all the statutory requirements and to understand the capabilities of the system. The Documentation Review consisted of analyzing the system specifications, user manuals, VSTL (Voting System Test Laboratories), and other third-party reports. Electronic poll books are heavily configurable distributed systems, typically consisting of networked tablets or laptops used at the polling place to check-in voters, and a central server performing the management functions including preparing the election data, performing voter history updates and monitoring deployed devices at polling places. The Documentation Review was done to confirm that the EPB can be efficiently used for elections in the Commonwealth of Pennsylvania and to aid in deciding the Electronic Poll Book connectivity configuration that can be approved for use in Pennsylvania.

B. Procedures

1. System Demonstration

The representatives from VOTEC demonstrated the VoteSafe (version PA-Cert) EPB system. The demonstration included an end to end set up and capability walkthrough of both the Field System and the Management system. The purposes of the demonstration 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) discuss compliance with the Commonwealth Information Technology Policies(ITPs) outlined in Attachment C of this report. The vendor provided an end-to-end demonstration of the system which included Field system set up and capability demonstration on May 19, 2016. VOTEC had not extracted the signature file from the test data during the initial demonstration. VOTEC further worked with Department of State staff to capture the signatures and completed that part of the demonstration along with a Management system demonstration on April 26, 2017. The Department of State videotaped the demonstrations.

2. Documentation Review

The Department requested the following documentation from VOTEC for review.

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. Glossary of Terms;
8. Known Anomalies; and
9. Reports from other states using the system.

Department of State staff reviewed the supplied documentation and analyzed the documentation of the system in detail.

3. Results

1. System Demonstration Results

a) Conformance to statutory requirements - The vendor successfully demonstrated that the EPB system conforms to the statutory requirements outlined in Pennsylvania law. *See* Attachment A for the list of statutory requirements discussed and validated during the demonstration.

b) Review of system capabilities - The Department reviewed the overall functional and nonfunctional capabilities of the system during the demonstration. *See* Attachment B for the list of system functional and nonfunctional capabilities discussed during the demonstration and a brief overview of the discussion points.

c) Compliance with Commonwealth IT policies – The Department provided VOTEC with a copy of the Commonwealth of Pennsylvania ITPs relating to the security of distributed systems and system connectivity. The Department also provided VOTEC with a list of questions so that it could evaluate compliance based on the responses. VOTEC provided responses to the questions during the demonstration on April 26, 2017. Time was set aside for a discussion of the questions and answers to determine level of compliance to Commonwealth ITPs. *See* Attachment C for the specific policies and discussion summary that occurred during the demonstration.

2. Documentation Review Results

The Department staff analyzed the documentation provided by VOTEC to understand the system capabilities in further detail.

In addition, the Department reviewed the VoteSafe certification reports issued by the states of Indiana and Ohio. The certification reports included testing reports by federally recognized VSTL (Voting System Test Laboratories) to attest conformance to the appropriate state standards. No anomalies were reported as part of the VSTL testing. The software version, VoteSafe (version PA-Cert) consisting of VoteSafe Pollbook Suite version: 8475, PollPower Management System version: 8374M demonstrated to Commonwealth of PA has been named differently but the vendor represented during the demonstration that the code base is the same. The corrected anomalies list provided by the vendor, "VoteSafe Anomalies V1-2.pdf" reports anomalies on fielded systems and remedial measures taken. The anomalies reported were on peripheral (Brother Printer and Signature Pad) connections, use of driver's license scanning device and communication from management system to Field System. See Attachment D for full description of the reported anomalies and the remedial measures taken.

The demonstration and documentation review determined that VoteSafe (PA-Cert) consists of COTS laptops configured as Field System to perform voter check-in activity at the polling place, and a Management System – a central server that resides at the county office or on a cloud server to perform administrative functions. The system allows a fully connected mode where data flows continuously between the central server and all Field Systems, allowing election officials to monitor the elections in real time. The system also allows a peer to peer mode where the Field Systems in use at a polling place will communicate check-in data to each other allowing the use of multiple Field Systems at a polling place while preventing multiple check-ins by a voter.

The networked environment makes the EPB system vulnerable to hacking attempts that can compromise the integrity of check-in data and/or result in unauthorized access to voter data. 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 come up with the connectivity configuration that can be approved for use in Commonwealth of Pennsylvania while minimizing the security risks and maximizing benefits in moving to an EPB solution.

3. Observations

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

1) VoteSafe (version PA-Cert) uses software configuration features to determine the final functional behavior of the system. VoteSafe (version PA-Cert) uses COTS components for Field System, Management System and peripheral devices. The Field Systems are configured by County IT Department. Management System is configured by the VOTEC or County IT Department depending on the configuration chosen. Even though demonstration showed that the system can be configured to satisfy all the statutory requirements, the Department will need assurance that the system setup complies with the approved configuration after purchase.

2) VOTEC provided system manuals to describe the functionality of the system. However, the supplied documentation lacked a version controlled full system user manual. The pdf file supplied was named pa_manual_05182017-brief.pdf. Delivery of a complete VoteSafe (version PA-Cert) system user manual will need to be verified on acquisition of the system.

3) VoteSafe (version PA-Cert) deployed in fully connected mode transmits transactional and operational data throughout Election Day to the Management System located outside of the polling place, either at the County office or a cloud server. The demonstration discussed the full capabilities of the system. The *fully connected mode* involves transmission of voter check-in between the Field Systems and the Management System throughout the Election Day. This configuration exposes the voter data for the entire period the polls are open. The product manufacturers

represented that the transmissions are secure but in absence of penetration testing it is not advisable to approve a connectivity configuration where the Field Systems communicate to the Management System in real time on Election Day.

IV. CONDITIONS FOR APPROVAL

Based on the demonstrations and the documentation review, the Secretary of the Commonwealth of Pennsylvania approves VoteSafe (version PA-Cert) subject to the following conditions:

A. The Field systems in operation at a polling place **must not** be configured to communicate to the Management System during the polling hours on Election Day. Any data transfer required between the Management System and Field System must happen via external media or secure file transfer process whenever possible. The connection to the Management System for election preparation shall happen before polling hours and Voter history updates must happen after Election Day is over. The Field systems in operation at a polling place can use sideways communication to synchronize voter check-in data during the polling hours.

B. The VoteSafe (version PA-Cert) Field systems communicating with each other must be configured and managed in a secure manner that they 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 any Voter Access Cards encoded on the EPB systems, USBs, SD cards, printers, CDs, etc.

D. Portable media used to transfer files between any components of the EPB system must be brand new. Alternatively, removable media that is being reused must be 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.

E. Any unused ports in the field system equipment must be sealed with tamper-evident seals.

F. Counties purchasing the VoteSafe (version PA-Cert) EPB system must work with VOTEC and BCEL (Bureau of Commissions, Elections and Legislation) to do the following:

1. Implement VoteSafe (version PA-Cert) EPB system in a manner that satisfies all statutory requirements outlined in Act 3 and the Pennsylvania Election Code. The parameter configuration and the text of informational messages must be approved by BCEL.
2. Implement VoteSafe (version PA-Cert) EPB system in a manner that complies with applicable Commonwealth IT policies and any best practices published by Department of State BCEL. The system configuration, connectivity set up, password configuration and password management policies must be approved by BCEL; and
3. Implement VoteSafe (version PA-Cert) EPB system with sound administrative practices and proper chain of custody in the same manner as counties deploy Electronic Voting Systems.

G. Counties must have a contingency plan to ensure that an election will not be affected should any component of the EPB system fail or any or all Field System units' malfunction on election day. The contingency plan must ensure that **no** "check in" information is lost. The contingency plan must be reviewed and approved by BCEL. At a minimum, the contingency plan must ensure the availability of a full voter list and a process for printing out voters who have already checked in if the EPB fails during voting hours.

H. Counties purchasing the VoteSafe (version PA-Cert) must work with BCEL 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 using scheduled programs. Any data transfer must happen via a file extract and secure file transfer process and must be encrypted. The extract must not contain any additional data elements than what was shared for the demonstration. The data elements and sharing mechanism must be approved by BCEL. Counties must ensure the accuracy of data loaded to the EPB system and maintain appropriate reports as necessary for auditability.

I. Counties implementing VoteSafe (version PA-Cert) must configure the system in such a manner that the poll worker cannot access other programs or applications during the polling hours. At a minimum, it is recommended that the poll worker training emphasizes that the poll workers shall not access any other programs or applications during polling hours.

J. VOTEC must notify the Department of State of any changes made to VoteSafe (version PA-Cert) EPB system. This includes any changes to the software and to the environment of the EPB system, including but not limited to VOTEC's development locations, cloud service vendors, data center locations, for example.

K. VOTEC must escrow a copy of the code, trusted build, any verification/identification software used and installation instructions for safe- keeping to the Commonwealth of PA and add the Commonwealth as a beneficiary to any Escrow accounts they have for safekeeping the VoteSafe (version PA-Cert) code.

L. VOTEC must provide fully prepared and version controlled user manuals for Field System and Management System for counties purchasing the EPB. The user manuals must clearly identify each user configurable parameter. Final user manuals must be submitted to the Department before sale of product in Pennsylvania.

M. The counties must work with VOTEC to define and implement policies on data retention and archiving on all parts of the EPB system including external servers and removable media. Any election data stored on devices outside of the county network must be deleted 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. VOTEC must keep audit logs of every data access event and make those audit logs available for inspection to the counties or BCEL upon request.

N. All jurisdictions implementing the VoteSafe(version PA-Cert) must carry out full Logic and Accuracy testing on each device and maintain records of Logic and Accuracy 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. 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. RECOMMENDATIONS

The Secretary makes the following recommendations to the counties purchasing the VoteSafe (version PA-Cert) EPB system:

a) The counties should perform a thorough evaluation and User Acceptance Test of the EPB system before purchase. This test should include all expected activities occurring as part of the election including data upload and download to the SURE system. This approval is based on a demonstration done by vendor and documentation review. Demonstration by the vendor should not be considered equivalent to testing.

b) The counties should consider using the EPB in pilot mode during the first use in an election. This allows the jurisdictions to ensure that all appropriate checks and balances are in place before using the EPB system in full production mode.

c) The Secretary urges counties to ensure that all poll workers and election officials receive appropriate training and are comfortable using the EPB. The training should include cyber hygiene practices and procedures for detecting cyber-attacks. The training should ensure that poll workers and elections officials can detect any warnings that signal cyber-attacks and immediately respond to it. The counties should develop and implement a disaster recovery plan that includes the possibility of a data breach or cyber-attack on the EPB.

d) The Secretary recommends counties purchasing the VoteSafe (version PA-Cert) EPB system perform proof of concept test onsite at all polling places to ensure 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 to what will be used on Election Day.

VI. CONCLUSION

Based on the demonstration, documentation review, and consultation with the Department staff, the Secretary of Commonwealth concludes that the VoteSafe (version PA-Cert) EPB meets all of the applicable requirements sets forth in Act 3 and the Pennsylvania Election Code, 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 (Yes/No)**
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 ● Internal ● External ▪ Data Preservation ▪ If the contingency for Electronic Poll Book failure is the printing of paper poll books/precinct lists from the EPB, the	**Yes**

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 keeps the data during operation on the hard disk of the Field System laptop and a removable SD card to ensure that data is always preserved. The system allows a capability to connect printers and configure reports. The EPB must prevent multiple “check-ins” by the same voter. **Demonstration Comments:** The system demonstration showed that the system identifies an attempt to check in an already checked in voter. The EPB displayed a message indicative of the duplicate check in attempt. In an environment where there are multiple filed systems connected data syncing between the devices has to be functioning to ensure multiple “check ins” are prevented.	
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.	**Yes**
Indication of whether the elector needs assistance to vote and, if so, the nature of the disability. (25 PaC.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	**Yes**

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)).	
"Absentee Ballot"-If an elector who voted an absentee ballot is in the municipality on Election Day, he or she must vote in the precinct, and the absentee ballot is voided. (25 P.S. § 3146.6(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: 42 U.S.C. § 15483(b)).	**Yes**

Attachment B - EPB Functionalities

Specific "check in"/voter handling Scenarios demonstrated

a) Provisional Ballot -
Process of performing a provisional check in and issuing a provisional ballot was demonstrated.

b) Absentee Ballot -
The system functionality that allows the poll worker to cancel the Absentee Ballot and allowing the voter to vote in person was demonstrated.

c) Cancel Check in -
The procedure for cancelling a Check in if an error/incorrect Check in happened was demonstrated.

d) Reissue Ballot -
The procedure for reissuing a new ballot in place of a spoiled ballot was demonstrated.

e) Inactive Voter Check in -
The process of checking in an Inactive voter with required affirmations was demonstrated. It was discussed that the process can be customized as required by statutes.

f) Redirecting a voter to the correct polling place -
The system behavior when the poll worker does a search for a voter who is registered to vote but is at the incorrect polling place was demonstrated. It was demonstrated that the system will indicate the poll worker that the voter is not at the correct polling place. The system allows the poll worker to check in the voter provisionally.

g) Search/Lookup voter Capabilities of the EPB -
It was discussed that the system allows a poll worker to look up the voter list to find a specific voter using different search combinations. The Search function is optimized with street number and first three letters of the voters last name. The typical configuration will search within the polling place first and then if the device has county wide data it will perform the search in the county wide data. VOTEC representatives suggested that a state-wide search is also possible for look up purposes and the system will not have a limitation holding the entire state data.

h) System behavior/messages when poll worker tries to check in an already checked in voter was demonstrated.

SURE System Interaction

a) Capability to import full and incremental data files from SURE -
It was demonstrated that the system allows loading data extracted in an agreed upon format from SURE system. Vendor representatives confirmed that the system can load the data including the signature files for any specific county in the Commonwealth of Pennsylvania. It was ascertained that the system allows loading either full files or incremental files as needed with appropriate password protection mechanisms to control and monitor the data load.

b) Reconciliation of the data load to the EPB -
The demonstration and discussion showed that the voter list/data load to the EPB system is reconciled and there is a process to handle exceptions.

c) Voting History Updates -
The process of getting an extract from the Management System to be loaded to SURE system for voting history updates was discussed.

d) County self-sufficiency in managing the interactions between SURE system and the EPB was discussed. VOTEC representatives suggested that after initial training the counties will be able to complete the processes by themselves.

Usability/User Interface

a) Procedures for setting up the Field System -
The procedures for setting up the Field System at the polling place were demonstrated. The set up required assembling the laptop the voter facing tablet and any additional peripherals needed. A stand/station that holds all the components comes with the system but is not mandatory.

b) Poll worker ability to access the system and login -
The process of poll worker login was demonstrated and was not complicated. The passwords are configurable and the system allows to set up unique passwords for each poll worker.

c) Screen navigation capabilities -
The screen navigation capabilities of the EPB were demonstrated and further discussed.

VOTEC representatives pointed out that there is customization possible with fonts and colors for better readability using configurable parameters without software changes.

d) Languages Supported by the system -
VOTEC representatives suggested that the voter facing signature tablet supports Spanish display for the voters.

e) Clarity of the messages displayed to the poll worker -
It was demonstrated the system displayed appropriate messages to the poll worker. The discussion suggested that there is a possibility to configure the verbiage of the messages using configurable parameters without software changes.

f) System power up and shutdown procedures -
System power up and shutdown procedures were discussed and were found to be not complicated.

g) System help availability -
The system provides the capability to upload help files for the poll worker. The system allows to upload video files or pdf files.

h) Additional Peripheral Connection Capabilities to the Field System -
The VOTEC representatives explained that EPB is a Windows based system running on laptops and hence additional peripherals can be connected depending on availability of the ports on the laptop used.

i) Election setup -
The Procedure for setting up the elections and preparing jar file for deployment to the Field Systems was discussed.

j) Usability Tests -
VOTEC provided their approach to improving the EPB System usability in a document, Usability_votesafe.pdf. The document suggests an iterative process with user feedback early and often in the design and build process. VOTEC representatives also suggested that VOTEC has participated in usability studies undertaken by Center for Civic Design and NIST aimed to understand the usability landscape for electronic poll books and to create a protocol for a usability test of Electronic Poll Books.

Auditability - Transaction Logging and Reports

a) Transaction Logging capability for Field System and Management System -
The logging capabilities for both the Field System and Management System were discussed. The mechanism to access the logs and ways to export the logs were discussed. The discussion was to ensure that the logging capabilities of the EPB system provided enough auditability.

b) Reporting -
The capability to configure and create reports from the EPB system was discussed.

Communication Protocols and Multiple Unit Synchronization

a) Field System to Field System communication -
The system provides Field system connectivity using private physical networks or wireless LANs. It was discussed that there is no limitation for the number of Field Systems connected in a polling place with wireless LANs.

b) Field System to Management System communication -
The poll book allows secure communication between Field System and Management System via VPN, secure wireless networks or via file export/import.

c) Frequency of check in activity sync up transmissions between Field systems -
The Field systems connected in an EPB system synchronizes multiple times a minute. If there is a connectivity issue, then the units in operation at a polling place will not be communicate check in data. Once the connectivity is restored the transaction sync up will happen and will include all the transactions during the period of connectivity loss.

d) Management System Hosting -
The different possibilities for hosting the Management System was discussed. The possibilities discussed were hosting the Management System on a County Server or on a Central server on cloud services. The details of each option were discussed to understand the security mechanisms in place.

Capacity, Redundancy, Fault tolerance and Continuity of Operations

a) Data Preservation -
The ability to continue election irrespective of any failure was discussed. VOTEC representatives explained that there are multiple ways to ensure there is no data loss in the event of a system failure. On each individual system, the data is stored

on the hard drive of the laptop and an additional backup is done to the SD card. If the system is running in peer to peer mode all data is backed up to its peer Field Systems as each transaction occurs. If the jurisdiction is running in a connected environment to the central server then all transactions are backed up continuously throughout the day.

b) Power supply and Battery Life -
The Power Supply and Battery life of the system was discussed to ensure that the system can work on battery as well as power.

c) Ability to remove/add new units without disturbing existing units -
VOTEC representatives suggested that new units could be added/removed into the EPB system without affecting existing Field Systems in operation.

d) Ability to add additional printers -
It was discussed that there is capability to add additional printers based on county's requirement.

e) System capability to support the volume of voters in any county in Pennsylvania -
It was discussed that the system will be able to support the volume of voters in any of the counties in PA without any performance degradations.

System monitoring and notification of system Errors or Deviations

a) Capability to perform a self-test to determine if all peripherals are operational -
The system allows the poll worker to run a test to ensure that the peripherals (signature tablet ad printer) connected to the system are operational.

b) Visible Display Indicating System Connectivity -
The demonstration showed that the system has a display of whether the unit is connected and communicating with other Field Systems.

c) Visible Display Indicating Power Supply/Batter Power -
The demonstration showed that the system has an indication that alerts the poll worker when running on battery and life of battery

Security and Chain of Custody

a) Password configuration and set up for admin and poll worker on Field System -
Vote Safe EPB allows password to be set up for poll workers and administrative users in addition to the Windows password to the Field System laptops. The

password lengths and configuration is user/county managed and can be set up when the system is being prepared for elections.

b) Information displayed to the voter on the signature pad -
The signature pad doesn't display the signature on file when being presented for signature to the voter.

c) Access controls for the Management System -
The Management System functionalities are password protected. This includes set up, full and incremental Data loads and configuration functions as well as individual Field Systems.

d) Data in Motion Security -
Please refer to Item J in Attachment C.

e) Data at Rest Security -
Please refer to Item F in Attachment C.

Maintenance, support and Training

a) Hardware and software acquisition options and support -
VOTEC representatives suggested that they will work with the county to configure an optimal system for use in the county. It was discussed that the EPB system used COTS hardware components and can be purchased either thru VOTEC or from any other vendor.

b) Service Agreement and Warranty Options -
The Service Agreement and Warranty options available for the system was discussed. VOTEC representatives suggested that they will work with the county to provide a tailored agreement as needed by the county.

c) Training Options -
It was discussed during the demonstration that a mutually agreed upon training plan will be worked with the county upon acquisition of the EPB.

d) Cost -
The average cost that would be incurred in acquiring the system was discussed.

Attachment C - Commonwealth IT Policies Discussion

A) ITP-SEC001 – Policy that governs Commonwealth's antivirus agent, host intrusion prevention agent (host-based intrusion prevention system), incident response servlet and patch management agent for all servers.

Discussion Summary: VoteSafe (version PA-Cert) uses COTS components configured as Field Systems. County IT personnel will need to install Antivirus and host intrusion prevention software. Field system patching also will need to be done by County IT personnel. The vendor did not recommend any specific antivirus or intrusion detection software. The vendor representatives suggested that they have not encountered any customer selected anti-virus software that prevents the EPB software from operating correctly.

VOTEC representatives suggested that Management System patching is controlled by the vendor to avoid regression defects, environment failures and interruption during Election times.

The discussions suggest that system can be configured to comply with this policy.

B) ITP -SEC004 - Establishes policy and enterprise-wide standards for commonwealth agencies on Web Application Firewalls

Discussion Summary: County IT is responsible for hardening Field system firewall settings or use a third-party software firewall which may be bundled with anti-virus modules such as those described in Commonwealth IT policy RFD-SEC001a. County IT is responsible for the use of an application firewall and the network isolation of the database for on premises Management System deployments. VOTEC provided details of firewall configuration on cloud based hosting of the Management System.

The discussions suggest that system can be configured to comply with this policy.

C) Do you have, as a part of your operational security standards, policies, procedures and scans for on-going security, including audits?

Discussion Summary: VOTEC did not have any specific reports to share and suggested that it can work with counties if needed for running security scans or audits.

D) ITP-SEC010 – Establishes policy and procedures associated with the use of Virtual Private Networks (VPNs).

Discussion Summary: The discussion and written answers provided suggest that data transmission is encrypted and complies to this policy.

E) ITP-SEC019 – Establishes policy and procedures to protect commonwealth electronic data.

Discussion Summary: VOTEC suggested that they will adhere to county's data cleansing procedures if any. It was also discussed that all data on the Field System is encrypted. VOTEC shared data encryption details on the Management System hosted on cloud which satisfies the standards mentioned in ITP-SEC019.

Do you continually perform security assessments?

Discussion Summary: VOTEC suggested that they do not have any third-party security assessments done but will support if the clients need to have a security assessment done.

F) ITP-SEC020 - Establishes policy and standards for encryption of data at rest

Discussion Summary: VOTEC suggested that the data on the WelcomeVoter kiosk is encrypted. The Data held on the Management system is also encrypted at storage level. The full disk encryption covers the underlying storage for the database instance as well as logs, backups and snapshots.

G) ITP-SEC024 – Establishes policies, procedures and standards related to reporting and managing of cyber security incidents.

Discussion Summary: VOTEC will assist customer in adhering to security reporting procedures as defined by the state. VOTEC policy, concerning security reporting, limits primary interaction to designated customer representatives. Secondary interactions are limited to other government agencies (SOS, law enforcement, courts) as dictated by the circumstances and customer policy.

H) ITP-SEC025 – Establishes guidelines for the proper electronic use and disclosure of Personally Identifiable Information.

Discussion Summary: VOTEC representatives suggested that the EPB system supports the State's PII requirements regarding a voter's election check-in requirements. The data at rest and data in motion encryptions in the poll book system satisfy appropriate Commonwealth IT policies.

I) ITP-SEC029 - Establishes policy and procedures for commonwealth agencies for physical security of IT resources.

Discussion Summary: County determines physical security policy for all local hardware equipment. VOTEC recommends the WelcomeVoter kiosk should be treated like any other critical polling place equipment. VOTEC recommends that counties adhere to similar processes as voting machines and ballots, such as the use of serial number asset tags, inventory tracking to poll place assignment, shipment with tamper resistant seals, etc.

J) ITP-SEC031 - Establishes policy and standards for encryption of data in transit to improve the confidentiality and integrity of data.

Discussion Summary: VOTEC suggested that all data in motion is encrypted and provided the encryption protocols used. The encryption standards used demonstrates compliance to this policy.

K) ITP-SEC032 Establishes compliance standards for enterprise Data Loss Prevention (DLP).

Discussion Summary: The policy refers compliance to the below mentioned policies. VOTEC's answers are provided below

The application and the infrastructure software rely on password protection to access voter data. VOTEC also recommends the county password protect WelcomeVoter Windows access.

1) ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data

Refer to Item E above.

2) ITP-SEC020 - Encryption Standards for Data at Rest

Refer to Item F above.

3) ITP-SEC031 - Encryption Standards for Data in Transit

Refer Item J above

4) ITP-SEC017 - CoPA Policy on Credit Card Use for e-Government Applications (if applicable)

Not applicable

VOTEC representatives suggested that the system has mechanisms for additional authorization via unique identifiers for communicating data to the host server and the communications to the host server are logged in the backend database.

L) ITP-SEC035 - This Information Technology Policy establishes policy, responsibilities, and procedures for connecting and using mobile communication devices to access commonwealth IT resources.

Discussion Summary: The EPB Solution utilizes a tablet for the voter facing display and signature capture. The tablet stores NO application data nor does the tablet connect to any other device other than the EPB Field System laptop. All data is ephemeral - not written to stable storage.

M) L) ITP-SEC007 - This Information Technology Policy establishes establish minimum standards for the implementation and administration of user, system, network, device, application account IDs, passwords, and requirements around multi-factor authentication

Discussion Summary: The Field Systems provide a capability of having unique passwords configured for poll workers for accessing the system. The Management System access is also password protected. All password functions are configurable complying to ITP-SEC007. The application password and logout features can be used in addition to the Windows password and timeout configurations for additional security.

Attachment D - Reported Anomalies and Remedial Measures

VoteSafe Anomalies
Updated 3/25/2016 VoteSafe Anomalies V 1.2

Issue: Brother Printer does not automatically resume printing job if print media runs out and needs to be replenished.
Resolution: Incorporated the updated B-Pac software from Brother in to the .jar (Java Archive) file.

Issue: Special characters in Live Help messages were preventing voter updates from being sent to the VoteSafe Field system.
Resolution: Updated management system software to allow for special characters to be included in Live Help messages

Issue: Signature pad would not connect to VoteSafe on first try. Sometimes multiple attempts were needed to re-establish connection.
Resolution: Updated the VoteSafe signature application to enhance the Reconnect to VoteSafe feature and make it reliable.

Issue: Scanning older driver's licenses would not return matches in VoteSafe (Illinois)
Resolution: Discovered driver's licenses issued prior to 2013 did not include address. We made changes to search for voters using name, birthdate, and addresses to accommodate these driver's licenses.

Issue: Scanning driver's licenses in Ohio for 17-year-old voters in a primary election would not trigger the Ballot Number Issued window.
Resolution: Made programming changes to show the Ballot Issue Number window for the 17-year-old voter work flow for all elections.