COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

RESULTS OF TENEX SOFTWARE SOLUTIONS ELECTRONIC POLL BOOK PRECINCT CENTRAL 3.2.0.1 DEMONSTRATION

Issued By:

Pedro A. Cortes

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

RESULTS OF THE TENEX PRECINCT CENTRAL 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 Tenex Software Solutions (Tenex), the Department of State (Department) evaluated the Tenex Precinct Central Touchpad Version 3.2.0.1 Electronic Poll Book (Tenex Precinct Central 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 Tenex on April 5 and April 28, 2017. The in-person demonstration on April 5, 2017 occurred in Hearing Room 3, Keystone Building, 400 North Street, Harrisburg, Pennsylvania. The Department recorded the demonstration on video. Marian Schneider, then-Deputy Secretary for Elections and Administration; Jonathan Marks, Commissioner of the Department's Bureau of Commissions, Elections and Legislation (BCEL); and Kathleen Kotula, the Department's Deputy Chief Counsel, represented the Secretary of the Commonwealth (Secretary) at the demonstration. Tenex President, Ravi Kallem, represented Tenex. Staff members of BCEL and the Department's Office of Chief Counsel also attended the demonstration.

II. THE TENEX Precinct Central 3.2.0.1 ELECTRONIC POLL BOOK

The Tenex Precinct Central 3.2.0.1 EPB demonstrated for use in Pennsylvania included the following components: (1) Precinct Central Touchpad; (2) Precinct Central Console; and (3) Precinct Central Data Studio. The following is a brief description of the components summarized from the documentation supplied by Tenex.

- **Precinct Central Touchpad** is the part of the electronic poll book solution that is used at the polling place. The primary function of this module is to facilitate voter check in at the polling place.

- **Precinct Central Console** is the real-time comprehensive monitoring platform that allows election staff to monitor devices, users, communications and performance metrics on a secure computing environment. Precinct Central Console is also the election office portal for all pre-election setup activity and post-election data reconciliation, auditing, and exporting.

- **Precinct Central Data Studio** forms the communication backbone for the product suite. This module provides all interfaces for integrating with the voter registration system and for communicating information between all Precinct Central Touchpads deployed.

Below is the Hardware/Software/Peripherals/Additional Equipment list provided by Tenex.

Hardware Components

Component	Required or Optional
32 GB iPad Mini 2	Required
16 GB iPad Air 2	Optional (not required if iPad Mini 2 is used)
Capacitive Stylus	Required
Brother QL710W	Optional
Epson TM-m30 Bluetooth Printer	Optional
Flip & Share Case/Stand Model 2.2	Optional
Jetpack MiFi 6620L (other local carrier models may differ)	Optional

Additional Equipment

Item	Description	Required or Optional
DD-WRT COTS Router	Four (4) Linksys or ASUS Routers to be used in a mesh configuration in warehouse for download and data activities	Optional
Download Appliance Windows Server	Local management and caching server for data	Optional
Mac Mini	Used for MDM of all Touchpad devices	Optional
Charging Chart	Stores and charges up to 75 EPBs	Optional
10 ft. MFi Certified Charging Cables	Chargers for EPBs to be used on Election Day	Optional

Consumables

Item	Description	Required or Optional
Epson TM-m30 Receipt Printer Paper Refills	Paper refill cartridge to be used in Epson printer	Required as needed
Brother QL710W Label Printer Refills	Label paper refill cartridge to be used in Brother printer	Required as needed
Capacitive Stylus	Stylus used by both the election workers and voters for tablet interactions	Required as needed

Software Components

License Type	Description
Precinct Central Touchpad Software	EPB application used on the iPad-based Precinct Central Touchpads
Precinct Central Data Studio Software	Data conversion utility used to create voter databases for use on the Touchpads
Precinct Central Console Software	Backend monitoring and election set-up web based system

III. EVALUATION APPROACH, PROCEDURES AND RESULTS

A. Evaluation Approach

To evaluate whether Tenex Precinct Central 3.2.0.1 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, and VSTL (Voting System Test Laboratories) and other third-party test reports. EPBs 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 confirms that the EPB can be efficiently used for elections in the Commonwealth of Pennsylvania and to aid in deciding the EPB connectivity configuration that can be approved for use in Pennsylvania.

B. Procedures

1. System Demonstration

Representatives from Tenex demonstrated the Tenex Precinct Central 3.2.0.1 EPB system. The demonstration included an end-to-end set-up and capability walkthrough of the Precinct Central Touchpad, the Precinct Central Console, and the Precinct Central Data Studio. The purpose of the demonstration was to: (1) validate that the system complies with Pennsylvania's statutory requirements for poll books; (2) discuss the overall capabilities of the system; and (3) discuss compliance with the Commonwealth Information Technology Policies (ITPs) outlined in Attachment C of this report. During the in-person demonstration conducted on April 5, 2017, the system did not successfully display the assistance codes extracted from the Statewide Uniform Registry of Electors (SURE) system on the Precinct Central Touchpad. Tenex representatives worked with Department staff to display the data correctly on the Precinct Central Touchpad. The demonstration of the display of the

assistance codes was completed via email exchange of system screenshots on April 28, 2017.

2. Documentation Review

The Department requested the following documentation from Tenex for review:

(a) System Specifications;

(b) Hardware/Software/Peripherals/Additional Equipment Requirements;

(c) Technical Data Sheet;

(d) User Manual;

(e) Usability Reports;

(f) Security and Penetration Testing Reports;

(g) Known Anomalies; and

(h) Reports from other States using the system.

Department staff reviewed and analyzed all relevant information and documentation for the Tenex Precinct Central 3.2.0.1 EPB system.

C. Results

1. System Demonstration Results

(a) Conformance to statutory requirements - The vendor successfully demonstrated that the Tenex Precinct Central 3.2.0.1 EPB system conforms to the statutory requirements outlined in Act 3 and the Pennsylvania Election Code. *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 Tenex Precinct Central 3.2.0.1 EPB 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 ITPs - The Department provided Tenex with a copy of the Commonwealth of Pennsylvania ITPs relating to the security of distributed systems and system connectivity. Time was set aside for discussion during the demonstration to determine the level of compliance to Commonwealth policies. *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 Tenex to understand the system capabilities.

In addition, the Department reviewed the Tenex Precinct Central 3.2.0.1 EPB certification reports issued by the State of Ohio. The certification reports included testing reports by a federally recognized VSTL to affirm conformance to Ohio state standards. The documentation included a security assessment report by MAD Security (MAD), an independent organization providing cybersecurity solutions. MAD stated that their assessment methodology focused on assessing the security of networks, systems, devices and applications that comprise the EPB system as separate entities each that could contribute to and build upon each other to create a secure environment. MAD identified four vulnerabilities and categorized them as "medium" and "low" risk. The vulnerabilities were remediated and the system was reexamined by MAD for confirmation. The MAD report documented the overall risk rating for the Tenex Precinct Central 3.2.0.1 EPB system as "low" and the overall security posture for the system as "robust.".

The demonstration and documentation review determined that Tenex Precinct Central 3.2.0.1 EPB consists of iPads configured as Precinct Central Touchpads to perform voter check-in activity at the polling place. Election preparation and monitoring activities are performed using Precinct Central Data Studio and Precinct Central Console. Precinct Central Console and Precinct Central Data Studio utilizes cloud-based servers and

computing services. The system allows the following modes of configuration:

- A live (fully connected) mode where data flows continuously between cloud-based servers and all Precinct Central Touchpads in use at a polling place;

- A restricted server communication mode where the system can be configured to transfer only operational/performance data from the Precinct Central Touchpads to the cloud server. The data transmitted doesn't contain any voter check-in data. This will allow monitoring of the polling place devices remotely;

- A configuration where only Precinct Central Touchpads at a polling place communicate to each other without any connection to the cloud server. This configuration allows voter check-in data to sync up in a particular polling place, thus allowing the use of multiple Precinct Central Touchpads at a polling place.

The networked environment makes the Tenex Precinct Central 3.2.0.1 EPB system vulnerable to hacking attempts that can compromise the integrity of check-in data and/or result in unauthorized access to voter data. Department staff analyzed the connectivity configurations discussed during the demonstration in conjunction with the documentation provided and existing Department test protocols for EPBs to determine the connectivity configuration for use in the Commonwealth of Pennsylvania. The Department is focused on minimizing the security risks and maximizing benefits in moving to an EPB solution.

3. Observations

Department staff noted the following during the demonstration and documentation review:

(a) The Tenex Precinct Central 3.2.0.1 EPB uses software configuration features to determine the final functional behavior of the system. 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.

(b) The demonstration showed that Tenex Precinct Central 3.2.0.1 EPB can be configured to comply with applicable Commonwealth ITPs. The final system configuration will depend on the parameters selected during the set up. System compliance will be ascertained after purchase.

(c) Tenex provided system manuals to describe the functionality of the Tenex Precinct Central 3.2.0.1 EPB system. However, the supplied documentation did not include all the manuals for the system. Delivery of a complete Tenex Precinct Central 3.2.0.1 EPB system user manual will be verified on acquisition of the system.

(d) Tenex Precinct Central 3.2.0.1 EPB deployed in live (fully connected) or restricted server communication mode communicates with a cloud server located outside of the polling place. The demonstration discussed the full capabilities of the system. The live or restricted mode maintains a communication channel between the polling place and cloud server for the entire time the polls are open on Election Day. The product manufacturers represent the transmission to be secure but in absence of penetration testing, it is not advisable to approve a connectivity configuration where the Touchpads communicate to the cloud server 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 Tenex Precinct Central 3.2.0.1 EPB subject to the

following conditions:

A. The Precinct Central Touchpads in operation at a polling place **shall not** be configured to communicate to the central cloud server during polling hours on Election Day. The connection to the central server for election preparation shall occur before polling hours and voter history updates shall happen after the polls close on Election Day. The Precinct Central Touchpads in operation at a polling place can use sideways communication to synchronize voter check-in data during the polling hours.

B. The Precinct Central Touchpad systems communicating with each other shall 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, shall not connect 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 holding voter data between any components of the EPB system shall be new and unused. Alternatively, removable media reused from previous elections shall be reformatted before each election. All removable media used for elections shall be managed with proper chain of custody and administrative safeguards to protect against data disclosure, theft, or damage.

E. Any unused ports in the Precinct Central Touchpad must be sealed with tamper-evident seals.

F. Counties purchasing the Tenex Precinct Central 3.2.0.1 EPB system shall work with Tenex and BCEL to:

1. Implement Tenex Precinct Central 3.2.0.1 EPB 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 shall be approved by BCEL;

2. Implement Tenex Precinct Central 3.2.0.1 EPB system in a manner that complies with applicable Commonwealth ITPs and any best practices published by Department of State BCEL. The system configuration, connectivity set up, password configuration and password management policies shall be approved by BCEL; and

3. Implement Tenex Precinct Central 3.2.0.1 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 elections will not be affected should any component of the EPB system fail or any or all Touchpads malfunction on Election Day. The contingency plan shall ensure that **no** "check in" information is lost. The contingency plan shall 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 Tenex Precinct Central 3.2.0.1 EPB 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 Tenex Precinct Central 3.2.0.1 EPB system shall implement at least two (2) Precinct Central Touchpads per polling location and must allow sideways communication to enable check-in activity to synchronize between the Touchpads. This is necessary to ensure data storage redundancy.

J. Counties implementing Tenex Precinct Central 3.2.0.1 EPB system 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.

K. Tenex must notify the Department of State of any changes made to the Tenex Precinct Central Electronic 3.2.0.1 EPB system. This includes any changes to the software or the environment of the EPB system including, but not limited to, Tenex Software Solutions development locations, cloud service vendors, data center locations, etc.

L. Tenex must escrow a copy of the code, trusted build 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 Precinct Central Electronic 3.2.0.1 EPB system code.

M. Tenex must provide fully prepared and version controlled user manuals for all components of the Tenex Precinct Central 3.2.0.1 EPB system. The user manuals

shall clearly identify all the user configurable parameters. Final user manuals shall be submitted to the Department before sale of product in Pennsylvania.

N. The counties must work with Tenex 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. Tenex must keep audit logs of every data access event and make those audit logs available for inspection to the counties or BCEL upon request.

O. All jurisdictions implementing the Tenex Precinct Central 3.2.0.1 EPB shall perform Logic and Accuracy Testing 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. The vendor supplied Logic and Accuracy checklist should be used as a reference, but shall not be accepted in lieu of a county specific plan.

V. RECOMMENDATIONS

The Secretary makes the following recommendations to counties purchasing the Tenex Precinct Central 3.2.0.1 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 available 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 all appropriate checks and balances are in place before using the EPB 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 on Election Day. The training should include cyber hygiene practices and procedures for detecting cyber-attacks. Training should ensure that poll workers are trained to detect warnings that signal cyber-attacks and immediately respond to those warnings. 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 Tenex Precinct Central 3.2.0.1 EPB system perform proof of concept testing onsite at all polling places to ensure connectivity and power supply availability. The Secretary further recommends the test be 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 Tenex Precinct Central 3.2.0.1 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 EPB should provide for the following relating to data recovery and adequate contingencies should one or more elements of the EPB fail: ▪ Memory Redundancy • Internal • External ▪ Data Preservation ▪ If the contingency for EPB failure is the printing of paper poll books/precinct lists from the EPB, the EPB must provide for	**Yes**

the printing of a paper poll book AND a copy of the list of registered voters within the precinct. **Demonstration Comments:** The manufacturer represented that Tenex Precinct Central 3.2.0.1 maintains redundancy when multiple Touchpads are used at the polling place. 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 could identify a checked in voter and displayed a message indicating that the voter had already voted. In an environment where there are multiple Precinct Central Touchpads are connected data syncing between the devices must be operational 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 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 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 – Tenex Precinct Central 3.2.0.1 EPB Functionalities

Specific "check in"/voter handling Scenarios

(a) Provisional Ballot -
Process of performing a provisional check in and issuing a provisional ballot was demonstrated. The discussion included situations under which a provisional ballot will be required in Pennsylvania and how the system captures the reason for the provisional ballot. The Precinct Central System allows the poll worker to issue a manual provisional ballot when the reason for the provisional ballot is not configured in the system.

(b) Absentee Ballot -
The system functionality that allows the poll worker to cancel an Absentee Ballot and allow the voter to vote in person was demonstrated. The system demonstrated considered this to be a provisional ballot. It was mentioned by Department staff that the regulations in Pennsylvania doesn't equate cancelling an absentee ballot as a provisional ballot situation. It was explained by the Tenex representatives that the system can be customized without software changes to achieve the result required.

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

(d) Inactive Voter Check In -
The process of checking in an Inactive voter with required affirmations was demonstrated. Tenex representatives mentioned that the process can be customized as required by jurisdictions.

(e) Redirecting a Voter -
The system behavior when the poll worker does a search for a voter who is at an incorrect polling place was demonstrated. It was demonstrated that the system will not allow the poll worker to check-in a voter who is not at the correct polling place. The system allows the poll worker to check-in the voter provisionally if needed. The system also allows printing and/or emailing or texting the directions to the redirected polling location.

(f) Search/Lookup Voter Capabilities of the EPB -
It was discussed that the system can search the voter list by using different search combinations. The system allows the following relevant search options:

- Last Name and House Number;

- Last Name and First Name;
- Last Name and Birth Year;
- Last Name and Birth Date; and
- Voter ID.

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

SURE System Interaction

(a) Capabilities to import full and incremental data files from SURE -
It was demonstrated that the system allows loading data in standard agreed upon format from SURE system. It was ascertained that the system allows loading either full files or incremental files as needed for set up before the elections. The data can be extracted from the SURE system either by using file export/import process or using a program that runs at scheduled intervals to extract the data. The extracted data is then prepared on cloud servers to be loaded to the Precinct Central touchpads. Tenex representatives expressed interest in having ".txt" files of a specific layout if possible to reduce data massaging, but it was suggested that the system can use the format that Department provided test data.

(b) Reconciliation of the data load to the Electronic Poll Book -
The demonstration and discussion showed that the 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 Tenex Precinct Central 3.2.0.1 system to be loaded to SURE system for voting history updates was discussed. The format of the files required by the SURE system would need to be shared with the vendor and further testing performed before implementation.

(d) County self-sufficiency in extracting and uploading data files from SURE to the EPB during election preparation was discussed. The entire process of data extraction and election preparation was discussed during the demonstration. Tenex 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 procedure for setting up the Precinct Central Touchpads at the polling place was demonstrated. The set-up process was not complicated.

(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 setting up unique passwords for each poll worker.

(c) Screen navigation capabilities -
The screen navigation capabilities for the EPB system were demonstrated and further discussed. Tenex representatives explained that there is customization possible with layout, fonts and colors for better readability using configurable parameters without software changes.

(d) Languages Supported by the system -
The documentation provided suggested that the Precinct Central can be configured to translate voter-facing screens into any language required by the State of Pennsylvania. This configurable option allows the poll worker to select a language for the voter by touching a button. It was mentioned that to date, Precinct Central customers have used the language option to translate voter facing screens into Spanish, Creole, and French.

(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 without any software changes.

(f) System power up and shutdown procedures -
System power up and shutdown procedures were discussed and were found to be easy enough for use on Election Day.

(g) Election set up -
The Procedure for accessing the Precinct Central Data Studio and Precinct Central Console to prepare for elections and loading the data to the Precinct Central Touchpad for election was discussed. Tenex representatives suggested the availability of training, user manuals and manufacturer support to aid in election preparation.

(h) Usability tests -
The discussion and documentation provided suggested that Tenex uses the following methods to conduct usability tests

(1) Mock Elections
(2) Field Studies

(3) Focus/User groups
(4) Customer feedback
(5) Internal Usability Testing

Auditability - Transaction Logging and Reports

(a) Transaction Logging capability for the Tenex Precinct Central 3.2.0.1 system was discussed. The logging capabilities of the system were discussed in detail to validate that the EPB system provides sufficient logging required for auditability.

(b) The mechanism to access the logs was discussed.

(c) The capability to configure and create reports from the EPB system was discussed.

Communication Protocols and Multiple Unit Synchronization

(a) Precinct Central Touchpads communicate to each other (Sideways communication) to synchronize voter check in data. Sideways communication is achieved using Wi-Fi with back up adhoc Wi-Fi or vice versa.
Documented details from Precinct Central specification
Each Touchpad registers with the neighboring Touchpads and communicates limited voter check-in data. This process gives jurisdictions that do not allow central server communications the ability to share information and allow data redundancy. This process also allows a voter to get service from any check-in station regardless of where the initial check-in was done. This bank teller like model keeps the voting process moving by allowing voters who need assistance (spoiling a ballot for example) to visit any check-in station because their initial check-in data will already be shown on all Touchpads in the precinct. When Election Day is over and the Touchpads are brought back to the Election Offices, they will then have the ability to communicate all saved voter check-ins and information to the Cloud.

(b) Precinct Central Touchpad to central server communication -
The communication between Precinct Central Touchpad and central server was discussed. The poll book allows communication between Touchpads and central server via secure wireless networks. The communication can happen in real-time throughout Election Day or can be achieved at the end of the day after polling is completed. Further discussions with Tenex Software Solutions and Cuyahoga county after the demonstration determined that the system can be configured in a mode whereby the Touchpads can communicate performance data to the Central

server thereby allowing counties to monitor the electronic poll books on election day.

(c) Frequency of sync up transmissions between Precinct Central Touchpads -
The Precinct Central Touchpads at a polling place synchronizes check in data near real time. If there is a connectivity issue during operation the data sync up will automatically happen when the connectivity is restored.

Capacity, Redundancy, Fault tolerance and Continuity of Operations

(a) Data Preservation –
The data is stored on iPad and once synchronized multiple devices at the polling place can provide redundancy if there is no central server communication. If there is communication to central server then it provides additional redundancy.

(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. It was discussed that the iPad can work for around 10 hours on battery. Tenex Software Solutions representatives suggested that Tenex recommends plugging in the systems during the polling hours.

(c) Ability to remove/add new units without disturbing existing units -
Tenex Software Solution representatives suggested that new units could be added/removed into the Electronic Poll Book system without affecting existing functioning systems.

(d) Ability to add additional printers –
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 Commonwealth of PAA 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 ensures that a printer is connected on set up and prints a poll opening slip prior to the start of the election.

(b) The demonstration showed that the system has a display of whether the unit is connected and communicating with other field systems.

(c) 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 for admin and poll worker on Precinct Central Touchpad -

Precinct Central Electronic Poll Book allows centrally administered password configuration that supports configuring uniquely identifiable user name and password. The system further requires password/s (one or two based on configuration) to open the polls

(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 setting up elections using Precinct Central Data Studio and Precinct Central Console -
Pre-Election set up activities using Precinct Central Console and Precinct Central Data Studio are password protected. This includes but are not limited to set up, full and incremental Data loads and any configuration functions.

(d) Data in Motion Security -
Please refer to Item H 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 -
The hardware and software acquisition options from Tenex Software Solutions were discussed. The poll book is generally sold as a system including the hardware and software.

(b) Service Agreement and Warranty Options -
The Service Agreement and Warranty options available for the system were discussed.

(c) Training Options -

The training options available for jurisdictions implementing the Precinct Central system was discussed.

Attachment C - Commonwealth ITPs 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: Precinct Central Touchpad uses iPads for field systems and doesn't use any antivirus software on the touchpads. Touchpad Patching is controlled and is done with support from Tenex Software Solutions. The antivirus used on Precinct Central Console was discussed. Patching is controlled by Tenex Software Solutions and is done within a month from the release of the patch.

The discussions suggest that system can be configured with appropriate antivirus and host intrusion prevention programs.

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

Discussion Summary: Firewall policies on the AWS instances were discussed. Tenex software solutions maintain a block list that is refreshed periodically to avoid ransomware/malware. The discussion suggested that the system can be configured to satisfy compliance to the policy. The Windows server implementation was represented to be CIS 1.7 compliant

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

It was mentioned that the benchmarks for Windows Server 2008 R2 and IIS 7.0 were applied to all the servers to make sure that system files were secure, malicious code could not be executed, and unauthorized users would not be allowed access to the server. CIS 7.0 has been attested by the security assessment by MAD security, the firm that performed penetration testing of the system. The vendor representatives suggested that Tenex Software Solutions is also evaluating the use of other products like Thycotic to secure account passwords and endpoints.

(C) ITP-SEC007 - This ITP 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 system has multiple levels of password protection and all of them are configurable to satisfy the Commonwealth policy. The Touchpads provide a capability of having unique passwords configured for poll workers accessing the system. Precinct Central Touchpad is equipped with security features to ensure that check in activities at a polling place are started with appropriate password controls. System also has a timeout/lock feature that allows election officials to temporarily lock the device if they step away from their station. The Touchpad can be configured to close the election

and lock the device to close the polls. The Precinct central console access is also password protected and has timeout configuration. The vendor also suggests best practices for management of passwords in the system documentation.

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

Discussion Summary – All data transmission is encrypted and web portal access to Precinct Central and Precinct Central Data Studio has time outs configured. It was represented that the highest level of encryption was used for any client connections to the server and remote desktop connections.

The policy specifically mentions about Commonwealth VPN policies but the discussion suggested that the product can be configured in a manner that satisfies the requirements mentioned in the policy for secure connections.

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

Discussion Summary: The poll book system has the voter data and the vendor realizes the importance of the data. Precinct Central uses industry standard leading edge technologies to secure and protect sensitive information. Every component of the system has hardware, software and physical safeguards to protect the data.

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

Discussion Summary: It was discussed that all data at rest is encrypted. The Touchpads used have hardware encrypted file system. The database is encrypted. The implementation also uses encryption and hashing together for configuration files to ensure that there is an additional level of protection.

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

Discussion Summary: The discussion suggested that the vendor realizes that the data needs to be protected and attack prevention is the best course of action. All data on the poll book is encrypted and all data transmission is also encrypted. In addition, the communication payload is encrypted using encryption libraries. Tenex Software Solutions representatives suggested that since the payload is encrypted, even if someone could sniff the package, parsing will be difficult due to the encrypted content

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

Discussion Summary: It was discussed that data transmission between components of the system uses encryption protocols which demonstrate compliance to this policy. Any file transfer is done using secure file transfer process. The system uses a Wi-Fi connection to sync check in data and the transmission is encrypted. There is an additional level of protection whereby the communication payload is encrypted using encryption libraries.

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

Discussion Summary: The policy refers compliance to the below mentioned policies.

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

Item E above.

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

Item F above.

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

Item H above

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

Not applicable

The vendor represented that the system has been built with a prevention approach in mind and has multiple levels of security to ensure that the attack is prevented and there is another layer of security to ensure that even if the attack happens the data and executables cannot be used due to the additional levels of protection.

(J) 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 an iPad at the polling place. The EPB does not connect to the Commonwealth network but the discussions suggest that the touchpad can be configured with the appropriate configuration mentioned in the policy.