



*Report Concerning the Evaluation
Results of Tenex Electronic Poll Book
Precinct Central 6.1.5*

Issued By:

A handwritten signature in blue ink, appearing to read 'Al Schmidt', written over a horizontal line.

Al Schmidt

Secretary of the Commonwealth

August 26th, 2026

www.dos.pa.gov



Contents

I.	Introduction.....	4
II.	The Precinct Central 6.1.5 Electronic Poll Book.....	5
A.	Precinct Central Touchpad Application and Polling Place Device	5
B.	Precinct Central Hardware.....	5
C.	Precinct Central Console.....	5
D.	Precinct Central Data Studio.....	6
E.	Thermal Receipt Printer(s).....	6
F.	Networking Configuration.....	6
III.	Evaluation Approach	7
	System Demonstration	7
	Documentation Review	7
IV.	Examination Processes and Procedures	8
	System Demonstration	8
	Documentation Review	8
V.	Examination Results	9
	System Demonstration Results	9
	Conformance to statutory requirements	9
	Review of system capabilities	9
	Level of compliance with Commonwealth IT policies	9
	Documentation Review Results	10
VI.	Observations	11
VII.	Conditions for Certification	12
VIII.	Recommendations.....	19
IX.	Conclusion	20

X.	Attachment A – Statutory Requirements	21
XI.	Attachment B - EPB Functionalities.....	25
	Voter Check-in Processes.....	25
	Usability/User Interface	25
	Security and Chain of Custody	26
XII.	Attachment C – Commonwealth IT Policies	27
XIII.	Attachment D – Supported Peripherals.....	32
XIV.	Attachment E – Sure Voter History Update Format.....	33

I. Introduction

Pennsylvania’s voter registration law, 25 Pa.C.S. § 1101, *et seq.* (“the law”), 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 a request from Tenex Software Solutions (Tenex), the Pennsylvania Department of State (Department) evaluated the Precinct Central 6.1.5 Electronic Poll Book (EPB) system, including the Precinct Central Console software that displays and tracks data sent to the Precinct Central Console server from Precinct Central electronic pollbook devices during an election in near-real time. This evaluation was undertaken to ensure that the system complies with all the applicable requirements of the law, including the regulations implementing the law, 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 changes between Precinct Central 3.2.0.1, the previously certified version of the EPB system, and Precinct Central 6.1.5 include performance and security upgrades, maintenance, functionality and quality updates.

The demonstration of Precinct Central 6.1.5 occurred on Monday, February 2, 2026, and was led by Nick Centonze, Project Manager representing Tenex. Casey Brady, Voting Systems Analyst, represented the Secretary of the Commonwealth.

II. The Precinct Central 6.1.5 Electronic Poll Book

The Precinct Central 6.1.5 EPB demonstrated for use in Pennsylvania included the following components as identified in the documentation submitted by Tenex:

A. Precinct Central Touchpad Application and Polling Place Device

The electronic pollbook software is pre-loaded on up to 11th generation Apple iPad tablets with the applicable poll book software version for the jurisdiction. It is used to display voter registration data in an electronic format to perform voter search, verification, and ballot issuance at polling places during an election event.

B. Precinct Central Hardware

The Precinct Central Touchpad hardware consists of a proprietary Flip and Share stand and Apple iPad tablet. The stand securely houses the tablet in the selected enclosure. Once the tablets are installed into the stands, no additional setup or configuration is required to use all features of the Precinct Central electronic pollbook.

The Precinct Central Touchpad includes one USB-C charging port that will charge the iPad tablet's internal battery while connected to power. When disconnected from power, the tablet's internal battery will provide up to ten hours of power to the tablet to allow for uninterrupted voter check-in. Optional accessory Bluetooth printers Epson TM-M30, TM-P80, Epson TM-L100 require power from outlets and do not affect tablet battery life meaningfully.

C. Precinct Central Console

The EPB system includes a real-time comprehensive monitoring platform that allows staff to monitor devices, users, communications, and performance metrics in a secure computing environment. Precinct Central Console is also the election office portal for all pre-election setup activity and post-election reconciliation, auditing, and exporting of voter history updates.

D. Precinct Central Data Studio

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.

E. Thermal Receipt Printer(s)

Optional COTS (Commercial-Off-The-Shelf) printers connected to the Apple iPad used to generate reports as required by the jurisdiction. The printer uses continuous feed thermal paper. Refer to Attachment D: Pollbook Components for specific printer model information.

F. Networking Configuration

The Precinct Central 6.1.5 system presented for evaluation provides the following operational communication structure configurations:

- Standalone Electronic Pollbook: Single unit, with no communication among devices within the polling location or across polling locations within the jurisdiction.
- Local Area Network Communication (Peer to Peer): Multiple units (up to six on a single wireless router) in a single location communicating via a connection to a secured wireless router device.
- Wide Area Network Communication (Host-Server Connected): Multiple units (up to 15 on a single MiFi device) in a single location and/or across a jurisdiction communicating to Host Server via a connection to a secured wireless modem and router device with an external internet connection.

The initial configuration of Precinct Central 6.1.5 presented for evaluation was identified as a Wide Area Network Communication. The Department is still in the process of evaluating the connectivity options that can be allowed securely for electronic poll books and will continue engaging Tenex as these evaluations continue. Hence, the Precinct Central 6.1.5 approval in this report is limited to Local Area Network Communication (Peer to Peer) where multiple Precinct Central 6.1.5 EPB units in the polling place communicate with each other via a secured wireless router device.

III. Evaluation Approach

To evaluate whether Precinct Central 6.1.5 can be successfully used for elections in the Commonwealth of Pennsylvania and meets all the requirements mandated by the law and the Pennsylvania Election Code, the following approach was used: (1) System Demonstration; and (2) Documentation Review.

Precinct Central 6.1.5 is an update to Precinct Central 3.2.0.1, which is approved for use in Pennsylvania. The Department leveraged details from the approval of Precinct Central 3.2.0.1 where applicable.

System Demonstration

The Department requires a System Demonstration on a field-ready system to examine and confirm that the EPB satisfies all the statutory requirements. The demonstration also allows the Department to gain a broad understanding of system capabilities.

Documentation Review

The Department requested the following documentation from Tenex for review:

1. System Specifications;
2. Hardware/Software/Peripherals/Additional Equipment Requirements;
3. Technical Data Sheet;
4. User Manual;
5. System Maintenance Manual;
6. Usability Reports;
7. Languages Supported;
8. System Change Notes; and
9. Security and Penetration Testing Reports from other states using the system;

Department staff completed a thorough review of the documentation provided by Tenex.

IV. Examination Processes and Procedures

System Demonstration

A Tenex representative demonstrated the Precinct Central 6.1.5 system on February 2, 2026. The demonstration included an end-to-end set up and capability walkthrough of the submitted EPB configuration. Tenex used test data supplied by the Department to configure the electronic poll book system for the demonstration. 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) to evaluate the system security posture and level of compliance with the Commonwealth Information Technology Policies (ITPs) outlined in Attachment C of this report.

Documentation Review

The Documentation Review consisted of analyzing the system specifications, release notes, user manuals and configuration recommendations pertaining to the Precinct Central 6.1.5 system. EPBs are highly configurable distributed systems, typically consisting of networked tablets or laptops used at polling places to check-in voters. They work in conjunction with a central server performing management functions, which include preparing the election data and preparing voter history updates. The Documentation Review was conducted to confirm that the system can be efficiently used for elections in the Commonwealth of Pennsylvania and to aid in deciding whether the EPB connectivity configuration should be approved for use in Pennsylvania.

V. Examination Results

System Demonstration Results

Below is a summary of the Department's findings from the evaluation of the Precinct Central 6.1.5 EPB system regarding statutory requirements, necessary system capabilities, and Commonwealth IT policies.

Conformance to statutory requirements

The vendor successfully demonstrated that the EPB system conforms to the statutory requirements outlined in Pennsylvania law. The demonstration of Precinct Central 6.1.5 proved that the system can be configured to meet the statutory requirements. See Attachment A for the list of statutory requirements discussed and validated during the demonstration.

Review of system capabilities

The Department reviewed the overall functional and nonfunctional capabilities of the system during the demonstration and documentation review. See Attachment B for the list of system functional and nonfunctional capabilities discussed during the demonstration and a brief overview of the discussion points.

Level of compliance with Commonwealth IT policies

The Department provided Tenex with a copy of the Commonwealth of Pennsylvania IT policies relating to the security of distributed systems and system connectivity. The Department also provided Tenex with a questionnaire which they completed and submitted as part of the examination request. The Department set aside time during the demonstrations to discuss the security architecture of the system. The written response to the questionnaire and the security discussion with the Tenex technical team during the demonstrations allowed Department staff to evaluate the system's level of compliance with Commonwealth IT policies and to understand the security features of the system.

See Attachment C for the specific policies and submission summary discussed during the demonstration.

Documentation Review Results

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

The demonstration and documentation review determined that Precinct Central 6.1.5 consists of Apple iPad tablets configured as terminal kiosks to perform voter check-in activity at the polling place doesn't require additional peripherals to perform voter lookup and check-in functionality. Election preparation and monitoring activities are performed using Precinct Central Data Studio and Precinct Central Console. The data from the Statewide Uniform Registry of Electors (SURE) system needs to be prepared by the Tenex data conversion team, and the encrypted election data needs to be loaded onto the tablets.

The system configuration presented for evaluation is represented as Local Area Network Communication (Peer to Peer), where multiple units in a single location or polling place are communicating via encrypted Wi-Fi connection to other Precinct Central Touchpads via a router.

VI. Observations

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

- A) Precinct Central 6.1.5 EPB uses software configuration features to determine the final functional behavior of the system. Even though the demonstration and subsequent evaluation 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 deployed system security posture will depend on the parameters selected during setup. This will necessitate validating the configuration during and after the setup activity to ensure that the system is configured in a secure manner.
- C) Precinct Central 6.1.5 election setup requires the involvement of a Tenex data conversion team to prepare the data to be loaded onto the tablets. The data extracted from the SURE system is transferred via secure file transfer to Tenex for conversion services. The Tenex team prepares the data, and the converted data is then transferred back to the county to be loaded onto the tablets. To avoid data compromise, the data transfer and conversion services that occur outside of county IT offices will require strict monitoring and access control policies, as well as documentation of compliance with those policies. All these data transfers must use encrypted processes.

VII. Conditions for Certification

Based on the evaluation, the Secretary of the Commonwealth of Pennsylvania approves Precinct Central 6.1.5 subject to the following conditions:

- A. The tablets in operation at a polling place can communicate among each other to synchronize voter check-in data during polling hours. Any data transfer required between the Precinct Central Console and tablets must happen outside of polling hours. Therefore, the tablets must be configured to prevent communication with the Precinct Central Console server during polling hours.
- B. The tablets at an individual polling place communicating with each other must be configured and managed so they always meet and maintain secure data management and transfer standards, including those contained in Commonwealth ITP policies, and must 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 and used. 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: Voter Access Cards encoded on the EPB systems; USBs; SD cards; printers; CDs; etc.
- D. Jurisdictions implementing the Precinct Central 6.1.5 system must not use a driver’s license or ID card barcode scanning capability to check in voters. This is to avoid voters being asked for an ID when presentation of identification is not required by law. Counties must implement the system with the barcode scanning option disabled. The system must not present poll workers the option of checking in voters by scanning an identification card with barcode.
- E. Jurisdictions printing barcodes at check-in to activate ballot-marking devices must ensure that the specific integration details are demonstrated and technical documentation about the integration is submitted for evaluation to the Department of State. Any

integrations to voting system ballot-marking devices must be submitted for approval separately.

- i. Jurisdictions implementing the use of barcodes to activate ballot marking devices must ensure that poll worker training emphasizes the need to double-check the accuracy of the ballot style activated.
- ii. Jurisdictions must ensure that during the Logic and Accuracy testing, all ballot-style activations are tested if integration with ballot marking devices is being utilized.

F. Tenex must work with implementing jurisdictions to ensure that jurisdictions have a process to provide vote history data for updates to the SURE system in a timely manner, and not later than the Thursday after the election. The process must allow counties to gather check-in information from polling place devices and create an extract in the format required by the SURE system. The existing system extract format is listed in Attachment E. Counties purchasing Precinct Central 6.1.5 must work with the Department's Bureau of Elections ("Bureau") to finalize the process of voter history updates during each election cycle. Tenex must be able to adhere to the extract format and timing of the update suggested by SURE system administrators.

G. Tenex must work with implementing jurisdictions to ensure that there is a defined plan to load voter data and prepare the poll books for use on Election Day. The plan must ensure that counties can capture all the voter poll book data updates required for use on Election Day. The plan must be reviewed and approved by the Bureau to ensure that the extracts can be generated from the SURE system on the required dates.

H. Jurisdictions implementing Precinct Central 6.1.5 must work with Tenex to check and validate data loaded onto pollbooks as part of pre-election testing to ensure all correct voter and configuration data has been captured for the current election. The following data points should be reconciled before deploying the electronic poll book system:

- i. Number of precincts, polling places and ballot styles (if applicable);
- ii. Total voters loaded by precinct and any flags required for displaying appropriate check-in messages and instructions for poll workers;
- iii. If the pre-election data load process includes multiple updates to voter data, data must be reconciled each time an update to voter data is provided; and

- iv. All required check-in scenarios for election day are appropriately configured.
- I. Jurisdictions implementing Precinct Central 6.1.5 must implement a post-election reconciliation process that includes the following points of comparison:
 - i. Reconciling check-in data from the poll books at each polling place with the number of ballots cast at the polling place; and
 - ii. Reconciling the voter history update file generated by electronic poll book system with the total number of check-ins at the polling place.
- J. Counties purchasing or leasing the Precinct Central 6.1.5 system must work with Bureau to decide what portion of the data from the SURE system can be shared with the vendor for use in electronic poll books. The counties shall not allow the vendor to run any data extraction utilities against the SURE database/system. Any data transfer must happen via a file extract and secure file transfer process and must be encrypted. The extract must not contain any additional data elements other than what was shared during the evaluation, and the data elements and sharing mechanism must be approved by the Department's Bureau of Elections. Counties must ensure the accuracy of data loaded onto the EPB system and maintain appropriate reports as necessary for auditability.
- K. Any data transfer required during the process of election setup and voter history updates between the county and Tenex data conversion services must happen via secure file transfer processes. The file transfer and download must be tracked and audited to make sure that data has not been accessed by unauthorized personnel.
- L. Portable media used to transfer files between any components of the EPB system must be new, unmodified and not refurbished. Alternatively, removable media that is being reused must be 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, loss or damage.
- M. Jurisdictions must ensure that the system does not capture poll workers' Social Security Numbers or any poll worker personally identifiable information ("PII") as part of the "add poll worker" workflow, or any other process. Counties must consult with the Department on any questions concerning what data can be captured.
- N. Any unused ports in tablets used at polling places must be sealed with tamper-evident seals, and practices prescribed for and followed by poll workers must ensure the

frequent checking of the tamper-evident seals and documentation of anomalies, including actions if tampering is discovered. Jurisdictions must configure the tablets and transport cases with tamper-evident and tamper-proof seals and locks as applicable to ensure physical security.

- O. Counties purchasing or leasing the Precinct Central 6.1.5 EPB system must work with Tenex and the Department's Bureau of Elections to do the following:
- i. Implement Precinct Central 6.1.5 EPB system in a manner that satisfies all statutory requirements outlined in the law, its regulations, and the Pennsylvania Election Code. The parameter configurations and the text of informational messages must be approved by the Bureau of Elections;
 - ii. Implement Precinct Central 6.1.5 EPB system in a secure manner that complies with applicable county and Commonwealth IT policies and any best practices published by the Bureau of Elections. The system configuration, connectivity setup, password configuration and password management policies must be approved by Bureau of Elections; and
 - iii. Implement Precinct Central 6.1.5 EPB system with sound administrative practices and proper chain of custody in the same manner as counties deploy electronic voting systems.
- P. Counties implementing Precinct Central 6.1.5 must change all default passwords during implementation. County election officials must implement processes to confirm and maintain records that default passwords were changed before fielding the system. The proof must be documented using export of the system log files whenever possible. A screenshot of the password change action performed at the county elections office or otherwise documenting the password change during acceptance testing can meet this condition. County election officials with administrative access on Precinct Central Console server must take proper precautions for password management and protection. The passwords and permissions management must, at a minimum, comply with the password requirements outlined in NIST 800-63-4. This publication can be accessed at <https://pages.nist.gov/800-63-4/>.
- Q. Counties must have a contingency plan to ensure that an election will not be affected should any component (including connectivity and power supply) of the EPB

system fail, or any or all tablets in use at a polling place 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 the Department’s Bureau of Elections. At a minimum, the contingency plan must ensure the availability of a full voter list and a process for maintaining and reproducing a list of voters who have already checked in if the EPB fails during voting hours.

- R. Tenex must notify the Department of State of any changes made to the Precinct Central 6.1.5 EPB system. This includes any changes to the software and to the environment of the EPB system, including but not limited to Tenex’s development locations, cloud service vendors, or data center locations, for example.
- S. Tenex must escrow a copy of the code, trusted build, any verification/identification software used, and installation instructions for safekeeping to the Commonwealth of Pennsylvania; add the Commonwealth as a beneficiary to any escrow accounts they have for safekeeping the Precinct Central 6.1.5 code; and provide written notification of this status to the Department, with an update on any successor escrow parties.
- T. Tenex must provide fully prepared and version-controlled system manuals for counties purchasing or leasing the EPB. The manuals must clearly identify each user-configurable parameter. Final user manuals must be submitted to the Department before the sale or lease of the product or delivery in Pennsylvania.
- U. Counties must perform a thorough evaluation and user acceptance test of the EPB system before purchase or lease. This test should include all expected activities occurring as part of the election including interactions with the SURE system. This approval report is based on a demonstration done by the vendor and a documentation review. Demonstration by the vendor cannot be considered equivalent to testing.
- V. Jurisdictions implementing the Precinct Central 6.1.5 system must keep an inventory of all the device identifiers deployed in the county. The systems must be audited at the beginning of the election cycle for any required maintenance. Any devices decommissioned, returned or otherwise disposed of at the end of a lease or end of useful life must be permanently erased of any software and voter data. Counties must implement processes to ensure that the “clean wipe” is validated, documented, and maintained for

audit purposes. Best practices on equipment sanitization are documented in publication NIST SP 800-88r2 and can be accessed at

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf>.

- W. 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 and/or archived to physical media with access control as soon as it is no longer required, or no later than ninety (90) days after Election Day. Voter data shared with the vendor must be tracked and deleted to avoid data breaches. Counties must retain, as required by law, archived copies of data sent and received from the vendor for audit purposes. Tenex must maintain and retain audit logs of every data access event and make those audit logs available for inspection to the counties or the Department's Bureau of Elections upon request.
- X. All jurisdictions implementing Precinct Central 6.1.5 must carry out full logic and accuracy testing on each device prior to every election in which Precinct Central 6.1.5 will be used and must maintain records of that 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.
- Y. Tenex must provide audit log specification documentation to the Department's Bureau of Elections and counties purchasing or leasing the Precinct Central 6.1.5 system. County election officials and IT personnel must work with Tenex to understand the system logging capabilities. The county must be able to identify and gather logs that provide an audit trail of the transactions at the polling place, and application suite audit logs or operating system logs that aid in identifying and managing security incidents, fraudulent activity, and operational problems. Processes must be implemented to harvest and safekeep the logs after every election for future analysis and review.
- Z. Counties using the EPB must implement reconciliation processes at the close of polls to avoid any discrepancies between ballots and voter check-ins recorded on the EPB. Checklists should be developed for poll workers to ensure compliance with all

requirements and reduce the chance of human error. Counties should also work with Tenex to produce quick reference cards for use by poll workers at the polling place on Election Day.

- AA. Any COTS components of certified EPB systems must be hardened with only the required software for the EPB system. No additional software applications or utilities shall be installed on the equipment being used at the polling place.
- BB. Counties must work with certified EPB vendor to ensure that the electronic poll books are configured in such a way that poll worker access to the system is restricted to performing check in activities required at the polling place only. The system must preclude the poll workers from accessing any other utilities and operating system files.

VIII. Recommendations

The Secretary makes the following recommendations to the counties purchasing or leasing the Precinct Central 6.1.5 EPB system:

- A. Counties should consider using the EPB in pilot mode during the first use in an election. This allows counties to ensure that all appropriate checks and balances are in place before using the EPB system in full production mode. Larger counties should also consider implementing the EPB in a phased approach to mitigate any unforeseen issues that may arise during implementation.
- B. The Secretary urges counties to ensure that all poll workers and election officials receive appropriate training and are comfortable using the EPB. The training activities should include but not be limited to hands-on training on devices to perform election set up and operations at a polling place and cyber hygiene practices and procedures for detecting cyber-attacks. The training should ensure that poll workers and election officials can detect any warnings that signal cyber-attacks and immediately respond to it. Involvement of poll workers during the implementation project from start to finish, with onsite training at the polling place, is recommended. Annual training for all poll workers and local election district personnel is also recommended, with documentation of training content and attendees. Tenex must work with counties to ensure that all training materials are updated as required and maintained for training activity before each election.
- C. The Secretary recommends that counties purchasing the Precinct Central 6.1.5 EPB system perform proof of concept testing onsite at all polling places to ensure peer-to-peer connectivity and power supply availability. The Secretary further recommends that the test is conducted with a test system using components of the same make, model and configuration as that being used on Election Day.
- D. Counties using the Precinct Central 6.1.5 EPB system should develop a disaster recovery plan that includes the possibility of a data breach or cyberattack on the EPB. Such a plan must identify the means of continuing the election in case a disaster occurs during the election.

IX. Conclusion

Based on the demonstration, documentation review, and consultation with Department staff, the Secretary of the Commonwealth concludes that the Tenex Precinct Central 6.1.5 EPB meets all applicable requirements set forth in the law, its regulations, and the Pennsylvania Election Code, and can be used for checking in voters during elections, provided that all the conditions listed in Section VII of this report are met.

X. Attachment A – Statutory Requirements

Statutory 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 EPB must provide	Yes

for 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 Precinct Central 6.1.5 maintains redundancy when multiple Touchpads are used at the polling place. The system allows the 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 indicating that the voter had already voted. In an environment where there are multiple Touchpads connected, data synching between the devices must be operation 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)). Demonstration Comments: The application has a "Poll Worker Initial" box that captures the initials of the poll worker performing the check in.	Yes
Indication of whether the elector needs assistance to vote and, if so, the nature of the disability. (25 Pa.C.S. § 1402(b)(2)).	Yes
The date of birth of the registrant. (4 Pa. Code § 183.11(b)(4)).	Yes
The SURE registration number of the registrant. (4 Pa. Code § 183.11(b)(5)).	Yes
The following elector's affirmation must appear above the signature area: "I hereby certify that I am qualified to vote in this election." (25 P.S. § 3043)	Yes
An identification of whether the registrant's status is active or inactive. (25 Pa.C.S. § 1901(c); 4 Pa. Code § 183.11(b)(6)).	Yes
Voter Status Flags Required by the SURE System	
For voters who are "inactive," affirmation is required. (25 Pa.C.S. § 1901(c) and (d)(3); 4 Pa. Code § 183.11).	Yes
"ID Required"- Identification of whether the elector needs to present voter identification. An elector who appears to vote in an election district for the first time must present valid voter identification. (25 P.S. § 3050(a)).	Yes

“Absentee or Mail-in Ballot”- An elector who received an absentee or mail-in ballot is ineligible to vote in the municipality on Election Day, although he or she may vote by provisional ballot if the district register does not show that the elector voted the absentee or mail-in ballot. The elector may vote by regular ballot if the mail ballot and envelope are remitted, and the voter signs the required declaration. (25 P.S. § 3146.6(b) and § 3150.16(b))	Yes
--	-----

XI. Attachment B - EPB Functionalities

Voter Check-in Processes

The following “check-in”/voter handling scenarios were demonstrated:

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

Usability/User Interface

The following capabilities/functions of the EPB system were demonstrated:

- a) Set up and procedures for setting up the field system/poll pad.
- b) Screen navigation capabilities.
- c) Languages Supported by the system.
- d) System power up and shutdown procedures.
- e) System help availability.

Security and Chain of Custody

The following security features/functions of the EPB system were demonstrated:

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

XII. Attachment C – Commonwealth IT Policies

- 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.

Submission Summary: Precinct Central touchpad uses Apple iPads for field systems and does not use any antivirus software. Tenex represented that the iPad’s innate security specifications satisfy FIPS 140-2 compliance requirements, and Precinct Central Console and Precinct Central Data Studio include various forms of protection which include Microsoft Defender. Patching is controlled by Tenex Software Solutions, and the timeframe of patching is informed by risk/vulnerability matrices. Patches that mitigate identified security vulnerabilities will be applied to all customers as a preventative measure.

The submissions and discussions suggest that the 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.

Submission Summary: The submission details Amazon Web Services instance firewall policies. Tenex maintains a block list that is periodically refreshed to avoid ransomware/malware. The submission suggests that the system can be configured to satisfy compliance to this policy. The submission indicates that the hardened Windows 2019 server is implemented in accordance to the CIS Benchmarks guideline for establishing a secure configuration posture for IT infrastructure.

- C) ITP-NET001 – Establishes enterprise-wide standards for Wireless Area Network (LAN) technologies and their secure usage in production environments by assurance of information security to protect confidentiality, integrity, and appropriate access to information.

Submission Summary: Tenex responded with wireless networking diagrams showcasing the network configuration used in a single polling place using a Wi-Fi via securely configured wireless MiFi hotspot.

- D) ITP-SEC019 and ITP -SEC016 – Establishes policies and procedures to protect Commonwealth electronic data.

Submission Summary: Tenex has engaged the U.S. Department of Homeland Security to perform regular security assessments and tests on its servers and infrastructure that house pollbook services, including network mapping and vulnerability scanning, phishing tests, web application and database evaluations, and bi-annual penetration testing. Tenex also participates in weekly CISA Cyber Hygiene Reports that perform scans for vulnerabilities and potential risks and is a member of IT-ISAC.

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

Submission Summary: All data at rest is encrypted, and Precinct Central Touchpad use hardware encrypted file systems. The implementation uses encryption and hashing together for configuration files to ensure there is additional protection.

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

Submission Summary: Tenex represented that they have a defined process in responding to cybersecurity incidents coordinated and escalated through an enterprise-wide contact following any industry and internal best practices for reporting and incident management.

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

Submission Summary: Tenex represents that PII data in the poll book system is protected via encryption, and access to this data is controlled on a role-based hierarchy, controlled by the County. Tenex follows security requirements for voter registration data and only users with sufficient privileges are allowed access. These data records are not made available in public record requests and can be included or not in voter file downloads (based on selections). Security privileges can be configured to only allow certain county users to see voters flagged as Confidential.

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

Submission Summary: Tenex represented that their organization follows policies to avoid unauthorized physical access to their facility, including access control systems and surveillance monitoring of the facility. Physical access to sensitive physical documents or storage devices is controlled to avoid unauthorized data access, and data sanitization practices for devices no longer in use are followed to ensure that sensitive data cannot be recovered.

The physical security of the EPB devices at the polling place is ensured by using tamper-evident locks and seals placed onto the protective cases the EPB is transported inside. The Apple iPad used for the Precinct Central Touchpad does not include ports for attaching external storage devices.

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

Submission Summary: The submission and discussion indicated that data transmitted between system components uses encryption protocols that demonstrate compliance with this policy. Any file transfer is done using secure file transfer processes. The system uses a Wi-Fi connection to synchronize check-in data, and the transmission of this synchronization data is encrypted. The communication payload is also encrypted.

Data Transfer	Encryption Method
Data Transferred from Precinct Central Console to Precinct Central Touchpads	All data is encrypted with AES 256 encryption using TLS 1.2 connection.
Data transferred between Precinct Central Touchpads	All data is encrypted with AES 256 encryption using TLS 1.2 connection.
Data transferred from Precinct Central Touchpads to Precinct Central Console via approved Wi-Fi networks	All data is encrypted with AES 256 encryption using TLS 1.2 connection.

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

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

- 1) ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data Refer to Item D above.
- 2) ITP-SEC020 - Encryption Standards for Data at Rest. Refer to Item E above.

3) ITP-SEC031 - Encryption Standards for Data in Transit. Refer Item I above

K) ITP-SEC035 - This information technology policy establishes policies, responsibilities, and procedures for connecting and using mobile communication devices to access commonwealth IT resources.

Submission Summary: The EPB solution utilizes an iPad at the polling place which is not connected to the Commonwealth network or IT resources, but the submission suggests that the Precinct Central Touchpad can be configured with the appropriate configuration mentioned in the policy.

L) ITP-SEC007 - This Information Technology Policy establishes minimum standards for the implementation and administration of users, systems, networks, devices, application account IDs, passwords, and requirements around multi-factor authentication.

Submission Summary: The system has multiple levels of password protection and all of them are configurable to satisfy the Commonwealth policy. The Touchpads provide capability for 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. 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.

XIII. Attachment D – Supported Peripherals

Below is a list of peripheral devices that are included in testing of the Tenex Precinct Central Touchpad application for the Apple iPad tablets. The list is from the Compatible Peripherals.pdf document submitted with the Technical Data Package for Tenex 6.1.5

Device Name	Interface	Required
Flip and Share Stand	N/A	Highly Recommended
Stylus	N/A	Optional
10-Foot Charging Cable	USB-C	Optional
Epson TM-m30 Bluetooth Printer	Bluetooth	Optional
Epson TM-p80 Powered Bluetooth Printer	Bluetooth	Optional
Epson TM – L90 Label Printer	Bluetooth	Optional
Gemstar 2x2 Carrying Case	N/A	Optional
Gemstar 1x1 Carrying Case	N/A	Optional

XIV. Attachment E – Sure Voter History Update Format



E-Pollbook VH
Example.csv

(All fields are required)