

COMMONWEALTH OF PENNSYLVANIA

DEPARTMENT OF STATE

**RESULTS OF ELECTRONIC POLL BOOK Knowink Pollpad 3.1.0
EVALUATION**



Issued By:



Leigh M. Chapman
Acting Secretary of the Commonwealth
November 3, 2022

RESULTS OF THE KNOWINK POLL PAD 3.1.0 ELECTRONIC POLL BOOK EVALUATION

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 of Knowink, the Department of State (Department) evaluated the Poll Pad 3.1.0, Electronic Poll Book (EPB) to ensure that the system complies with all the applicable requirements of Act 3, including the regulations implementing Act 3, 4 Pa. Code §§ 183.1 et seq., and the Pennsylvania Election Code, 25 P.S. §§ 2601, et seq., and therefore can be used in Pennsylvania elections. The evaluation consisted of a system demonstration via video conference conducted by Daniel Peters, Eastern Regional Manager representing Knowink, email communications and conference calls with Knowink personnel, and documentation review. Mitch Milleville, Product Manager, also attended the demonstration representing Knowink. The system demonstration video conference occurred on April 1, 2022. Sindhu Ramachandran, Voting Systems Analyst; Matt Ruch, Voting Systems Analyst, Bureau of Elections; John Hartzell, Deputy Chief Counsel, Office of Chief Counsel; attended the demonstration representing the Secretary. Department’s election security collaboration partners, the PA National Guard Cyber Branch team, also attended the demonstration to assist in evaluating the EPB system security posture. The demonstration was completed via video conference to enable completion of approval activities, considering that the Department had viewed a previous version of the same system, the changes were specific to the EPB application software, and the submission for approval was in close proximity to the primary election.

II. Poll Pad 3.1.0 ELECTRONIC POLL BOOK

The Poll Pad 3.1.0 EPB demonstrated for use in Pennsylvania included the following

components:

1. Poll Pads – Poll Pads are iPads configured for use at the polling place to perform voter check-in activities. The Poll Pad 3.1.0 software application installed on iPad allows poll workers to perform the polling place activities typically performed using a printed paper poll book. The Poll Pads work in kiosk mode, allowing the poll workers to access only the poll pad application.
2. ePulse 3.1.0 (ePulse) - ePulse is a web-based platform that supports the management functions of the EPB system. ePulse allows the county election officials to prepare the voter and precinct data for use on Poll Pads. It also, when permitted, can provide an Election Day monitoring platform that connects election officials to polling places, but this function can also be inactivated. The system, when activated, can facilitate managing Election Day operations by providing functionalities like monitoring polling place status, hardware health, and system operational status. Monitoring functionalities can allow election officials to address potential issues and have better control of polling places on Election Day. The system also allows election officials to prepare customizable reports for analysis.
3. Poll Pad accessories, case and stand.

(Refer to Attachment D for a list of all the items in the Poll Pad EPB system case)

III. EVALUATION APPROACH, PROCEDURES AND RESULTS

A. Evaluation Approach

To evaluate whether Poll Pad 3.1.0 EPB can be successfully used for elections in the Commonwealth of Pennsylvania and meets all the requirements mandated by Act 3 and the Pennsylvania Election Code, the following approach was used: (1) System Demonstration; and (2) Documentation Review. Poll Pad 3.1.0 is an update to Poll Pad 2.5.1, which is

approved for use in Pennsylvania. The enhancements included were represented in the approval application. The Department leveraged details from the approval of Poll Pad 2.5.1 where applicable.

The Department requires a System Demonstration to examine and confirm on a field-ready system that the EPB satisfies all the statutory requirements. The demonstration also allows the Department to gain a broad understanding of the system capabilities. The documentation review consisted of analyzing the system specifications, user manuals, state certification and third-party test reports pertaining to the Knowink Poll Pad system. Electronic poll books are heavily configurable distributed systems, typically consisting of networked tablets or laptops used at polling places to check-in voters. They work in conjunction with a central server performing the management functions, which include preparing the election data, performing voter history updates, and monitoring deployed devices at polling places. The documentation review was conducted to confirm that the system can be efficiently used for elections in the Commonwealth of Pennsylvania and to aid in deciding the EPB connectivity configuration to be approved for use in Pennsylvania.

B. Procedures

1. System Demonstration

A Knowink representative demonstrated the Poll Pad 3.1.0 system on April 1, 2022. The demonstration included a polling place capability walkthrough of the Apple iPad tablet installed with the Poll Pad 3.1.0. application used at the polling place, a discussion of preparing and loading the data to the Poll Pads, and an explanation of the system security features. Knowink used the test data supplied by the Department 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.

2. Documentation Review

The Department requested the following documentation from Knowink for review.

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

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

3. Results

a. System Demonstration Results

Poll Pad v3.1 is an upgrade to Poll Pad v1.3.3, approved for use in Pennsylvania. The system functionalities largely remained the same with enhancements to the application security and addition of features to support certain jurisdiction specific requests.

- i. Conformance to statutory requirements - The vendor successfully demonstrated that the Poll Pad 3.1.0 EPB system conforms to the statutory requirements outlined in Pennsylvania law. The demonstration proved that the system can be configured to meet the statutory requirements. *See Attachment A* for the list of statutory requirements discussed and validated during the demonstration.
- ii. Review of system capabilities - The Department reviewed the overall system capabilities during the demonstration and documentation review. *See Attachment B* for a summary of the demonstration discussion points.
- iii. Level of Compliance with Commonwealth IT policies and system security posture – The Department provided Knowink with a copy of the Commonwealth of Pennsylvania IT policies relating to the security of distributed systems and network connectivity. The Department also provided Knowink with a questionnaire to

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

b. Documentation Review Results

Department staff analyzed the documentation provided by Knowink 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 Poll Pad 3.1.0 consists of iPads installed with Poll Pad 3.1.0 application configured as Poll Pad kiosks (Poll Pads) to perform voter check-in activity at the polling place, and ePulse 3.1.0 hosted on a cloud server to perform administrative functions. The system can allow the following modes of configuration, but these can also be deactivated where not permitted:

- A live (fully connected) mode where data flows continuously between cloud-based ePulse servers and all Poll Pads 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 Poll Pads to the ePulse cloud server. The data transmitted does not contain any voter check-in data. This configuration, if permitted, allows monitoring of the polling place devices remotely;

- A peer-to-peer communication mode where the Poll Pads at a polling place communicate to each other without any connection to the ePulse cloud server. This configuration allows voter check-in data to sync up in a polling place, thus allowing the use of multiple Poll Pads at a polling place.

The networked environment, if activated, could make the EPB system vulnerable to hacking attempts, possibly compromising the integrity of check-in data and/or allowing unauthorized access to voter data. The Department staff analyzed the connectivity configurations discussed during the demonstration in conjunction with the documentation provided and existing Department test protocols for Electronic Poll Books to determine the connectivity approved for use in Commonwealth of Pennsylvania, which minimizes the security risks and maximizes the benefits in moving to an EPB solution.

c. Observations

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

- 1) Poll Pad 3.1.0 uses software configuration features to determine the final functional behavior of the system. In addition to the demonstration and subsequent analysis and evaluation performed demonstrating that the system can be configured to satisfy all the statutory requirements, the Department also requires documentation after purchase confirming that the system setup complies with the approved configuration.
- 2) Poll Pad 3.1.0 includes configurable functionalities added to be system executables to satisfy certain jurisdictional specific requests.
- 3) The deployed system security posture will depend on the parameters selected during setup. This will necessitate validating the configuration during and after setup to ensure that the system is configured in a secure manner.
- 4) Poll Pad 3.1.0 when deployed in live (fully connected) and restricted server communication mode can communicate with the cloud server located outside of the polling place and transmit transactional and operational data throughout Election Day

to the ePulse server. The live (fully connected) and restricted communication mode maintain a communication channel between the polling place and cloud server for the entire time the polls are open on Election Day. These can be disconnected, which is the only approved setting during polling hours in Pennsylvania.

- 5) The data from Statewide Uniform Registry of Electors (SURE) system is prepared for loading on Poll Pads using the ePulse system. The data preparation process is reconciled via a high-level onscreen summary of the records processed on ePulse, but the prepared data will need to be validated for accuracy and completeness after loading to the Poll Pads to avoid any data inconsistencies on Election Day.

IV. CONDITIONS FOR APPROVAL

Based on the evaluation, the Secretary of the Commonwealth of Pennsylvania approves Poll Pad 3.1.0 subject to the following conditions:

- A. The Poll Pads in operation at a polling place **must not** be configured to communicate to the ePulse server during the polling hours on Election Day. The tablets in operation at a polling place can communicate only to each other to synchronize voter check-in data between each other at the polling place during the polling hours. Any data transfer required between the ePulse system and Poll Pads may only happen outside of polling hours. Therefore, the Poll Pads must be configured to prevent communication with the ePulse server during polling hours.
- B. The tablets at an individual polling place communicating with each other must be configured and managed in a secure manner and may never connect to a publicly accessible network. The network at the polling place must be a “closed network” allowing only components of the EPB system to connect and encryption must be enabled. The security settings must prevent other devices from detecting and connecting to the network at the polling place.

- C. Any components which are/were part of the EPB system, including removable media, must not be connected to the Electronic Voting system. This includes, but is not limited to: PEB encoders and Voter Access Cards encoded on the EPB systems; USBs; SD cards; printers; CDs; etc.
- D. Jurisdictions implementing Poll Pad 3.1.0 EPB system **must not** use the driver's license or ID card bar code scanning capability to check in voters. This is to avoid voters being asked for presentation of identification when not required by law. Counties must implement the system with the bar code scanning option disabled. The system must not present poll workers the option of checking in voters by scanning an identification card with bar code.
- E. Jurisdictions printing barcodes at check-in to activate ballot marking devices must ensure that the specific integration details are demonstrated and technical documentation about the integration is submitted for evaluation to the Department of State. Only Freedom Vote Tablet (FVT) integration is approved for use with this report. Any additional integrations to voting system ballot marking devices must be submitted for approval separately.
- F. Jurisdictions using the QR code for activating ballot styles on FVT must ensure that poll worker training emphasizes the need to double check to ensure that the correct ballot style is activated for every voting session.
- G. Jurisdictions must ensure that during the Logic and Accuracy testing, all ballot-style activations on FVT are tested.
- H. Jurisdictions must ensure that the system doesn't capture the poll worker Social Security Number (SSN) as part of the add poll worker workflow.

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

- J. Any unused ports in the Poll Pad used at the polling place must be sealed with tamper-evident seals. The Poll Pad case also must be locked and sealed.

- K. Counties purchasing the Poll Pad 3.1.0 EPB system must work with Knowink and Bureau of Elections to do the following:
 - 1. Implement Poll Pad 3.1.0 EPB system in a manner that satisfies all statutory requirements outlined in Act 3 of 2002 and the Pennsylvania Election Code. The parameter configurations and the text of informational messages must be approved by the Bureau of Elections.
 - 2. Implement Poll Pad 3.1.0 EPB system in a secure manner that complies with applicable county and Commonwealth IT policies and any directives or guidance published by Department of State Bureau of Elections. The system configuration, connectivity setup, password configurations and password management policies must be approved by the Bureau of Elections; and
 - 3. Implement Poll Pad 3.1.0 EPB system with sound administrative practices and proper chain of custody in the same manner as counties deploy Electronic Voting Systems.

Counties implementing Poll Pad 3.1.0 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 ePulse 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. This publication can be accessed at <https://pages.nist.gov/800-63-3/sp800-63-3.html>.
- L. Counties must work with Knowink to ensure that the Poll Pads are configured in kiosk mode or Guided Access Mode. The iPads must be hardened with only the required software for the EPB system. No additional software applications or utilities shall be installed on the Apple iPads being used at the polling place.
 - M. Counties implementing Knowink Poll Pad 3.1.0 EPB system shall implement at least two (2) Poll Pads per polling location and must allow peer-to-peer communication to enable check-in activity to synchronize between the Poll Pads. This is necessary to ensure data storage redundancy.
 - N. Jurisdictions implementing the Poll Pad 3.1.0 EPB system must keep an inventory of all the device identifiers deployed in the county. The systems must be audited at the beginning of the Election cycle for any required maintenance. Any devices decommissioned, returned or otherwise disposed of at the end of a lease or end of useful life must be permanently erased of any software and voter data. Counties must implement processes to ensure that the “clean wipe” is validated, documented, and maintained for audit purposes. Best practices on equipment sanitization are documented in publication NIST SP 800-88r1 and can be accessed at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
 - O. Counties must have a contingency plan to ensure that an election will not be affected should any component (including connectivity and power supply) of the EPB system

fail due to malfunction, cyber incident or other cause on Election Day.

The

contingency plan must ensure that no “check in” information is lost. The contingency plan must be reviewed and approved by the Bureau of Elections. At a minimum, the contingency plan must ensure the availability of a full voter list and a process for maintaining and reproducing a list of voters who have already checked in if the EPB fails during voting hours.

- P. Counties purchasing the Poll Pad 3.1.0 must work with the Bureau of Elections to decide what portion of the data from the Statewide Uniform Registry of Electors (SURE) system can be shared with the vendor. The counties shall not allow the vendor to run any data extraction utilities against the SURE database/system. Any data transfer must happen via a file extract and secure file transfer process, and must be encrypted. The voter data extract must not contain any additional data elements than what was shared during the evaluation. The data elements and sharing mechanism must be approved by the Bureau of Elections. Counties must ensure the accuracy of data loaded to the EPB system and maintain appropriate reports as necessary for auditability.
- Q. Counties purchasing the Poll Pad 3.1.0 must work with the Bureau of Elections to finalize the process of voter history updates. Knowink must be able to adhere to the extract format and timing of the update suggested by SURE system administrators.
- R. Knowink must notify the Department of State in writing of any changes made to Poll Pad 3.1.0 EPB system, including software, hardware, or configuration and present the system for approval before use in elections. This includes any changes to the software of the EPB system and to the environment of the EPB system, including but not limited to Knowink’s development locations, cloud service vendors, or data center locations, for example.

- S. Knowink must escrow a copy of the code, trusted build, any verification/identification software used and installation instructions for safekeeping to the Commonwealth of PA and add the Commonwealth as a beneficiary to any Escrow accounts they have for safekeeping of the Poll Pad 1.3.3 code.

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

- U. Counties must perform a thorough evaluation and User Acceptance Test of the EPB system before purchase. This test should include demonstrations of all expected activities occurring as part of the election, including interactions with the SURE system. This approval is based on a demonstration by the vendor and documentation reviews. Demonstration by the vendor cannot be considered equivalent to testing.

- V. Counties implementing the Poll Pad 3.1.0 must work with Knowink to define and implement policies on data retention and archiving of the EPB system, including external servers and any removable media. Any election data stored on devices outside of the county network must be deleted and/or archived to physical media with access control as soon as it is no longer required, or no later than ninety (90) days after Election Day. Voter data shared with the vendor must be tracked and deleted to avoid data breaches. Counties must retain, as required by law, archived copies of data sent and received from the vendor for audit purposes. Knowink must keep audit logs of every data access event and make those audit logs available for inspection by the counties or the Bureau of Elections, upon request.

- W. All jurisdictions implementing the Poll Pad 3.1.0 must carry out full Logic and Accuracy testing prior to every election on each device and maintain records of

this testing. The Department recommends creating a county-specific plan for Logic and Accuracy testing that includes all peripherals and anticipated check-in scenarios on Election Day, including any integrations. The vendor-supplied Logic and Accuracy checklist should be used as a reference but must not be accepted in lieu of a county-specific plan.

- X. Knowink must provide audit log specification documentation to the Bureau of Elections and counties purchasing Poll Pad 3.1.0 system. The county election officials and IT personnel must work with Knowink to fully utilize and optimize the system-logging capabilities. The county must be able to identify and gather logs that provide audit trails of the election data preparation and transactions at the polling place, and logs that aid in identifying and managing security incidents, fraudulent activity and operational problems. Processes must be implemented to harvest and safekeep the logs after each election for future analysis and review. The log files must be extracted and saved in a manner that allows identifying the device from which the logs files were extracted. The EPB log files must be retained for five (5) years in accordance with the statutory retention period for poll books.
- Y. Knowink must ensure that future releases of the software with enhanced security features are presented for approval to Department.

V. RECOMMENDATIONS

The Secretary makes the following recommendations to the counties purchasing the Poll Pad 3.1.0 EPB system:

- a) Counties should consider using the EPB in pilot mode during its first use in an election, in conjunction with printed poll books. This allows the jurisdictions to ensure that all appropriate checks and balances are in place before using the EPB system in full production mode. For larger counties, the county should also consider

- implementing 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 trainings at the polling place is also recommended. Knowink must work with counties to ensure that all training materials are updated as required and maintained for training activity before each election.
 - c) Counties using EPBs should implement processes of reconciliation at the open and close of polls to avoid any data discrepancies. Checklists should be developed for poll workers to ensure compliance with all requirements and to reduce the chance of human error. Counties should also work with Knowink to produce quick reference cards and/or help files for use at the polling place on Election Day.
 - d) The Secretary recommends that counties purchasing the Poll Pad 3.1.0 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.
 - e) Counties using the Poll Pad 3.1.0 EPB system should work with Knowink to develop and implement a plan that recognizes the possibility of a data breach or cyber attack on the EPB and prepares a mechanism for completing election activities. The plan should detail processes and procedures to be followed by poll

workers and election officials in the event of a cyber attack.

VI. CONCLUSION

Based on the demonstration, documentation review, and consultation with the Department staff, the Secretary of the Commonwealth concludes that the Knowink Poll Pad

2.5.1 EPB meets all the applicable requirements set forth in Act 3 of 2002 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
<p>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:</p> <ul style="list-style-type: none"> ▪ Memory Redundancy ▪ Data Preservation 	Yes

<ul style="list-style-type: none"> ▪ If the contingency for Electronic Poll Book failure is the printing of paper poll books/precinct lists from the EPB, the EPB must provide for the printing of a paper poll book AND a copy of the list of registered voters within the precinct. <p>Demonstration Comments: EPB system keeps the data during operation on the hard disk of the Poll Pad. Data redundancy at a polling place can be maintained by having multiple Poll Pads in a polling place, and having the check in data synchronized between them and also using the iSync drives. Reports can be configured, exported, and saved to preserve data at any point in time.</p> <p>The EPB must prevent multiple “check-ins” by the same voter.</p> <p>Demonstration Comments: The system identifies an attempt to check in an already checked in voter. The Poll Pad displays an indication of the original check in. The system can be configured for the poll worker to take additional actions like cancelling the check in, reprinting the voter slip, etc. In an environment where there are multiple Poll Pads connected, data syncing between the devices must be functioning to ensure multiple “check ins” are prevented on different devices.</p>	
<p>A legible digitized signature for each registered elector. (25 Pa.C.S. § 1402(b)(2)).</p> <p>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.</p>	Yes
<p>Street address of each registered elector. (25 Pa.C.S. § 1402(b)(2)).</p>	Yes
<p>Political party designation of each registered elector. (25 Pa.C.S. § 1402(b)(2)).</p>	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
<p>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)).</p> <p>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.</p> <p>Demonstration comments: The application has a “Poll Worker Initial” box that captures the initials of the poll worker performing the check in.</p>	Yes
Indication of whether the elector needs assistance to vote and, if so, the nature of the disability. (25 Pa.C.S. § 1402(b)(2)).	Yes
The date of birth of the registrant. (4 Pa. Code § 183.11(b)(4)).	Yes
The SURE registration number of the registrant. (4 Pa. Code § 183.11(b)(5)).	Yes
The following elector’s affirmation must appear above the signature area: “I hereby certify that I am qualified to vote in this election.” (25 P.S. § 3043).	Yes

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

Attachment B - EPB Functionalities

Specific “check in”/voter handling Scenarios demonstrated

- a) Provisional Ballot: The process for issue of a provisional ballot was demonstrated.
- 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 was demonstrated 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 was demonstrated.
- d) Reissue Ballot: The process of re-issue of a ballot for a spoiled ballot was demonstrated.
- 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 was demonstrated.
- f) Redirecting a voter to the correct polling place: The system capabilities for redirecting a voter to the correct polling place were discussed.
- g) Search/Lookup voter Capabilities of the EPB: The EPB system voter lookup capabilities and usability were demonstrated.
- h) Identifying a Duplicate check-in: It was demonstrated that the system prevented the same voter from checking in multiple times.

Usability/User Interface Discussion

The following capabilities/functions of the EPB system was demonstrated.

- a) Set up and Procedures for setting up the Field System/Poll Pad
- b) Poll worker ability to access the system and login
- c) Screen navigation capabilities
- d) Languages Supported by the system

- e) System power up and shutdown procedures
- f) System help availability

Security and Chain of Custody

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

Attachment C - Commonwealth 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:

The Poll Pad is equipped with Apple iOS encryption and is combined with the Amazon Web Services (AWS) Gov Cloud hosting system. It was represented that, iOS also achieves a reduced-attack surface by limiting listening ports and removing unnecessary network utilities such as telnet, shells, or a web server. Knowink uses tools such as Amazon Web Services (AWS) Web Application Firewall (WAF) configured with security rules to mitigate common OWASP vulnerabilities as well as AWS Guard Duty which analyzes log files to alert system administrators of any suspicious activity. The Poll Pads run in kiosk mode where only the required software is installed and available for use. Knowink also represented that all systems are monitored using AWS Cloudwatch and AWS Guard Duty for any suspicious behavior. The engineering team is available to respond to any threats that may occur.

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

Submission Summary:

The submitted software architecture document suggests that the Poll Pad and ePulse systems maintain multiple levels of security to ensure confidentiality and integrity of all devices, communications, data, and systems. Poll Pads use iOS and ePulse is cloud-hosted. The ePulse system uses many defenses to keep the system both secure and available during peak periods, like an election. Traffic is encrypted and the database resources are isolated from the public Internet. Traffic is distributed using application load balancer to maintain high availability and scalability of internal resources. Application servers are hosted on different availability zones. ePulse follows best practices for access control and provides detailed audit trails of transactions.

- C) ITP-SEC019 and ITP -SEC016 – Establishes policies and procedures to protect commonwealth electronic data.

Submission Summary:

Knowink represented that they have an appointed contact for security coordination who adheres to the company's Information Security Policy for handling security-related duties. All data on the Poll Pad is encrypted in transit and at rest. All files are uploaded to the secure storage solution provided by AWS. Knowink noted the process they undertake to ensure that data is accessed only by authorized users. It was also represented that the Poll Pad can be physically secured to avoid compromise of data once they are prepared for elections.

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

Submission Summary:

Knowink represented that all data is encrypted at rest using FIPS 140-2 level encryption.

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

Submission Summary:

Knowink supplied their incident management policy which suggests defined processes exist for responding to security incidents. Knowink also represented that it performs periodic security reviews as part of its certification procedures with all states. The entire system is reviewed for security at multiple points during the year.

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

Submission Summary:

Knowink provided the company Information Security Policy which governs the use of sensitive data. It was represented that they have not had a breach and have never had a client that suffered a data breach for implementing the EPB solution.

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

Submission Summary:

The Poll Pad device and peripheral components including printers, ID scanning trays, stylus, charging cables and stand are locked in the weatherproof/shockproof cases

provided as part of the solution. Authentication requirements will prevent access to the Poll Pad and ePulse application. External hardware connection capability is limited to the Apple-approved, proprietary Knowink iSync drive and printers. Poll Pads contain a “decommission” feature which allows all election data to be wiped from the device. Knowink would recommend jurisdictions use the same level of protection for all voting equipment such as voting machines as the electronic poll books.

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

Submission Summary:

Knowink representation suggests that the poll book system involves encryptions and secure transmission protocols. All data in transit is encrypted to standards as mentioned below

Data Transfer	Encryption Method
Data Transferred from ePulse to PollPad	All data is encrypted with AES 256 encryption using TLS 1.2 connection
Data Transferred from Pollpad to Pollpad	Data is encrypted with AES 256 level encryption. See “Peer to Peer Security” document for more information
Data Transferred from Poll Pad via WiFi	Data is encrypted using WPA2 protection
Data Transferred via iSync	All data placed on iSync devices is encrypted with AES 256 level encryption. See Peer to Peer security document for more information

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

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

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

Refer to Item C above.

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

Refer to Item D above.

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

Refer Item H above

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

Not applicable.

The information security policy suggests that Knowink enforces secure coding guidelines. The system had undergone code review and security testing as part of approval for California State certification testing.

- J) 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 field system can be configured to require username/passwords from one or multiple poll workers to access. The management system requires credentials from election authorities and supports Multi Factor Authentication. All users are added to ePulse by the administrator user(s). New users will receive an email prompting them to create a password for their account. User logins are stored in ePulse and all activities are monitored and logged. ePulse user access levels may also be customized and restricted to certain modules and functions.

Attachment D - Poll Pad Components

(The below screenshot from the Poll Pad Guide submitted as part of the application for approval)

Pollpad 3.1

Attachment D.pdf



PollPad 3.1
components.pdf

meet the

POLL PAD[®]



1 Power Button

2 Home Button

3 Poll Pad & Plastic Shell

4 Stand Arm

5 Poll Pad Base

6 Camera

7 ID Tray



- 1 Green Case
- 2 iPad
- 3 Poll Pad Base
(stand arm located under base)
- 4 Lightning to USB Cable & USB Power Adapter
- 5 (2) Stylus
- 6 ID Tray
- 7 Printer & Cords
- 8 Screen Cloth