Electronic Poll Book System

Vendor Assessment Report

Tenex Software Solutions, Inc.

40 North Pearl Street, Suite 5

Albany, NY 12207-2729

June 4, 2019

Version History

06.04.19 – Original Version

Table of Contents

1. Introduction

New York State has authorized early voting and, to support this initiative, electronic poll book systems (EPBS) may be used by county board of elections (CBOE).

The New York State Board of Elections (NYSBOE) was tasked with developing and promulgating minimum functional and security standards for any electronic device, and any network or system to which the electronic device is connected, that is used to store or otherwise access a computer-generated registration list (Electronic Poll Book System - EPBS). NYSBOE is also to promulgate a list of systems that are approved for use. No local board of elections shall be permitted to use such a system unless NYSBOE has previously approved it for use and has certified that the network to which any components are connected is compliant with the minimum-security standards.

To accomplish this, NYSBOE developed an evaluation process designed to validate via vendor attestations, provided artifacts and demonstrations that mandatory functional, non-functional, security, and networking requirements were understood and able to be met by each EPBS submitted for review. Requirements were evaluated against each vendor configuration for determination if the requirement has been implemented and observed via demonstration or explained and attested to by the vendor. Each requirement based on this approach was then marked successfully (Pass) or unsuccessfully (Fail).

Each system was also reviewed to determine its ability to fulfill the requirements under Section 8-508 of NYS Election Law providing for the production of a Challenge Report. This functionality was considered optional and only systems claiming to support this functionality were reviewed for compliance against the specific requirements developed by NYSBOE for this purpose.

NYSBOE also partnered with the NYS Division of Homeland Security and Emergency Services (DHSES) and the NYS Technology Enterprise Corporation (NYSTEC) for performing vulnerability scans of all applicable system components for any potential vulnerabilities and to confirm that no unnecessary ports or services were exposed beyond those required for the operation of the system. In addition, DHSES scanned all submitted systems to determine if information was being properly protected through encryption. NYSTEC was also engaged to review a subset of technical documentation submitted by each vendor and to provide assurance that documentation requirements were addressed. In addition, they reviewed NYSBOE's evaluation of functional and security requirements to provide assurance that all processes were followed consistently for each system reviewed.

A submitted configuration will be considered for approval if the EPBS successfully passes the above evaluation process, has a documented non-impact issue that has no negative effect on system usage or implements an approved compensating control(s).

Further details on the results of the observations and demonstrations conducted by NYSBOE and its partners are contained in the information below.

2. System Overview

The Tenex Software Solutions, Inc. Precinct Central solution was submitted for State Board approval. The Precinct Central solution is comprised of three modules: Precinct Central Touchpad, Precinct Central Console, and Precinct Central Data Studio.

Central Touchpad is the application that runs on the iPad hardware platform which is used by poll workers for checking in voters at poll sites. Network devices then allow for a secure connection between these devices and the Precinct Central Console backend application. Precinct Central Console is a real-time monitoring and election configuration platform that allows elections staff to monitor devices, users, communications, and performance metrics. The Precinct Central Console is also the election office portal for all pre-election setup activity and post- election data reconciliation, auditing, and export. The Precinct Central Data Studio facilitates the communication of information between all Touchpads deployed in the election.

3. Documentation/Artifact Compliance

To ensure compliance with a number of designated functional and security requirements, vendors were required to provide documentation or narratives, along with any relevant artifacts, which provided evidence of such compliance. Examples of artifacts included, but were not limited to, screenshots, logs, sample reports, etc. Some requirements mandated that a vendor describe their system's ability, or inability, to support certain functionality without necessarily requiring the functionality itself be present.

All initial written responses were reviewed to determine if the submissions, along with any artifacts provided, demonstrated clear evidence of requirement compliance. If the vendor's system did not provide for the functionality mentioned in a specific requirement, then the vendor provided a description explaining as much. If a compensating control or additional information was needed for a system to successfully meet a given requirement, such information was provided by the vendor

for review by NYSBOE. The findings presented below are separated into the application packet categories of Functional Requirements, Security Requirements and Challenge Report.

3.1 Written Responses/Artifacts to Identified Requirements

3.1.1 Functional Requirements

Nineteen (19) functional requirements required a written response and/or artifact submission. After examination and review of the totality of documentation provided by the vendor as part of this process, it was determined that all designated mandatory functional requirements had been satisfactorily met or attested to.

3.1.2 Security Requirements

Fifty-five (55) security requirements required a written response and/or artifact submission. After examination and review of the totality of documentation provided by the vendor as part of this process, it was determined that all designated mandatory security requirements had been satisfactorily met or attested to.

3.1.3 Challenge Report (Optional)

One challenge report requirement required a written response and/or artifact submission. After examination and review of the totality of documentation provided by the vendor as part of this process, it was determined that the designated challenge report requirement had been met or attested to.

3.2 Technical Data Package

Each vendor was required to provide a Technical Data Package (TDP) for their system. This documentation defines the required design configuration, technical information and any procedures required to ensure adequacy of system performance.

Technical Data Package contents were required to include the following:

- System configuration overview
- System hardware specifications
- System test and verification specifications
- User/system operations procedures
- Personnel deployment and training requirements
- Quality assurance program
- System functionality description

- Software design and specifications
- System security specifications
- System maintenance procedures
- Configuration management plan
- System change notes

NYSTEC performed an examination and review of the totality of materials provided by the vendor and reported their findings to NYSBOE. It was then determined by NYSBOE that the submitted documentation demonstrated compliance with this requirement.

4. Vendor Demonstrations and Observations

An on-site demonstration conducted by Tenex Software Solutions, Inc. of the mandatory functionality for each requirement was conducted on May 28, 2019. During this demonstration, the system was observed to determine if each requirement had been met. The findings presented below are separated into the application packet categories of Functional Requirements, Security Requirements and Challenge Report.

4.1 Functional Requirements

Fifty-three (53) functional requirements required a vendor demonstration. After review of this system during the demonstration provided by the vendor as part of this process, it was determined that **all but one** designated mandatory functionality requirements had been satisfactorily demonstrated. Requirement F-17 requires that, in accordance with Section 11-206(4) of NYS Election Law, an EPBS have the ability to display the names of special federal voters separate and apart from other voters contained in the list. As the configuration submitted by Tenex Software Solutions, Inc. does not currently support this function, an acceptable compensating control for this requirement would be that, at each election at which the ballots of special federal voters are delivered to the inspectors of election in each election district, the CBOE must prepare and distribute a separate paper list of special federal voters.

4.2 Security Requirements

Thirty-four (34) security requirements required a vendor demonstration and/or support and stated compliance via submission of a TDP and/or supporting documentation. After review of this system during the demonstration provided by the vendor as part of this process, it was determined that all designated mandatory security requirements had been satisfactorily demonstrated or compliance was stated via attestation and through provided documentation.

4.3 Challenge Report (Optional)

Seven (7) challenge report requirements required a vendor demonstration (if the vendor's submission include this functionality). After review of this system during the demonstration provided by the vendor as part of this process, it was determined that the designated challenge report requirements had **not** been satisfactorily demonstrated.

5. Vulnerability Scanning

NYSBOE partnered with the NYS Division of Homeland Security and Emergency Services (DHSES) and NYSTEC to perform vulnerability scanning as part of the evaluation of each EPBS submitted.

5.1 NYS Division of Homeland Security and Emergency Services Testing

DHSES was responsible for performing the following objectives of the vulnerability scanning and traffic inspection:

- Perform non-authenticated vulnerability scanning all EPBS hardware devices provided; and
- Validate data confidentiality is maintained during both external data transmissions to a vendor cloud service, and data transmissions between two EPBS devices connected to the same local network.

As a result of their testing, DHSES found that no critical, high, medium, or low vulnerabilities were identified on any of the three iPad ePollbooks scanned. DHSES did identify a single port that was open and accessible. The vendor was asked to explain if there was a business function requiring this port to be left open or if it could be closed. The vendor explained that the open port is used for emergency data recovery, is locked down by their mobile device management platform and is the standard configuration for iPads. In addition, validation of peer-to-peer transmission confidentiality could not be performed by DHSES during their testing. However, the vendor was able to provide a satisfactory demonstration of the encrypted peer-to-peer communication of their system during their in-person demonstration. Also observed during testing was that the mobile hotspot provided by the vendor was configured to broadcast the default service set identity (SSID) and allowed usage of default administrative credentials. The vendor explained that their system is intended to be used with whatever connectivity is provided by each county but produced documentation on how to properly harden such devices to comply with our requirements. In addition, users had access to the iPad Settings application with privileges to make modifications to the device configuration. The vendor explained this was necessary to allow for general troubleshooting functions. They also explain that all critical applications are locked, there is only

one application (Precinct Central Touchpad) loaded on the device, there is no browser installed on the device and their Meraki Mobile Device Management platform provides additional monitoring and control.

5.2 NYSTEC Vulnerability Scanning

NYSTEC researched each solution and, working with the team doing the security testing of the EPBS, ascertained how the devices themselves and the administration/management interface to the systems were architected. Also in scope, was identifying the URLS and IP addresses to which they connected. From this, test plans were created to use three (3) separate security tools to scan those online endpoints.

The tools used to perform the scanning were:

- AppScan

- Nessus

- WebInspect

For this testing the scans were all unauthenticated and from the internet. The goal of the scanning was to identify ports and services, that may be open and represent potential points of attack, beyond those ports and services which are open, available and necessary to support the following:

- Communication from pollbooks to server(s)

- Communication from system administrators to administrate and manage the system, data and individual pollbooks.

The scan types completed by NYSTEC were basic network and web application scans (AppScan and Nessus) and OWASP Top 10 (for WebInspect) with defaults enabled. The systems scanned were as configured by the vendors. Manual application testing, penetration testing and other security testing were not in scope.

There was nothing found in any of the scans that raise concerns or disqualify any of these systems.

6. Conclusion

After completing its evaluation of the system configurations submitted by Tenex Software Solutions, Inc., as described in this document, the Election Operations Unit has determined that this system has shown compliance with all mandatory functional and security requirements through

submitted documentation, in-person demonstration and compensating controls as described above. Vulnerability scanning performed did not identify any issues that would raise security concerns for its use. Therefore, we are recommending the electronic poll book system submitted by Tenex Software Solutions, Inc. for approval.

Such approval is based on the Electronic Poll Book System's hardware and software submitted by the vendor and reviewed by the State Board of Elections. Should the vendor make, or plan to make, any modifications or alterations to the Electronic Poll Book System's hardware and/or software, such modifications or alterations shall be reviewed by the State Board of Elections for approval, consistent with its "Electronic Poll Book System Change Management Procedure".

7. Appendix

7.1 Completed and Signed Application

7.2 Functional Requirements

7.3 Security Requirements

7.4 Challenge Report Requirements

7.5 Technical Data Package Review

7.1 Completed and Signed Application

NEW YORK STATE | Board of Elections

NEW YORK STATE BOARD OF ELECTIONS
ELECTION OPERATIONS UNIT
40 North Pearl Street Ste 5
ALBANY, NEW YORK 12207

Application for Approval of Electronic Poll Book System (EPBS)

NAME OF VENDOR: Tenex Software Solutions, Inc.

CONTACT PERSON: Ravi Kallem, President

ADDRESS OF COMPANY: 5402 W Laurel St, Suite 206, Tampa FL 33607

TELEPHONE NUMBER: 813-618-3639   FAX NUMBER: n/a

E-MAIL ADDRESS: ravi.kallem@tenexsolutions.com   CELL PHONE: 813-758-8951

Description of EPBS:

Precinct Central is a modern platform that brings together the latest technologies and best-of-breed functionalities in a cost-effective package. Great care and design work have been completed in selecting and building the system components, including the software, the hardware, and the Tenex original "flip and share" stand. Precinct Central started with a basic concept of an electronic poll book system that replaces the paper check-in process and allows checking in voters in an electronic format. In its current state it has evolved into a complete monitoring platform allowing election officials to track and react to issues in the field before they are magnified into larger problems.

The underlying hardware used for running the e-pollbook system is another very important factor to consider. Tenex has selected a modern tablet-based platform for Precinct Central - the award-winning iPad tablet hardware from Apple. The Apple iPad is one of the most secure tablets available and boasts security features such as encrypted file system, FIPS certification, and no ports for external device interfaces that could introduce malware and unwanted behavior.

The Precinct Central solution is comprised of three modules: Precinct Central Touchpad, Precinct Central Console, and Precinct Central Data Studio.

Precinct Central Touchpad is a highly customizable electronic poll book solution that runs on the award-winning iPad hardware platform. This hardware platform, along with the intuitive software from Tenex, offers familiarity and ease of use for poll workers. There are no additional peripherals required for reading barcodes and gathering voter signatures. Housed in the flip-and-share stand, the platform is lightweight and easy to setup, operate, transport, and store.

EPBS Hardware Information (List all):

Touchpad (EPB)
Flip and Share Stand

Optional items: Epson TM-m30 Printer, 10 ft certified charging cable, transport case for 2 complete units, styli, charging carts, battery back-ups.

EPBS Firmware and Software Release Information (List all):

Precinct Central: Versions 3.2.5.9 – 4.0 (Release as needed and/or every year)

Precinct Central Touchpad: Versions 3.8.5 – 4.1.3 (Release as needed and/or every year)

General information

Do you own all rights to this system?   (Yes)   No
If not, please explain:

Date system and documentation/artifacts will be delivered
to the New York State Board of Elections for examination: May 3rd close of business

Is any part of the system manufactured or assembled by another company?   **Yes**   (No)
If "yes," name & address:

Applicant hereby agrees:

To provide the Electronic Poll Book System (EPBS) and to furnish all documentation/artifacts required by the state board of elections or its designee. Applicant understands that it may be required to place the EPBS in the state board's possession for as long as such system is in use in New York State.

That the submitted EPBS complies with all applicable requirements and standards adopted by the state board and is suitable for use by County Board of Elections.

That the submitted EPBS software does not contain any code, procedures or other material (including but not limited to 'viruses', 'worms', 'time bombs', and 'drop-dead' devices that may cause the EPBS to cease functioning at a future time), which may disable, damage, disarm or otherwise affect the proper operation of the EPBS, any hardware, or any system or other property of state board or county board.

Applicant consents to vulnerability and penetration testing on their electronic poll book system as allowed by Public Law 105-304 - Digital Millennium Copyright Act, §1201(j) Security Testing.

All proposals and submissions are subject to New York's Freedom of Information Law. It is the policy of the New York State Board of Elections, in relation to applications for approval of EPBS, that the State Board shall make available to the public all non-proprietary documentation submitted by the Vendor. The Vendor may designate those portions of the proposal that contain trade secrets or other proprietary data that must remain confidential. Blanket statements that either attempt to cover all information in a document, or which allows for a reactive assertion of exemption by the Vendor upon a future request for disclosure, will not be accepted.

[signature]   **Date: 4/30/20129**

Ravi Kallem, President

7.2 Functional Requirements

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-1	The parts of the electronic poll book system to be used at the poll site (EPBS-PS) shall have the capability to be labelled, locked and sealed in carrying cases with tamper-evident security seals when transported to and from the county board of elections.	Mandatory	Security	X		Pass
F-2	The EPBS-PS shall have the capability to be labelled, locked and sealed in carrying cases with tamper-evident security seals when not in use at the poll site.	Mandatory	Security	X		Pass
F-3	The EPBS-PS shall support a dual authentication feature where the coordinated action of (2) election inspectors who are not members of the same political party is required to enable use of the electronic poll books when poll sites open.	Mandatory	Security	X		Pass
F-4	The EPBS-PS shall display the date of the election being conducted on each screen.	Mandatory	Functional	X		Pass
F-5	The EPBS-PS shall be capable of utilizing an "appropriate marking device" to capture the signature as signed by the registered voter.	Mandatory	Functional	X		Pass
F-6	The EPBS-PS shall conceal the voter's facsimile signature until after the voter has completed signing their signature, at which point both signatures will be displayed for inspector comparison.	Mandatory	Functional	X		Pass
F-7	The EPBS-PS shall have the ability to display an electronic list of voters in alphabetical order for a: - single election district or - poll site.	Mandatory	Functional	X		Pass
F-8	The EPBS electronic list of voters shall be generated from a computer registration file for each election.	Mandatory	Functional	X		Pass
F-9	When used at a primary election, the EPBS-PS shall have the ability to display the names of the voters enrolled in a particular political party.	Mandatory	Functional	X		Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-10	The EPBS shall display, for each voter record, at least the following: - County Voter ID - Name - Street Address - Town, City or Ward - Election District - Assembly District, where appropriate - Date of Birth - Date of Registration (Month/Day/Year) - Party enrollment - Facsimile of the voter's signature or an indication that the voter is unable to sign his/her name - A notation indicating if the voter's identity was not yet verified as required by the federal Help America Vote Act.	Mandatory	Functional	X		Pass
F-11	The EPBS-PS shall include for each voter listed the following: - Place where a voter can sign his/her name or where it can be indicated by the inspectors that a voter is unable to sign his/her name - For voters requiring assistance, a place to enter the name of each officer or person rendering such assistance - Place for inspectors to record the number appearing on the stub of any election day paper ballot given to the voter, or other information to allow for ballot reconciliation - Place for inspectors to sign their names or initials after satisfaction of signature comparison and by comparison of his/her appearance with the descriptive material in the poll record - Place for inspectors to indicate that a voter has produced one of the required types of identification if ID has not been verified.	Mandatory	Functional	X		Pass
F-12	For voters requiring assistance, the EPBS-PS should display the assistance oath.	Optional	Functional	X		Pass
F-13	For the canvass of absentee, military or special ballots, or ballots cast by voters with registration poll records missing, or for voters that have not had their identity previously verified or who have moved after registering, the EPBS shall provide an ability for the inspectors to place their initials in a space provided if the person is found to be registered and signatures are found to correspond.	Optional	Functional	X		Fail

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-14	For voters described in F-13, the EPBS shall provide an ability for the inspectors to record information including but not limited to the following items: - absentee vote, - military vote, - year of election, - month of election	Optional	Functional	X		Fail
F-15	The EPBS-PS shall enable a poll worker to search for a voter's record. Search criteria must include either a complete or partial match to one or more of the following: - Last Name - First Name - Date of Birth - Address	Mandatory	Functional	X		Pass
F-16	For primary elections, the search criteria should include all items from F-15, as well as Party Enrollment.	Optional	Functional	X		Fail
F-17	The EPBS-PS shall have the ability to display the names of special federal voters separate and apart from other voters contained in the list.	Mandatory	Functional	X		Pass
F-18	The EPBS-PS may provide a street finder or other tool that would enable election inspectors and/or poll site coordinators to determine the correct election district and polling place for a voter who is in an incorrect poll site	Optional	Functional	X		Pass
F-19	The EPBS shall indicate whether a voter has already cast a ballot.	Mandatory	Functional	X		Pass
F-20	In addition to alphabetical order, the EPBS-PS should be configurable to provide a list of voters in some other order defined by an administrative user.	Optional	Functional	X		Fail
F-21	The vendor shall describe how their EPBS shall be configurable to allow for the importing of voter registration data from voter registration systems in use by a County Board of Elections in New York State.	Mandatory	Functional	X	X	Pass
F-22	The EPBS shall provide the ability for county board of elections staff to verify the import of any and all data previously exported from the county board's voter registration system (voter records, poll site files, etc.).	Mandatory	Functional	X		Pass
F-23	The EPBS shall be configurable to allow for the exporting of election data (both early and election day) in a format that can be imported into any voter registration system in use by a County Board of Elections in New York State.	Mandatory	Functional	X		Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-24	The EPBS shall be capable of exporting voter history in a format that can be used to transfer such information into any voter registration system in use by a County Board of Elections in New York State.	Mandatory	Functional	X		Pass
F-25	The vendor shall describe the process by which maintenance and diagnostic activities of EPBSs, when performed by an entity other than a CBOE, is coordinated with a CBOE, and what allowances the CBOE has to monitor and control these activities.	Mandatory	Functional		X	Pass
F-26	The EPBS shall have the ability to export any voter signature captured by a EPBS-PS in a well established, non-proprietary format.	Mandatory	Functional	X		Pass
F-27	The EPBS must guarantee that a voter can be checked in at most once during normal connectivity.	Mandatory	Functional	X		Pass
F-28	The EPBS shall identify voters that have been checked in at two or more different electronic poll books.	Mandatory	Functional	X		Pass
F-29	In the event of a temporary interruption of connectivity within an EPBS, the EPBS-PS must permit the continuation of the voter check-in process.	Mandatory	Functional	X		Pass
F-30	In the event of a temporary interruption of connectivity within an EPBS, the EPBS must automatically restore voter list consistency across the EPBS-PS after connectivity is restored.	Mandatory	Functional	X		Pass
F-31	In the event of a temporary interruption of connectivity within an EPBS, the EPBS must indicate that there has been an interruption of connectivity by entering relevant event information into the audit log.	Mandatory	Functional	X		Pass
F-32	The vendor shall describe the process by which they will develop and provide training options and materials to each County Board of Elections under contract which will allow CBOE staff and polling inspectors to be trained in the use of the EPBS/EPBS-PS, where appropriate.	Mandatory	Training		X	Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-33	The vendor shall provide help-desk support to each County Board of Elections under contract and describe the following: - Help-desk ticket submission process - Help-desk ticket response time standards (follow-up and resolution). - Help-desk ticket escalation and resolution model - Help-desk ticket status reporting - Schedule of Help-desk hours of operation and availability (at minimum help-desk support must be provided from 9:00 a.m. to 5:00 p.m. – Eastern Time – Monday to Friday.	Mandatory	Technical Support		X	Pass
F-34	The vendor shall provide enhanced help desk services to support CBOE during the following peak timeframes: - For the period of Early Voting Day 1 to Early Voting Day 9, telephone support shall be provided between the hours of 5:00 am and 10:00 pm Eastern Time. - For the period including Election Day minus 1, Election Day and Election Day plus 1, telephone support must be available during this entire 72-hour period. - For the post election period, which is defined as Election Day plus 1 through Election Day plus 15, phone support shall be provided by the vendor, on each of said days, between the hours of 7:00 am until 7:00 pm, EST.	Mandatory	Technical Support		X	Pass
F-35	The EPBS shall have the ability to generate reports based on any defined data fields.	Mandatory	Reporting	X		Pass
F-36	Vendor shall provide a list of data fields which the EPBS is capable of generating a bar code for in a report.	Mandatory	Reporting		X	Pass
F-37	The EPBS should allow authorized users the capability to create, modify and save custom reports and queries.	Optional	Reporting	X		Pass
F-38	The EPBS shall generate reports in a well established, non-proprietary format including, but not limited to, one of the following: - Hypertext Markup Language (.html) - Microsoft Excel (.xlsx) - Microsoft Excel (.csv) - Adobe Acrobat Portable Document Format (.pdf) - Microsoft Word (.docx)	Mandatory	Reporting	X		Pass
F-39	The EPBS should allow authorized users to select from a list of available report templates and enter report criteria prior to generating the report.	Optional	Reporting	X		Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-40	The EPBS shall allow authorized users to view reports before saving or printing them.	Mandatory	Reporting	X		Pass
F-41	The EPBS should allow including the name of the report, the date generated, and the page number on each page of a report.	Optional	Reporting	X		Pass
F-42	The vendor shall describe the required electrical supply specifications for the EPBS-PS in polling places.	Mandatory	Power/Battery		X	Pass
F-43	The vendor shall describe the EPBS-PS battery specification including but not limited to: - Hours of continual use by inspectors - Hours of stand-by (when not being used to check in a voter)	Mandatory	Power/Battery		X	Pass
F-44	The vendor shall describe how to: - Charge the EPBS-PS battery before deployment to a poll site - Charge the EPBS-PS battery at the poll site both during voting hours and when the polls are closed (include specification on power plug length)	Mandatory	Power/Battery		X	Pass
F-45	The vendor shall describe how the EPBS-PS retains its data when power to the device is exhausted.	Mandatory	Power/Battery		X	Pass
F-46	In the event of a temporary loss of power, the EPBS-PS must permit a voter to check-in. The electronic poll book system's battery supply must allow for at least two (2) hours of operation without external power supply.	Mandatory	Power/Battery	X		Pass
F-47	The EPBS-PS shall be configured in such a way that the operator is provided with a continuous visual indication of whether the device is operating on battery or AC power and, if the former, a visual indication of how much battery power remains.	Mandatory	Power/Battery	X		Pass
F-48	The EPBS-PS shall be capable of automatically switching to a backup power source (e.g. battery) and not interrupt the operation or integrity of the data.	Mandatory	Power/Battery	X		Pass
F-49	The EPBS shall concurrently support all connected devices from all poll site locations within the county.	Mandatory	Non-Functional	X		Pass
F-50	The vendor shall attest that they will have the ability to deliver the contracted number of EPBS-PS. If the vendor contracts with all CBOE, the estimated number is between 18,000 and 20,000 EPBS-PS.	Mandatory	Non-Functional		X	Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-51	As of the date of the vendor's application for approval of the EPBS by the NYSBOE, the vendor must provide a complete and working iteration of their EPBS to NYSBOE including, but not limited to: - At least three (3) EPBS-PS devices - Any equipment, as defined in the configuration submitted, necessary to network the devices either together or to a backend software system - URL and credentials to access any hosted or cloud-based backend software system configured to work with any hardware components submitted	Mandatory	Non-Functional		X	Pass
F-52	The vendor must provide a list of customers who are using, or have previously used, the vendor's EPBS. This list must be current as of the date of the vendor's application for approval of the EPBS by NYSBOE.	Mandatory	Non-Functional		X	Pass
F-53	The vendor must provide a description of any known anomalies in the function of the EPBS as well as a description of the method for resolving those anomalies. This list must be current as of the date of the vendor's application for approval of the EPBS by NYSBOE.	Mandatory	Non-Functional		X	Pass
F-54	The vendor shall provide instructions and materials sufficient for the CBOE to carry out a pre-election test of the EPBS (including EPBS-PS) to verify the integrity of the system components before their use in an election.	Mandatory	Non-Functional	X	X	Pass
F-55	The EPBS shall provide means for the integration of an additional EPBS-PS into its configuration at any point throughout the election without requiring a shutdown or a restart of the EPBS. This system event must be documented in the audit log.	Mandatory	Technical	X		Pass
F-56	The EPBS shall provide means for the exclusion of an existing EPBS-PS from its configuration at any point throughout the election without requiring a shutdown, or restart of the EPBS. This action does not require physical access to the EPBS-PS that is to be excluded. This system event must be documented in the audit log.	Mandatory	Technical	X		Pass
F-57	Each EPBS-PS within an EPBS configuration must have a unique identifier. Any component within an EPBS configuration must be able to uniquely identify said EPBS-PS by its identifier.	Mandatory	Technical	X		Pass
F-58	The EPBS must be designed to tolerate any single point of failure scenarios.	Mandatory	Technical	X	X	Pass

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
F-59	The EPBS-PS shall have the capability to display a prompt or warning if an individual cannot be found in the list of voters during the check in process.	Mandatory	Functional	X		Pass
F-60	An EPBS-PS must provide a user interface through which authorized users can verify an individual's voting eligibility and document the voter's election related activity.	Mandatory	User Interface	X		Pass
F-61	The EPBS-PS should provide election inspectors with access to on-screen support, configurable by administrative users and relevant to the action being executed at a given time.	Optional	User Interface	X		Pass
F-62	The EPBS must provide a user interface through which authorized users can configure the system. This includes the initial setup of the system, reconfiguration, viewing the current configuration, as well as adding or removing an EPBS-PS device.	Mandatory	User Interface	X		Pass
F-63	The EPBS must provide a user interface through which authorized users can manage user accounts. This includes adding and disabling and managing their access privileges.	Mandatory	User Interface	X		Pass
F-64	The EPBS-PS may include a bar code reader.	Optional	Barcode	X		Pass
F-65	The EPBS-PS should display a voter's record based on the processing of information contained within a bar code when scanned by a bar code reader.	Optional	Barcode	X		Pass
F-66	The vendor shall describe how their EPBS supports existing Section 203 Language Provisions of the Voting Rights Act and the ability to add languages if designated by the Director of Census.	Mandatory	Functional		X	Pass
F-67	The vendor shall describe how their EPBS provides accessibility functionality for voters with disabilities (e.g. high contrast, large font or audio).	Mandatory	Functional		X	Pass
F-68	The EPBS should be capable of importing ballot schema that will enable the printing of a receipt with the voter's ballot style or be used in conjunction with a ballot on demand printer solution.	Optional	Functional	X		Pass
F-69	Vendor shall provide the results and supporting documentation related to any 3rd party or internal usability testing performed on the EPBS. Supporting documentation shall include, but not be limited to, test plans, test cases and results from all usability testing that was conducted.	Mandatory	Functional		X	Pass

7.3 Security Requirements

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration / Artifact	Response	Pass/Fail
S-1	Vendor shall provide a system overview and functional diagram of the entire EPBS and how each component integrates into it. The description shall include how the entire system is administered, configured and managed.	Mandatory	Documentation	Entire ePoll Book System		X	Pass
S-2	Vendor shall provide a system architecture diagram for their proposed solution that includes a description of how the solution is architected addressing on-prem and cloud or hosted or any hybrid combination thereof. If customer systems are needed to host software, information on how those systems must be configured and hardened shall be provided.	Mandatory	Documentation	Vendor		X	Pass
S-3	Vendor shall provide software system design documentation describing the logical design of the software. This documentation shall clearly indicate the various modules of the software, their functions, and their interrelationships with each other. This shall include the data format(s) the system is capable of importing and exporting.	Mandatory	Documentation	Vendor		X	Pass
S-4	Vendor should provide, for any cloud hosted components, proof that those components have achieved a FedRAMP compliance and are hosted by a FedRAMP authorized cloud service provider. Vendor should provide proof of FedRAMP compliance as well as documentation of who is responsible for each required security control.	Optional	Documentation	Vendor		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-5	All EPBS data shall remain in the Continental United States (CONUS). Any EPBS data stored, or acted upon, must be located solely in data centers in CONUS. Services which directly or indirectly access EPBS data shall only be performed from locations within CONUS. Vendor shall provide proof of compliance.	Mandatory	Access Control	Entire ePoll Book System	X	X	Pass
S-6	All EPBS data in transit shall remain in CONUS and be encrypted in accordance with requirement #S-55 below. Vendor shall provide proof of compliance.	Mandatory	Encryption	Entire ePoll Book System	X	X	Pass
S-7	Vendor shall provide, for any non-cloud hosted components, evidence of any third party validation of security controls or assessments that have been completed.	Mandatory	Documentation	Vendor		X	Pass
S-8	Vendor shall develop, document and maintain the baseline configuration of the EPBS hardware and software components. The vendor documentation shall describe all maintenance activities that are necessary to ensure the EPBS remains in the desired configuration and functioning in a secure manner. This baseline configuration and maintenance procedures document shall be provided and shall clearly identify the software versions that must be in	Mandatory	Documentation	Entire ePoll Book System		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-9	Vendor shall provide documentation on how the poll book solution and its related components have been hardened to any applicable Center for Internet Security (CIS) benchmarks, or to other standards (e.g., DoD DISA STIGs). Name all standards used and to which component they apply to (e.g., servers, mobile devices, wireless).	Mandatory	Documentation	Entire ePoll Book System		X	Pass
S-10	The EPBS shall support the use of multi-factor authentication for all privileged and administrator access other than at the poll site.	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-11	The EPBS shall incorporate protections to prevent fraudulent manipulation of the voter check-in process. Vendor shall describe both the preventative and detective controls within the system.	Mandatory	Access Control	Entire ePoll Book System	X	X	Pass
S-12	The EPBS shall employ the principle of least privilege for each permitted role within the system, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks such as poll worker and voter roles as well as administrators. Vendor shall document how incorporated role based access controls accomplish this.	Mandatory	Access Control	Entire ePoll Book System	X	X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demons tration	Response / Artifact	Pass/Fail
S-13	The EPBS shall require the coordinated action of (2) election inspectors who are not members of the same political party to enable use of the electronic poll books for poll site operation.	Mandatory	Access Control	ePoll Book/Poll Site	X		Pass
S-14	Vendor shall describe what configuration item changes can be made by authorized individuals through system defined Administration role(s).	Mandatory	Access Control	Entire ePoll Book System		X	Pass
S-15	Vendor shall describe the capabilities of the EPBS related to automated timeout of inactive sessions (e.g. poll devices, remote admin connections, account login sessions, etc.).	Mandatory	Access Control	Entire ePoll Book System		X	Pass
S-16	The EPBS shall prevent unauthorized or unrecognized electronic poll book device communication with known and trusted components, including poll book backend servers, peer poll book devices and/or wireless access points.	Mandatory	Access Control	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-17	The EPBS shall not require a direct connection to any other election system or election system component (i.e. voter registration system, voting machines, etc.).	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-18	The EPBS shall support: a. The ability to define groups and role-based access b. The ability to create, enable, modify, disable, and archive EPBS accounts c. The ability to monitor the use of EPBS accounts	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-19	The EPBS shall: a. Enforce a configurable limit of consecutive invalid login attempts by a user b. Automatically disable or lock an account until released by an administrator or after a configurable time period when the maximum number of unsuccessful attempts is exceeded	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-20	The EPBS shall: a. Prevent access to the system by initiating a session lock after a configurable number of minutes of inactivity **or** upon receiving a request from a user b. Retains the session lock until the user reestablishes access using established identification and authentication procedures c. Conceals via the session lock, information previously	Mandatory	Access Control	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demons tration	Response / Artifact	Pass/Fail
S-21	The EPBS shall: a. Monitor for and prevent all unauthorized remote access, including wireless where relevant, to the EPBS b. Allow and monitor all authorized connection(s) for all privileged and non-privileged accounts, including usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-22	The EPBS shall support the use of unique user IDs.	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-23	The EPBS shall support industry best practices regarding passwords (e.g. password length, password aging, password complexity, etc.).	Mandatory	Access Control	Entire ePoll Book System	X		Pass
S-24	The EPBS shall support mutual device authentication.	Mandatory	Access Control	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-25	Vendor shall describe how the EPBS components can be tracked, recovered, or disabled if stolen or removed from the polling location. Vendor shall describe any preventative, corrective or detective controls that are present in the system to handle such a scenario.	Mandatory	Access Control	Entire ePoll Book System		X	Pass
S-26	The EPBS shall be capable of providing comprehensive audit logs that can be exported in non-proprietary, human readable format.	Mandatory	Audit	Entire ePoll Book System	X	X	Pass
S-27	Vendor shall provide a listing and description of what messages and events generated by the EPBS (including poll book devices) become part of the audit record.	Mandatory	Audit	Entire ePoll Book System		X	Pass
S-28	The EPBS shall support capturing, at a minimum, date and time-stamped records for the following actions performed by any user on the EPBS, including but not limited to: a. All related operating system events b. All user related events c. All system administration activities d. All network activity	Mandatory	Audit	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-29	The EPBS shall support the generation of alerts to responsible staff (by role) when a log processing error occurs (e.g. lack of space, logging stops unexpectedly, etc.). Vendor shall describe what alerting thresholds are configurable and what alerting methods can be used (page, email, text, phone call, etc.).	Mandatory	Audit	Entire ePoll Book System	X	X	Pass
S-30	The EPBS shall manage and allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.	Mandatory	Audit	Entire ePoll Book System	X		Pass
S-31	The EPBS shall provide the capability to review and analyze EPBS audit records regularly for indications of inappropriate or unusual activity. The EPBS shall not alter the original content or date/time marking of audit records. Vendor shall describe what alerting thresholds are configurable and what alerting methods can be used (page, email, text, phone call, etc.) if any activity described is identified.	Mandatory	Audit	Entire ePoll Book System	X	X	Pass
S-32	The EPBS shall: a. Use internal system clocks to generate time stamps for audit records b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and is accurate to within 30 seconds	Mandatory	Audit	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-33	The EPBS shall protect audit information and audit tools from unauthorized access, modification, and deletion.	Mandatory	Audit	Entire ePoll Book System	X		Pass
S-34	The EPBS shall: a. Support the back up of audit records onto a physically different system or system component other than the system or component being audited b. Export data into a format that can be used to reconstruct the backend database on another server	Mandatory	Backup & Recovery	Backend System	X		Pass
S-35	The EPBS shall support a hot-swappable feature to be configured in such a manner to automatically replicate and securely encrypt a copy of the data at any time to a removable/relocatable memory device or via obtaining configuration data from another electronic poll book device. The saved or imported data will be sufficient to restore another electronic poll book in the event of a malfunction. This functionality shall not require network connection.	Mandatory	Backup & Recovery	Entire ePoll Book System	X		Pass
S-36	The EPBS shall be able to recover from the following events: a non-catastrophic failure of an electronic poll book, a power failure, or from any error or malfunction that is within the poll worker's ability to correct. Recovery from a non-catastrophic failure will mean the restoration of the electronic poll book to the operating condition existing prior to the error or failure, without loss or corruption of data previously stored in the device.	Mandatory	Backup & Recovery	Entire ePoll Book System	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demons tration	Response / Artifact	Pass/Fail
S-37	The EPBS shall: a. Conduct backups of user and system level information contained in the EPBS in a configurable frequency b. Protect the confidentiality, integrity, and availability of backup information	Mandatory	Contingency Planning	Entire ePoll Book System	X		Pass
S-38	Vendor shall provide documentation on how their Software Development Life Cycle (SDLC): a. Aligns with industry standard SDLC practices to incorporate information security control considerations b. Identifies individuals having information system security roles and responsibilities c. Integrates the organizational information security risk ~~management process into system development life cycle~~	Mandatory	Documentation	Vendor		X	Pass
S-39	Vendor shall describe how it employs best practices and methodologies for protecting against supply chain threats to the EPBS and its system components. The vendor shall indicate whether any components of the EPBS have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security ~~strategy.~~	Mandatory	Documentation	Vendor		X	Pass
S-40	Vendor shall describe what capabilities the EPBS has to detect, alert and or prevent any suspicious software behavior in any part of the EPBS.	Mandatory	Documentation	Vendor		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-41	Vendor shall provide documentation and testing results showing that the electronic poll book solution does not exhibit vulnerabilities and weaknesses from sources such as Open Web Application Security Project (OWASP) and the Common Weakness Enumeration (CWE).	Mandatory	Documentation	Vendor		X	Pass
S-42	Vendor shall provide all the documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan for conducting system testing, collectively referred to as the Technical Data Package (TDP).	Mandatory	Documentation	Vendor		X	Pass
S-43	Minimum TDP documentation: system configuration ~~overview, system functionality description, system hardware~~ Vendor shall provide documentation from other election jurisdictions (other states) that have: a. Certified/approved/authorized the proposed EPBS b. Denied certification/approval/authorization of the proposed EPBS c. Withdrawn certification/approval/authorization of the proposed EPBS	Mandatory	Documentation	Vendor		X	Pass
S-44	Vendor documentation shall include recommendations for protecting all electronic poll books from electrical damage related to power surges, brownouts, lightning and other transient current and voltage spikes.	Mandatory	Documentation	Vendor		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-45	Vendor shall provide detailed information concerning all consumables used by the EPBS and the vendor's supply chain for those consumables.	Mandatory	Documentation	Vendor		X	Pass
S-46	Vendor shall describe encryption and other security measures in place to protect data if the proposed system involves Internet or Cloud based transmission of data to and from local electronic poll book components.	Mandatory	Documentation	Vendor		X	Pass
S-47	Vendor shall describe recommended or included, internet intrusion detection / intrusion prevention and control protocols for any part of the system which involves network connections.	Mandatory	Documentation	Network		X	Pass
S-48	Vendor shall provide documentation on a system's non-functional qualities including, but not limited to, Accessibility, Performance, Availability, Reliability, Safety, Security, Usability and Auditability.	Mandatory	Documentation	Entire ePoll Book System		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration / Artifact	Response	Pass/Fail
S-49	Vendor shall describe the security controls used in the development of the system. Such controls include code management to ensure no unauthorized code is entered into the system, coding standards used by developers to give assurance that the code is not subject to known security errors, QA processes during the development cycle and any security testing standards.	Mandatory	Documentation	Vendor		X	Pass
S-50	Vendor shall provide "User Guide" documentation for each user role that specifies how each user can utilize the system in a secure and functional manner.	Mandatory	Documentation	ePoll Book/Poll Site		X	Pass
S-51	Vendor shall describe all recommended controls, processes and procedures, relevant to the EPBS, available to a county BOE to assist them in developing: a. Policy and supporting procedures to facilitate the implementation of the security and privacy awareness training b. Associated security and privacy awareness and training controls.	Optional	Documentation	Vendor		X	Pass
S-52	Vendor shall describe, when cryptography is required and used within the EPBS, the capabilities of the EPBS to establish and manage cryptographic keys including, but not limited to, key generation, distribution, storage, access, and destruction.	Mandatory	Encryption	Entire ePoll Book System		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-53	Vendor shall describe, when cryptographic mechanisms are used, the encryption products used have been validated under the Cryptographic Module Validation Program (see http://csrc.nist.gov/cryptval/) to confirm compliance with FIPS 140-2, in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards. The vendor shall provide the certificate number.	Mandatory	Encryption	Entire ePoll Book System		X	Pass
S-54	The EPBS shall support non-repudiation and protection against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.	Mandatory	Encryption	Vendor	X		Pass
S-55	The EPBS shall encrypt all data at rest and in transit utilizing FIPS 140-2 validated modules compliant encryption. For data in transit, only secure protocols shall be used (e.g., TLS, IPSEC, HTTPS, SFTP).	Mandatory	Encryption	Entire ePoll Book System	X		Pass
S-56	The EPBS shall utilize cryptographic hashing and storage for all system credentials.	Mandatory	Encryption	Vendor	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-57	Vendor shall describe how it protects and controls digital (e.g., CD, DVD, USB drive etc.) and non-digital media (e.g., paper), defined within NIST SP 800-88 (Guidelines for Media Sanitization), containing sensitive information during transport outside of controlled areas (e.g., delivery to SBOE or CBOE) through the use of digital signatures, cryptography (FIPS 140-2 encryption) and/or tamper evident packaging.	Mandatory	Evaluation	Entire ePoll Book System		X	Pass
S-58	Vendor shall provide the results and supporting documentation related to any 3rd party or internal testing performed on the EPBS. Supporting documentation shall include, but not be limited to, test plans, test cases and results from all security testing (vulnerability, penetration, etc.) that was done on the system. Vendor shall also provide how any vulnerabilities were mitigated and any which are outstanding.	Mandatory	Evaluation	Vendor		X	Pass
S-59	The EPBS shall uniquely identify and authenticate defined types of devices that require authentication mechanisms before establishing a connection that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access.	Mandatory	Identification & Authorization	Entire ePoll Book System	X		Pass
S-60	Vendor shall describe, for hosted solution offerings, how their incident response plan documentation aligns with NIST SP 800-61.	Mandatory	Incident Response	Vendor		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-61	Vendor shall describe how any file to be used within the EPBS, (e.g., for information exchange with other election systems, audit purposes, etc.,) can be hashed and/or cryptographically signed before it is exported from the EPBS. Vendor shall describe if their solution achieves this in compliance with Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard.	Mandatory	Integrity	Vendor		X	Pass
S-62	The EPBS shall be protected against malware. The vendor shall provide documentation of controls within the system and procedural recommendations relevant to this.	Mandatory	Integrity	Vendor	X	X	Pass
S-63	Vendor shall describe how they: a. Identify, report, and correct EPBS flaws b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation c. Install security-relevant software and firmware updates as required d. Incorporate flaw remediation into the organizational	Mandatory	Integrity	Vendor		X	Pass
S-64	Vendor shall describe how remote system administration, software package deployment and system updates are done securely (e.g. secure protocols such as TLS, IPSEC, etc.).	Mandatory	Integrity	Entire ePoll Book System		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-65	Vendor shall describe how their EPBS solution verifies the integrity of the code base and future software updates (e.g. hashing algorithms, digital signatures, etc.).	Mandatory	Integrity	Vendor		X	Pass
S-66	Vendor shall describe how EPBS-PS are synchronized/networked with other EPBS-PS within the same polling place/county (including any diagrams or flow charts).	Mandatory	Network	ePoll Book/Poll Site	X	X	Pass
S-67	Vendor shall describe how all voter activity shall be securely captured and protected during an interruption in network connectivity of an EPBS-PS. The EPBS-PS shall have the capacity to securely transmit that voter activity upon connectivity being restored.	Mandatory	Network	Entire ePoll Book System	X	X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-68	Vendor shall describe, if an electronic poll book device be enabled or installed with wireless technology, the wireless security controls that are in place to include, but not be limited to, the following: a. Encryption type and strength: Wi-Fi Protected Access II (WPA2) / Wi-Fi Protected Access III (WPA3) – Advanced Encryption Standard (AES) must be utilized and a minimum 256-bit key encryption length b. Use of personal firewall on wireless client devices c. What default factory settings have been changed (e.g., SSIDS, pass phrases) d. What wireless settings/options are configurable by CBOE (e.g., SSIDS, pass phrases, transmission power) e. How the wireless access points are physically protected against tampering f. Type of authentication used between access point and connected devices g. Use of static IP address, no DHCP utilized h. What wireless settings/options cannot be changed i. Capability to disable wireless j. Built-in wireless intrusion detection system, if any	Mandatory	Network	Network		X	Pass
S-69	The EPBS shall enable WPA3 for all wireless connections, if available. If WPA3 is not available, WPA2 shall be used.	Mandatory	Network	Network	X		Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration / Artifact	Response	Pass/Fail
S-70	Vendor shall provide a detailed list of system error messages one might see while using the EPBS, definition of what the message means, and actions which shall be taken to address each error.	Mandatory	Operational	ePoll Book/Poll Site		X	Pass
S-71	Vendor shall describe how the EPBS protects against unauthorized use. Vendor shall describe what physical or logical controls are in place to lock down or disable unused EPBS hardware interfaces (e.g. tamper evident seals, physical locks, disabled via secure configuration baseline) during use.	Mandatory	Physical	Vendor		X	Pass
S-72	Vendor shall describe what options are available to protect the EPBS-PS devices from theft or destruction during transport and voting (e.g. sealed case or enclosure).	Mandatory	Physical	ePoll Book/Poll Site		X	Pass
S-73	Vendor shall describe for EPBS-PS, what security risks are mitigated through the use of and verification upon removal of tamper evident seals.	Mandatory	Physical	ePoll Book/Poll Site		X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration / Response Artifact	Pass/Fail
S-74	Vendor shall describe how redundancy is built into the EPBS to minimize risk of failure or data loss and to ensure high availability.	Mandatory	Server	Entire ePoll Book System	X	Pass
S-75	Vendor shall document how the EPBS protects the integrity and confidentiality of transmitted information.	Mandatory	System and Communication	Vendor	X	Pass
S-76	Vendor shall describe how, if utilized, public key certificates are issued under an appropriate certificate policy or public key certificates are obtained from an approved service provider.	Mandatory	System and Communication	Network	X	Pass
S-77	Vendor shall describe how the EPBS fails to a known secure state for all failures, while preserving the maximum amount of system state information.	Mandatory	System and Communication	Entire ePoll Book System	X	Pass

Req #	Electronic Poll Book System Security Requirements	Status	Category	Implemented at	Demonstration	Response / Artifact	Pass/Fail
S-78	Vendor shall produce security patches within the service-level agreement (SLA) timelines and shall provide instructions on how to keep the hardware and software up to date.	Mandatory	Network	Entire ePoll Book System		X	Pass
S-79	Vendor shall describe how software and devices meet the least functionality principle and disable unneeded services such as telnet, SNMP and remote administration (Web Mode) etc.	Mandatory	Network	Network		X	Pass

7.4 Challenge Report Requirements

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
CR-1	County Board of Elections are required to complete a challenge report based on the criteria set forth in New York State Election Law §8–508. Challenge report; preparation. The vendor shall describe if and how their solution implements the requirements for each section of the challenge report. If the vendor's solution does not implement this functionality' in their response. Please see attached appendices required to complete the challenge process (Challenge Report, Challenge Report Inspector Certification, Challenge Poll Site Oaths)	Mandatory	Functional		X	Pass
CR-2	Section One – change of name or address The EPBS-PS may provide inspectors of election the ability to enter the name, address and registration serial number of each person who claims a change in name, or a change of address within the election district, together with the new name or address of each such person. The EPBS-PS may provide a place in the voter's record for the inspectors to record the information required to be entered in such 'section one' or provide a separate section for the inspectors of election to enter such information in the EPBS-PS.	Optional	Functional	X		Fail
CR-3	Section Two – voters challenged The EPBS-PS may provide inspectors the ability to enter the name, address and county voter ID of each person who is challenged on the day of election, together with the reason for the challenge. The EPBS-PS may provide a place in the voter's record for the inspectors to record the information required to be entered in such 'section two' or provide a separate section for the inspectors to enter such information in the EPBS-PS. If no voters are challenged, the EPBS-PS shall provide inspectors the ability to enter the words "No Challenges'' in the space reserved for such names in the EPBS-PS.	Optional	Functional	X		Fail
CR-4	Section Three – voters requiring assistance and who assisted The EPBS-PS may provide inspectors the ability to enter the name, address and county voter ID of each voter given assistance, together with the reason the voter was allowed assistance, the name of the person giving such assistance and his address if not an inspector. The EPBS-PS may provide a place next to the voter's name for the inspectors to record the information required to be entered in such 'section three' or provide a place for the inspectors to enter such information in the EPBS-PS. If no voters are given assistance, the EPBS-PS shall provide inspectors the ability to enter the words ''No Assistance'' in the space reserved for such names in the EPBS-PS.	Optional	Functional	X		Fail

Req #	Electronic Poll Book System Functional Requirements	Status	Category	Demonstration	Response/Artifact	Pass/Fail
CR-5	Section Four – voters pursuant to court order or affidavit The EPBS-PS may provide inspectors the ability to enter the name, address and county voter ID of each person who was permitted to vote pursuant to a court order, or to vote on a paper ballot which was inserted in an affidavit envelope. The EPBS-PS may provide a place in the voter's record for the inspectors to record the information required to be entered in such 'section four' or provide a place for the inspectors to enter such information in the EPBS-PS. If there are no such names, the EPBS-PS shall provide inspectors the ability to enter the word "None" in the space provided for such names in the EPBS-PS.	Optional	Functional	X		Fail
CR-6	The EPBS-PS may be capable of printing a challenge report which contains the names of: - All persons who were reported a name or address change (section 1); - All persons who were challenged on the day of election, and that each voter so reported as having been challenged took the oaths as required (section 2); - All voters to whom such board gave or allowed assistance and lists the nature of the disability which required such assistance to be given and the names and family relationship, if any, to the voter of the persons by whom such assistance was rendered; that each such assisted voter informed such board under oath that he required such assistance and that each person rendering such assistance took the required oath (section 3); - All voters who were permitted to vote although their registration poll records were missing (affidavit ballots / court orders) (section 4)	Optional	Functional	X		Fail
CR-7	The EPBS-PS may be capable of printing a certification at the end of the challenge report stating that the entries made are a true and accurate record of its proceedings with respect to the persons named in such report.	Optional	Functional	X		Fail
CR-8	The EPBS-PS may be capable of printing additional information on the challenge report including but not limited to: - City / town - Ward - Election District - Assembly district - Oath - Space for signatures of the board of inspectors of election - Space for notes	Optional	Functional	X		Fail

7.5 Technical Data Package Review

NYSTEC performed an examination and review of the totality of materials provided by the vendors in response to the TDP Requirements of the *Electronic Poll Book System (EPBS) Application for Approval Checklist*. The *Voluntary Voting System Guidelines 1.0 2005* was used as a framework for guidance to determine contents of each of the 12 TDP sections. Each submission was reviewed to determine if the vendor had provided information for each of the categories listed, and enough information in the aggregate to comply with the requirement's stated purpose of identifying the full system configuration for evaluation.

Technical Data Package contents include the following:

- System configuration overview

- System hardware specifications

- System test and verification specifications

- User/system operations procedures

- Personnel deployment and training requirements

- Quality assurance program

- System functionality description

- Software design and specifications

- System security specifications

- System maintenance procedures

- Configuration management plan

- System change notes

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
1	System Configuration Overview	VVSG Vol 2: 2.2	System Overview	In the system overview, the vendor shall provide information that enables identification the functional and physical components of the system, how the components are structured, and the interfaces between them. The vendor shall include system description and details of the system performance.	Tenex TDP pages 2,3
2	System functionality description	VVSG Vol 2: 2.3	System Description	The vendor shall declare the scope of the system's functional capabilities, thereby establishing the performance, design, test, manufacture, and acceptance context for the system. The vendor shall provide a listing of the system's functional processing capabilities, encompassing capabilities required by the Guidelines and any additional capabilities provided by the system. This listing shall provide a simple description of each capability. Detailed specifications shall be provided in other documentation required for the TDP.	Tenex TDP pages 6-8
3	System hardware specifications	VVSG Vol 2: 2.4	System Hardware Specification	The vendor shall expand on the system overview by providing detailed specifications of the hardware components of the system, including specifications of hardware used to support the telecommunications capabilities of the system, if applicable.	Tenex TDP Page 5, 7730 Configuration Updated, MiFiGuideTemplate, iOS_Security Guide, CIS_Microsoft_Windows_Serve r_2016_RTM_Release_1607_B enchmark_v.1.1.0
4	System hardware specifications	VVSG Vol 2: 2.4.2	Design and Construction	The vendor shall provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing. The vendor shall provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.	Tenex TDP Page 5, 7730 Configuration Updated, MiFiGuideTemplate, iOS_Security Guide, CIS_Microsoft_Windows_Serve r_2016_RTM_Release_1607_B enchmark_v.1.1.0

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
5	System hardware specifications	VVSG Vol 2: 2.4.1	System Hardware Characteristics	The vendor shall provide a detailed discussion of the characteristics of the system including: -Performance characteristics: basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance. -Physical characteristics: This discussion addresses suitability for intended use, requirements for transportation and storage, health and safety criteria, security criteria, and vulnerability to adverse environmental factors. -Reliability: This discussion addresses system and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability. -Maintainability: Maintainability represents the ease with which maintenance actions can be performed based on the design characteristics of equipment and software and the processes the vendor and election officials have in place for preventing failures and for reacting to failures. Maintainability includes the ability of equipment and software to self-diagnose problems and make non-technical election workers aware of a problem. Maintainability also addresses a range of scheduled and unscheduled events. -Environmental conditions: This discussion addresses the ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, any additional facilities or resources required to install and operate the system	Tenex TDP Page 5, 7730 Configuration Updated, MiFiGuideTemplate, iOS_Security Guide, CIS_Microsoft_Windows_Server_2016_RTM_Release_1607_Benchmark_v.1.1.0

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
6	Software design and specifications	VVSG Vol 2: 2.5	Software Design and Specification	The vendor shall expand on the system overview by providing detailed specifications of the software components of the system, including software used to support the telecommunications capabilities of the system, if applicable. This includes software overview, software standards and conventions, software operating environment, hardware environment and constraints, software environment, software functional specifications, configurations and operating modes, software functions, programming specifications with overview and details, system database, interfaces, and interface identification and description.	Tenex TDP pages 15-17 TenexNY - SBE Additional Info Requested 5-16-19, 7730 Configuration Updated, MiFiGuideTemplate, CIS_Microsoft_Windows_Serve r_2016_RTM_Release_1607_B enchmark_v.1.1.0
7	System security specifications	VVSG Vol 2: 2.6	System Security Specification	Vendors shall submit a system security specification that addresses the level of security provided by the system in terms of the specific security risks addressed by the system, the means by which each risk is addressed, the process used to test and verify the effective operation of security capabilities and, for systems that use public telecommunications networks the means used to keep the security capabilities of the system current to respond to the evolving threats against these systems.	Tenex TDP, page 11, iOS_Security Guide, MiFiGuideTemplate, Precinct Central Security Features #1, Precinct Central Security Features #2, CIS_Microsoft_Windows_Serve r_2016_RTM_Release_1607_B enchmark_v.1.1.0
8	System security specifications	VVSG Vol 2: 2.6.1	Access Control Policy	The vendor shall specify the features and capabilities of the access control policy recommended to purchasing jurisdictions to provide effective EPBS security. The access control policy shall address the general features and capabilities and individual access privileges.	Tenex TDP, page 11, iOS_Security Guide, MiFiGuideTemplate, Precinct Central Security Features #1, Precinct Central Security Features #2, CIS_Microsoft_Windows_Serve r_2016_RTM_Release_1607_B enchmark_v.1.1.0

ePoll Book TDP Submission Analysis - Tenex

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
9	System security specifications	VVSG Vol 2: 2.6.2	Access Control Measures	The vendor shall provide a detailed description of all system access control measures and mandatory procedures designed to permit access to system states in accordance with the access policy, and to prevent all other types of access. The vendor also shall define and provide a detailed description of the methods used to preclude unauthorized access to the access control capabilities of the system itself.	*Tenex TDP, page 11, iOS_Security Guide, MiFiGuideTemplate, Precinct Central Security Features #1, Precinct Central Security Features #2, CIS_Microsoft_Windows_Server_2016_RTM_Release_1607_Benchmark_v.1.1.0*
10	System security specifications	VVSG Vol 2: 2.6.3	Equipment and Data Security	The vendor shall provide a detailed description of system capabilities and mandatory procedures for purchasing jurisdictions to prevent disruption of the voting process and corruption of voting data. This information shall address measures for polling place security.	*Tenex TDP page 11, iOS_Security Guide, MiFiGuideTemplate, Precinct Central Security Features #1, Precinct Central Security Features #2, CIS_Microsoft_Windows_Server_2016_RTM_Release_1607_Benchmark_v.1.1.0*
11	System security specifications	VVSG Vol 2: 2.6.4	Software Installation	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure software (including firmware) installation to meet the specific requirements. This information shall address software installation for all system components.	*Tenex TDP page 9* Devices are delivered pre-installed

ePoll Book TDP Submission Analysis - Tenex

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
12	System security specifications	VVSG Vol 2: 2.6.5	Telecommunications and Data Transmission Security	The vendor shall provide a detailed description of the system capabilities and mandatory procedures for purchasing jurisdictions to ensure secure data transmission. For all systems, this information shall address access control, and prevention of data interception.	*iOS_Security Guide, Precinct Central Security Features #1, Precinct Central Security Features #2, MiFiGuide Template*
13	System test and verification specifications	VVSG Vol 2: 2.7	System Test and Verification Specification	The vendor shall provide test and verification specifications for development test specifications. The vendor shall describe the plans, procedures, and data used during software development and system integration to verify system logic correctness, data quality, and security.	*Tenex TDP pages 9-11*
14	User/system operations procedures	VVSG Vol 2: 2.8	System Operations Procedures	This documentation shall provide all information necessary for system use by all personnel who support pre-election and election preparation, polling place activities and central counting activities, as applicable, with regard to all system functions and operations identified in Subsection 2.3 above. The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel. The system operations procedures shall contain all information that is required for the preparation of detailed system operating procedures, and for operator training. This includes details describing the operational environment, system installation and test specification, operational features, operating procedures, and operations support.	*Tenex TDP page 18 -68*

ePoll Book TDP Submission Analysis - Tenex

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
15	System maintenance procedures	VVSG Vol 2: 2.9	System Maintenance Manual	The system maintenance procedures shall provide information in sufficient detail to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field. Technical documentation needed solely to support the repair of defective components or modules ordinarily done by the manufacturer or software developer is not required. Recommended service actions to correct malfunctions or problems shall be discussed, along with personnel and expertise required to repair and maintain the system; and equipment, materials, and facilities needed for proper maintenance. This manual shall include maintenance procedures, corrective maintenance procedures, preventative maintenance procedures, identification of maintenance equipment as well as parts and materials, common standards, maintenance facilities and support.	*Tenex TDP page 11*
16	Personnel deployment and training requirements	VVSG Vol 2: 2.10	Personnel Deployment and Training Requirements	The vendor shall specify the number of personnel and skill levels required to perform each of the following functions: Pre-election or election preparation functions (e.g., entering an election, generating pre-election reports. System operations for voting system functions performed at the polling place System operations for voting system functions performed at the central count facility Preventive maintenance tasks. Diagnosis of faulty hardware or software Corrective maintenance tasks. Testing to verify the correction of problems.	*Tenex TDP page 12,13,14*

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
17	Configuration management plan	WVSG Vol 2: 2.11	Configuration Management Plan	Vendors shall submit a Configuration Management Plan that describes all policies, processes, and procedures employed by the vendor to carry out these requirements. Information submitted by the vendor shall be used by to assist in developing and executing the test plan. This information is particularly important to support the design of test plans for system modifications. A well-organized, robust and detailed Configuration Management Plan will enable testers to more readily determine the nature and scope of tests needed to fully test the modifications.

The Configuration Management Plan shall contain Configuration Management Policy, Configuration Identification, Baseline and Promotion, Configuration Control Procedures, Release Process, Configuration Audits, and Configuration Management Resources. | Tenex TDP pages 3,4,5 |
| 18 | Quality assurance program | WVSG Vol 2: 2.12 | Quality Assurance Program | Vendors shall submit a Quality Assurance Program that addresses the quality assurance policies, processes, and procedures employed by the vendor to ensure the overall quality of the system for its initial development and release and for subsequent modifications and releases. This information is particularly important to support the design of test plans by the accredited test lab. A well-organized, robust and detailed Quality Assurance Program will more readily determine the nature and scope of tests needed to test the system appropriately. The Quality Assurance Program shall, at a minimum, address Quality Assurance Policy, Parts and Materials Tests, and Quality Conformance Inspections. | Tenex TDP page 15, TenexNY - SBE Additional Info Requested 5-16-19 |

ePoll Book TDP Submission Analysis - Tenex

#	Application Requirements	VVSG Vol. 2 Mapping	Requirement Type (VVSG Category)	Guidance	Documentation Provided
19	System change notes	VVSG Vol 2: 2.13	System Change Notes	Vendors submitting modifications for a system that has been previously approved by NYSBOE shall submit system change notes. These will be used to assist in developing and executing the test plan for the modified system. The an example of the system change notes shall include the following information: Summary description of the nature and scope of the changes, reasons for each change, a listing of the specific changes made, citing the specific system configuration items changed, providing detailed references to the documentation sections changed, a detail of the specific sections of the documentation that are changed (or completely revised documents, if more suitable to address a large number of changes), documentation of the test plan and procedures executed by the vendor for testing the individual changes, and the system as a whole, and records of test results.	Tenex TDP page 12