



Proposed Resolution 24-06

February 6, 2024

Approval of Voter Registration System

WHEREAS, Part 6217.3 of the Rules and Regulations of the State Board of Elections requires that any proposed county voter registration system must be approved by the State Board to ensure it meets the technical specifications promulgated by the State Board to interface with the official statewide voter registration list prior to the purchase or installation of the system; and

WHEREAS, ES&S has submitted PowerProfile Voter Registration System for approval to be used in New York State; and

WHEREAS, the State Board's Election Operations and Information Technology Units have been tasked with evaluating both existing and proposed systems to ensure they meet functional, communications, security and any other relevant standards; and

WHEREAS, the staff from such units have conducted an evaluation of said system, and have provided a summary report for the consideration of the Board; and

WHEREAS, having considered the reports and the results of evaluation the Election Operations and Information Technology Units, recommend the approval of the ES&S PowerProfile Voter Registration System for use in New York State;

NOW THEREFORE BE IT RESOLVED that having considered the reports and the results of evaluation the Commissioners of the New York State Board of Elections, do hereby approve the ES&S PowerProfile Voter Registration System.



ES&S PowerProfile Voter Registration System Vendor Assessment Report

40 North Pearl Street, Suite 5

Albany, NY 12207-2729

January 30, 2024

Version 1.0

Table of Contents

PowerProfile Voter Registration System Vendor Assessment Report.....	1
1. Introduction.....	3
2. System Overview	3
3. Compliance Testing	4
3.1 Functional	4
3.2 Security	4
3.3 Communications	5
4. Technical Data Package	5
5. Conclusion	6
6. Appendix - Voter Registration System Requirements	7

1. Introduction

The Help America Vote Act (HAVA), Section 303, requires states to implement a single, centralized interactive computerized statewide voter registration list. The list must contain the name and registration information of every legally registered voter in the state and assign a unique identifier to each. Resulting from New York State Election Law (ELN) §5-614, there is a statewide secure electronic voter registration data repository known as NYSVOTER. Every county board of elections (CBOE) is mandated to supply voter registration (VR) data to NYSVOTER, which contributes to a centralized VR database. It is incumbent upon each CBOE to provide accurate, up-to-date VR data to NYSVOTER. Various VR technologies have been deployed across the counties to store VR data and provide it to NYSVOTER.

Part 6217 of the Rules and Regulations of the State Board of Elections requires that every county voter registration system must be approved by the State Board to ensure it continually meets the functional, technical and security specifications promulgated by the State Board for interfacing with the official statewide voter registration list. For proposed systems, this approval must be obtained prior to sending data to the statewide list. See the Appendix for a complete list of the requirements used for evaluation.

The NYSBOE testing process will verify that mandatory functional, security, and communication requirements are met by the proposed VR system. Requirements will be tested against each vendor configuration and will it be determined if the requirement has been implemented successfully 'Pass' or unsuccessfully 'Fail'. The submitted configuration will be considered a 'pass' if the VR system successfully implements all mandatory requirements, has a documented non-impact issue that has no negative affect system usage or implements an approved compensating control(s).

This report details the results of the testing conducted by NYSBOE.

2. System Overview

The PowerProfile voter registration solution was submitted for State Board approval. PowerProfile is designed for use by CBOE staff to conduct multiple election management tasks. The configuration consists of a local application that is accessed by secured local computers through a secure web address, communicating with a central application host. The web environment is either hosted on site on a localized server, or at a centralized vendor hosted server.

The PowerProfile solution has modules for election management, voter registration, polling place management, absentee ballots, and petitioning. The focus of State Board approval is functional and secure access and data exchange to the NYSVoter system.

3. Compliance Testing

To ensure compliance with a number of designated functional and security requirements, PowerProfile was required to show either via demonstration or through the provisions of 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, Security and Communications Requirements.

3.1 Functional Testing

There are 135 requirements to be evaluated during functional testing which are required under various sections of Election Law. Of these requirements, 85 focus on data elements, 29 focus on functionality and 21 focus on reporting.

After demonstration of the VR system to comply with particular requirements, and 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.

3.2 Security Testing

There are 71 requirements to be evaluated during security testing. Of these requirements, sixteen (16) related to Access Control, Audit, and Backup & Recovery are dependent on

implementation by the CBOE and their IT support. ES&S will provide documentation to support County compliance with these requirements.

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.

3.3 Communications Testing

To ensure compliance, the vendor was required to test communications with the NYSVoter system. There were 141 requirements to be evaluated during communications testing. Testing was conducted using the NYSVoter test environment, over the course of two months in an iterative process. All the test cases were required to be completed successfully. This was done to the satisfaction of the NYSBOE NYSVoter team.

4. Technical Data Package

ES&S 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 (TDP) contents:

- 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

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

5. Conclusion

The PowerProfile voter registration system was submitted to the State Board for evaluation. It was tested for compliance with all requirements promulgated by the State Board for said systems, 347 individual requirements in all, broken down into three main categories – functional, security and communications. The results testing showed that, either via demonstration or through the provisions of documentation or narratives, that the PowerProfile system complies with all mandatory requirements. As mentioned in Section 3.2 (Security Testing), there were a number of requirements for which compliance is dependent on the implementation of this system by the CBOE and their IT support. Therefore, additional review of any county's implementation of this software will be necessary to ensure that compliance with all requirements is maintained.

6. Appendix - Voter Registration System Requirements

Functional Requirements

Requirement #	Field Name/Description	Election Law/NYCCR Reference	Required or Optional	Required Field Values/Voter Optional
FDEVR-1	Last Name	§6217.4(d)	Required	
FDEVR-2	First Name	§6217.4(d)	Required	
FDEVR-3	Middle Initial	§6217.4(d)	Required	
FDEVR-4	Name Suffix	§6217.4(d)	Required	
FDEVR-5	Residence House Number	§6217.4(d)	Required	
FDEVR-6	Residence Fractional Address Number	§6217.4(d)	Required	
FDEVR-7	Residence Apartment	§6217.4(d)	Required	
FDEVR-8	Residence Street Name	§6217.4(d)	Required	
FDEVR-9	Residence Pre Street Direction	§6217.4(d)	Required	
FDEVR-10	Residence Post Street Direction	§6217.4(d)	Required	
FDEVR-11	Residence City	§6217.4(d)	Required	
FDEVR-12	Residence Zip Code 5	§6217.4(d)	Required	
FDEVR-13	Residence Zip Code plus 4	§6217.4(d)	Required	
FDEVR-14	Indication of non-standard residence address	§6217.4(d)	Required	
FDEVR-15	Mailing House Number	§6217.4(d)	Required	
FDEVR-16	Mailing Apartment	§6217.4(d)	Required	
FDEVR-17	Mailing PO Box Number	§6217.4(d)	Required	
FDEVR-18	Mailing Street Name	§6217.4(d)	Required	
FDEVR-19	Mailing Pre Street Direction	§6217.4(d)	Required	
FDEVR-20	Mailing Post Street Direction	§6217.4(d)	Required	
FDEVR-21	Mailing City	§6217.4(d)	Required	
FDEVR-22	Mailing Zip Code 5	§6217.4(d)	Required	
FDEVR-23	Mailing Zip Code plus 4	§6217.4(d)	Required	
FDEVR-24	Date of Birth	§6217.4(d)	Required	
FDEVR-25	Telephone	§6217.4(d)	Required	Voter Optional
FDEVR-26	Email	§5-500(d)	Required	Voter Optional
FDEVR-27	Gender/Sex	§6217.4(d)	Required	Voter Optional
FDEVR-28	NYS Driver's License Number	§6217.4(d)	Required	
FDEVR-29	NYS Non-Driver's License Number	§6217.4(d)	Required	
FDEVR-30	Last 4 of SSN	§6217.4(d)	Required	
FDEVR-31	Indication of no driver's license number, no non-driver's license, or no SSN	§6217.4(d)	Required	
FDEVR-32	Political Party	§6217.4(d)	Required	
FDEVR-33	Signature	§6217.4(d)	Required	
FDEVR-34	Voter previously registered	§5-500(4)(g)	Required	
FDEVR-35	Last Date Voted	§5-500(4)(g)	Required	
FDEVR-36	Previous Last Name	§5-500(4)(g)	Required	
FDEVR-37	Previous First Name	§5-500(4)(g)	Required	

FDEVR-38	Previous Middle Initial	§5-500(4)(g)	Required	
FDEVR-39	Previous Name Suffix	§5-500(4)(g)	Required	
FDEVR-40	Previous House Number	§5-500(4)(g)	Required	
FDEVR-41	Previous Fractional Address Number	§5-500(4)(g)	Required	
FDEVR-42	Previous Apartment	§5-500(4)(g)	Required	
FDEVR-43	Previous Street Name	§5-500(4)(g)	Required	
FDEVR-44	Previous Pre Street Direction	§5-500(4)(g)	Required	
FDEVR-45	Previous Post Street Direction	§5-500(4)(g)	Required	
FDEVR-46	Previous City	§5-500(4)(g)	Required	
FDEVR-47	Previous Zip Code 5	§5-500(4)(g)	Required	
FDEVR-48	Previous Zip Code plus 4	§5-500(4)(g)	Required	
FDEVR-49	Length of residence in county or city	§5-500(4)(f)	Required	
FDEVR-50	US Citizen	§5-500(4)(i)	Required	
FDEVR-51	Statewide Unique Identifier	§6217.4(d)	Required	
FDEVR-52	Voter Status Code	§6217.4(d) §6217.9	Required	Active Active Military Active UOCAVA Active Special Presidential Active Special Federal Inactive per election material returned undeliverable Inactive per moved with no forwarding address Inactive per affidavit ballot Inactive per mail check Inactive per NCOA Inactive per returned mail Purged per death Purged per voter request Purged per felon Purged per ADF incompetent Purged per NVRA Purged per moved out of county
FDEVR-53	County Voter Registration Number	§6217.4(d)	Required	
FDEVR-54	County Code	§6217.4(d)	Required	
FDEVR-55	County	§6217.4(d)	Required	
FDEVR-56	Data Entry Date	§6217.4(d)	Required	
FDEVR-57	Application Date	§6217.4(d)	Required	
FDEVR-58	Registration Date	§5-500(4)(c)	Required	
FDEVR-59	Application Source Code	§6217.4(d)	Required	
FDEVR-60	Indication Voter is Unable to Sign	§5-506(c)	Required	
FDEVR-61	Voter History	§6211.6(d)(e)(f)	Required	Which elections voter voted in
FDEVR-62	Voter History Method	§6211.6(d)(e)(f)	Required	What method voter voted by in given election
FDEVR-63	Home political subdivision	§5-500(4)(f)	Required	
FDEVR-64	Election District	§5-500(4)(f)(g)	Required	
FDEVR-65	Town	§5-500(4)(f)(g)	Required	
FDEVR-66	Town Ward	§5-500(4)(f)	Required	
FDEVR-67	Ward	§5-500(4)(g)	Required	
FDEVR-68	Assembly District	§5-500(4)(f)(g)	Required	

FDEVR-69	Legislative District	§5-500(4)(g)	Required	
FDEVR-70	Congressional District	§5-500(4)(f)	Required	
FDEVR-71	Senate District	§5-500(4)(f)	Required	
FDEVR-72	Signature from system and signature signed by the voter when voting	§5-506(c)	Required	
FDEVR-73	USPS Coding Accuracy Support Service Address	§6217.4(d)	Optional	
FDEVR-74	Identification required flag	§5-500(4)(f)	Required	
FDEVR-75	Identification Verification requirement met flag	§5-500(4)(f)	Required	
FDEVR-76	Length of voter's residence in county or city calculated to the time of the next general election	§5-500(4)(f)	Required	
FDEVR-77	Voter Transaction History	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-78	Voter Transaction History Change Made	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-79	Voter Transaction History Reason Change Made	§5-500(4)(f) §6217.1(b) §6217.1(b)	Required	
FDEVR-80	Voter Transaction History Change Date	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-81	Voter Transaction History Change Time Stamp	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-82	Voter Transaction History the ID of the county board operator	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-83	Voter Transaction History system that updated record	§5-500(4)(f) §6217.1(b)	Required	
FDEVR-84	Voter Transaction History Key Element	§5-500(4)(f) §6217.1(b)	Required	Party Enrollment History Voter Name Voter Address Cancelled Registration Voter Status

Requirement #	VR System Feature	Election Law/NYCCR Reference	Required or Optional	Required Field Values (where applicable)	Specification of Requirement (where applicable)
FFVR-1	Require Bipartisan approval on all voter registration activity and transactions	§6217.5(c)	Required		
FFVR-2	Interact with NYSVoter send data	§6217.3 §6217.7	Required		
FFVR-3	Interact with NYSVoter receive notices	§6217.3 §6217.7	Required		
FFVR-4	Issuance of Absentee ballots	§5-614(3)	Required		
FFVR-5	Return of Absentee ballots	§5-614(3)	Required		
FFVR-6	Undeliverable Absentee ballots	§5-614(3)	Required		
FFVR-7	Invalidated Absentee ballots	§5-614(3)	Required		
FFVR-8	Duplicate Absentee ballot requests	§5-614(3)	Required		
FFVR-9	Administration of poll workers	§5-614(3)	Required		
FFVR-10	Administration of poll sites	§5-614(3)	Required		
FFVR-11	Assignment/Reassignment of Election Jurisdiction	§5-506(c)	Required		
FFVR-12	Ability to mark voters with specialized flags	§8-404(1) §10-106(2) §11-206 §15-122	Required	Specialized Flags Hospital Veteran/Hospital Veteran's relative Military Voter Special Federal Voter Permanently Disabled	
FFVR-13	Space for notes	§5-500	Required	Refusing to register applicant Challenged voters Cancellation of registration Enrollment Corrections Transferred Registrations Permanently Disabled	
FFVR-14	Flag that notice is needed	§6217.10	Required		
FFVR-15	Inclusion of voters for a specific election but not all elections	§5-302(4)	Required		
FFVR-16	Allow for parties to be added or deleted		Required		
FFVR-17	Allow for additional gender to be added		Required		
FFVR-18	Ability to filter or arrange by (multiple layers of filtering and arranging need to be supported)	§5-504(d) §4-100(3) §5-602(1) §6-204(4) §5-612(3) §5-500(4)(i) §5-704	Required	Alphabetize by Name Alphabetize by Streets Arrange Numeric Election District Party Registration Date Registration Status Village State for people that have registered with NY but reported being registered previously in another state	
FFVR-19	Store images of source document for voter signature	§5-506(d) §6212.8(c)	Required		registration poll record or voter registration application School Board Registration Military Registration Special Federal Registration Change of Name Registration FPCA Absentee Voting Application Absentee Ballot Envelope Affidavit Ballot Envelope Challenge Report Special Form, Card, Letter mailed to voter for signature
FFVR-20	Signature Quality Standards	§6212.8(d)	Required		Properly Positioned; Image quality of signature when printed, or on a computer screen for registration poll list, should be comparable
FFVR-21	Duplicate all computer registration files	§6212.10(a)	Required		
FFVR-22	Separate or separately store voter registration record of domestic violence victim	§5-508(2)	Required		
FFVR-23	Place for both commissioners to sign registration	§5-500(4)	Required		
FFVR-24	Report defines areas that may not have converted properly when using a new system		Optional		
FFVR-25	Reports can be exported to excel for functions that may be handled outside of system		Optional		
FFVR-26	Search function that provides near matches		Optional		
FFVR-27	Ability to migrate voter history from earlier system/NYSVoter		Optional		

FFVR-28	Function that allows system to flag any party affiliation change due to party no longer being recognized so that should the party become recognized again, voters' party affiliation can be reinstated		Optional		
FFVR-29	Ability to back-date date of registration for those received prior to deadline but processed after		Optional		

Requirement #	Report Description	Election Law/NYCCR Reference	Required or Optional	Required Field Values/Voter Optional
FRVR-1	Active Status Voters	§5-602(1)	Required	
FRVR-2	Voters per Election District	§4-134(2)	Required	
FRVR-3	Cancelled Registrations	§5-402(4)	Required	Last Name First Name
FRVR-4	Reinstated Voter Registrations	§5-404(2)	Required	
FRVR-5	Corrections	§5-226	Required	
FRVR-6	Permanently Disabled Voters	§5-612(1)	Required	
FRVR-7	Applicants for Special Presidential	§11-110(4)	Required	
FRVR-8	Applicants for Absentee Ballot	§15-118	Required	
FRVR-9	Voters to be Challenged	§8-502	Required	
FRVR-10	Registrants who name did not appear on the last list published	§5-602(1)	Required	
FRVR-11	Voters made inactive since annual enrollment	§5-602(1)	Required	
FRVR-12	Voters had registration cancelled since annual enrollment	§5-602(1)	Required	
FRVR-13	Voters who had registered and were previously registered in other	§5-704(1)	Required	Last Name First Name
FRVR-14	Names and Residence Addresses of hospitalized veterans and	§8-404(2)	Required	
FRVR-15	Persons whose applications were received	§5-210(15)(a)	Required	Last Name First Name
FRVR-16	Persons whose applications were approved	§5-210(15)(b)	Required	Last Name First Name
FRVR-17	Voter Registrations without a signature	§5-208(5)	Required	
FRVR-18	Voters reporting having previously been registered in another state	§5-704	Required	
FRVR-19	First Time voters in state that provided ID		Optional	
FRVR-20	Save report format for commonly pulled reports		Optional	
FRVR-21	When completing voter registrations, check against entries		Optional	

Communications Requirements

Requirement #	NYSVOTER Requirement	Applicable to NYSVOTER, VR System, or Both
NVR-1	GENERAL BUSINESS	
NVR-1.1	NYSVoter shall serve as the single statewide voter registration system for storing and managing the official list of registered voters throughout the state.	NYSVOTER
NVR-1.1.1	NYSVOTER must accept voter registration data directly from remediating county voter registration/election management systems (VR/EMS), which will serve as "front ends" to NYSVOTER.	NYSVOTER
NVR-1.1.2	NYSVOTER must ensure that all voter registration data used for processing and reporting in county VR/EMS is derived subsequently from the official data in NYSVOTER and is used unchanged.	NYSVOTER
NVR-1.2	NYSVOTER shall maintain one record for each registered voter, including the statewide unique identifier, entire history (including voting history, previous names, etc.) and status of that voter.	NYSVOTER
NVR-1.3	NYSVOTER shall provide the ability to automatically archive data based on business rules.	NYSVOTER
NVR-1.3.1	NYSVOTER shall provide the ability to archive data automatically based on user defined parameters.	NYSVOTER
NVR-1.3.2	NYSVOTER shall provide the ability to restore data from an archive.	NYSVOTER
NVR-1.3.3	NYSVOTER shall provide the ability to view online metadata for archived records.	NYSVOTER
NVR-1.5	NYSVOTER shall provide the ability to adjust business policies that govern the acceptance/correctness of data and the ability to change in response to changes in law and policy.	NYSVOTER
NVR-1.5.1	Whenever possible, business rules must be parameter based and configurable by NYSVOTER administrators.	NYSVOTER
NVR-1.2	Data Normalization and Validation	
NVR-1.2.1	NYSVOTER shall ensure that all data complies with the data standards for the database (proper coding for name suffix, street type, gender, etc.).	NYSVOTER
NVR-1.2.2	County systems must be configured so that all data sent to the centralized database meet NYSVOTER standards.	VR System
NVR-1.2.3	NYSVOTER shall ensure that all required fields have appropriate information.	NYSVOTER
NVR-1.2.4	County systems must be configured so that all required data is sent to the centralized database.	VR System
NVR-2	VOTER REGISTRATION	
NVR-2.1	Registration Processing	
NVR-2.1.1	Using their VR as the direct interface to NYSVOTER, county local election officials must be able to enter all voter registration information into the list at the time the information is provided to the county official. County VR systems shall synchronize with NYSVOTER at least every 24 hours.	VR System
NVR-2.1.1.1	NYSVOTER shall notify county VR of the receipt and status of each registration transaction, with appropriate detail.	NYSVOTER
NVR-2.1.1.2	NYSVOTER shall support an exception processing system that will track and report on such registration transactions awaiting resolution.	NYSVOTER
NVR-2.1.2	Both VR and NYSVoter shall track, normalize to standards, and store voter registrant information provided (current and prior) on the registration, including but not limited to:	Both
NVR-2.1.2.1	Full Name	Both
NVR-2.1.2.2	Residence Address (standard and non-standard)	Both
NVR-2.1.2.3	Mailing Address (if any) (standard and non-standard)	Both
NVR-2.1.2.4	Birthdate	Both
NVR-2.1.2.5	CASS Address	Both
NVR-2.1.2.6	Telephone Number (if any)	Both
NVR-2.1.2.7	Gender	Both
NVR-2.1.2.8	Last 4 Digits of Social Security Number	Both
NVR-2.1.2.9	Political Party Affiliation (or lack thereof)	Both
NVR-2.1.2.10	Registration Number	Both
NVR-2.1.2.11	New York DL#	Both
NVR-2.1.2.12	Data Entry Date	Both
NVR-2.1.2.13	Application Date (timestamp date)	Both
NVR-2.1.2.14	NVRA Tracking Code	Both
NVR-2.1.2.15	Last Year Voted	Both
NVR-2.1.2.16	Last County Voted In	Both
NVR-2.1.2.17	First Time Voter Status Flag	Both
NVR-2.1.2.18	ID Requirement Met Flag	Both
NVR-2.1.2.2	NYSVOTER must be able to collect/track the source of registrations and summarize/report on registration activity in accordance with NVRA reporting requirements.	NYSVOTER
NVR-2.1.3	NYSVOTER shall capture and store a graphic image of the signature on a registration application.	Both
NVR-2.1.3.1	NYSVOTER must receive and store the image of the signature captured and provided by the county VR/EMS (does not have to be at VR entry time).	Both

NVR-2.1.3.2	Upon request from the county VR/EMS, system must retrieve and provide the signature image to the requesting NYSVOTER, both individually and as part of a batch.	Both
NVR-2.1.3.3	<i>Associate Signature Image with VR Record</i> – NYSVOTER shall provide the ability to link and re-link card and signature image data to an existing voter record.	NYSVOTER
NVR-2.1.3.4	<i>Signature Images from VR</i> – Signatures will need to be captured from voter registration forms.	Both
NVR-2.1.3.5	<i>Ease of Signature Comparison</i> – The signatures shall be stored in a way to enhance speed of display. NYSVOTER shall provide functionality to assist data entry operators to visually verify that the captured signature is from the correct voter or applicant's document before associating the signature image to the voter registration/applicant's database record.	NYSVOTER
NVR-2.1.4	<i>Images in Format</i> – The scanned images shall be in a standard, nonproprietary format.	Both
NVR-2.1.5	<i>Capabilities and Restrictions of Image Editing</i> – NYSVOTER shall provide users with the ability to de-skew, rotate by single degrees or more, and de-speckle all scanned signature images. NYSVOTER shall not allow the authorized user to modify the basic characteristics, structure, and recognizable format of the registrant's signature.	Both
NVR-2.1.6	NYSVOTER shall track and maintain voter registration status; e.g., pending, active, inactive, canceled.	Both
F2.1.7	NYSVOTER shall store and track unverified registrations and shall provide notice to counties of missing/invalid information for their resolution.	NYSVOTER
NVR-2.1.8	NYSVOTER shall support eligibility determination of voter registrants.	Both
NVR-2.1.8.1	NYSVOTER shall verify whether the registrant will be at least 18 by any upcoming election. If so, NYSVOTER will flag registrant as pending until that election.	Both
NVR-2.1.9.2	NYSVOTER shall have the ability to process voter registrations entered in county VR/EMS for registrants who are not 18 at the time of entry into the county VR/EMS (i.e., send registration in early and county enters inactive registration) but will be 18 by election day (for inclusion in poll books).	Both
NVR-2.1.8.3	<i>Change of Political Party Enrollment</i> - Allow for voter registration political party change to be captured and made effective at a future date and not disclosed until that future date.	Both
NVR-2.1.8.4	NYSVOTER shall have the ability to process a voter registrant transaction for registrants who change party affiliation according to NYS Election Law (i.e., voter cannot vote in a primary after the party affiliation change if they registered after the last day to register in the previous year).	Both
NVR-2.1.9.2	NYSVOTER and remediated county VR/EMS shall allow for exception processing of registrations that do not process completely and automatically, allowing county election officials to resolve any issues and to accept or deny the registration (e.g., missing/invalid information).	Both
NVR-2.1.9.1	NYSVOTER shall store and track unverified registrations and shall provide notice to counties of missing/invalid information for their resolution.	NYSVOTER
NVR-2.1.10	NYSVOTER shall check voter's ID, and if it is determined that voter has no verified ID, the county is so notified. If voter is a first-time voter with no verified ID, county VR/EMS shall flag voter as requiring ID resolution to vote, and this flag shall be recorded in NYSVOTER.	NYSVOTER
NVR-2.1.10.1	When transactions fail, NYSVOTER must respond to the county system, providing notice of the failure and its cause(s). Further, a mechanism for notifying a county VR/EMS when a transaction sent from the county is not received by NYSVOTER shall be implemented, as well as the ability to re-send transactions from the county VR/EMS (i.e., ACK/NACK).	Both
NVR-2.1.11	NYSVOTER must maintain a transaction history associated with each registrant that is a record of changes made to a registration record. NYSVOTER must maintain a record history for every transaction associated with an applicant, beginning at the point an application is received. This must include each of the changes made and the reasons therefore. The transaction history must include a date and time stamp to record the date and time of change and the ID of the individual and system that updated the record, as well as key data elements that were changed.	Both
NVR-2.1.12	County System must be able maintain confidential voter	Both
NVR-2.2	Data Collection from County VR/EMS	
NVR-2.2.1	NYSVOTER must minimize interference with data entry and maintenance activities on county VR/EMS by remaining in the background throughout those activities.	NYSVOTER
NVR-2.2.2	NYSVOTER shall support near real-time data entry and interfacing between NYSVOTER and county VR/EMS.	Both
NVR-2.2.2.1	<i>Transaction Confirmations</i> - Provide confirming messages on acceptance of every transaction.	Both
NVR-2.2.3	<i>Flag VR Records</i> - NYSVOTER shall allow authorized county users to enter an indicator showing that research on a record is being performed and the record being searched may not be valid.	Both
NVR-2.3	DMV/SSA Verification	
NVR-2.3.1	NYSVOTER shall provide the ability to check—by driver license or non-driver number—for an existing voter registration record in NYSVOTER.	Both
NVR-2.3.2	NYSVOTER shall provide the ability to check—by driver license, non-driver number, or SSN4 in the DMV records—for ID verification.	Both
NVR-2.4	Voter Registration Finalization	
NVR-2.4.1	NYSVOTER shall assign a unique identifier to every registered voter.	Both
NVR-2.4.1.1	NYSVOTER shall have the ability to assign a unique identifier that will remain with the voter for their voting life.	Both
NVR-2.4.2	NYSVOTER shall store the registrant's home political subdivision(s).	Both
NVR-2.4.2.1	NYSVOTER shall accept district assignments provided by counties with county-entered registrations.	Both
NVR-2.4.3	NYSVOTER shall electronically notify the county VR/EMS with a response that includes confirmation of the transaction, an assigned unique identifier, and registration status in NYSVOTER.	Both
NVR-2.4.4	NYSVOTER shall notify the "to" county and "from" county if a voter has moved his/her registration between the counties.	NYSVOTER
NVR-2.4.4.1	NYSVOTER shall facilitate the move process if the "to" county has been informed of the registrant's "from" county on the voter registration form or from the registrant to avoid any exception processing from NYSVOTER (e.g., marking the registration as a possible duplicate).	Both
NVR-2.4.4.2	For registration changes involving a move from one county to another, the transaction will be handled as an exception, with appropriate notices sent to each county involved for final resolution.	Both

NVR-2.4.4.3	In the case of a suspected duplicate, NYSVOTER shall flag the records and notify the counties of a possible move. The affected counties will determine if a move has occurred between counties. Where both counties definitively determine that a move has occurred between counties—based upon a match of an applicant's name, date of birth, signature, and either the state or federal ID number or matching of the previous address of the voter—the "from county" will cancel their voter record, and the "to county" will activate a new record and transfer the unique identifier. In all other cases of a suspected duplicate, the "from county" will inactivate their voter record, and the "to county" will activate a new record.	NYSVOTER
NVR-3	Voter Registration List Maintenance	
NVR-3.1	Voter Status and Classification Updates (Active, Inactive, Canceled, etc.)	
NVR-3.1.1	NYSVOTER shall provide the ability to identify and track all registered voters— regardless of status— per HAVA, NYS law, and SBOE rules and regulations.	Both
NVR-3.1.2	NYSVOTER shall have the capability to map status codes and reason codes from county VR/EMS into NYSVOTER.	Both
NVR-3.1.2.1	NYSVOTER shall allow a county election official to designate a voter as inactive, noting the reason for the designation, such as "election material mailed to registrant returned as undeliverable" or "moved with an out of county forwarding address," "affidavit ballots".	Both
NVR-3.1.2.2	NYSVOTER shall have the ability to record and track NCOA activities, such as identification of new address, and provide notification to the appropriate county.	NYSVOTER
NVR-3.1.2.3	NYSVOTER shall allow a county election official to reactivate an inactive voter and to record the reason for doing so.	Both
NVR-3.1.3	NYSVOTER shall allow a county election official to cancel a voter registration based upon specific NYS Election Law and county BOE business rules, and NYSVOTER shall capture reason(s) for cancellation.	Both
NVR-3.1.4	NYSVOTER shall have the capability to store and inquire on absentee status (e.g., permanents) (for future use pending policy).	Both
NVR-3.2	External Agency Updates (New/Re-Registration Activity, Death, Felon Status)	
NVR-3.2.1	NYSVOTER shall have the ability to receive death notifications from NYSDOH and from the NYC DOHMH. Upon full implementation, NYSVOTER shall be matched against the SSA Master Death Index. Notification shall be sent to the appropriate county for follow-up and determination.	NYSVOTER
NVR-3.2.2	NYSVOTER shall have the ability to receive felon and mentally incompetent notifications from OCA. Notifications shall be sent to the appropriate county for follow-up and determination.	NYSVOTER
NVR-3.2.3	NYSVOTER may receive data from DMV regarding license surrenders. Notifications shall be sent to the appropriate county for follow-up and determination.	NYSVOTER
NVR-3.2.4	NYSVOTER shall track and flag potential felon, mentally incompetent, or deceased voters to allow SBOE to monitor county resolution of those voters.	NYSVOTER
NVR-3.3	Duplicate Checking	
NVR-3.3.1	NYSVOTER shall perform a near real-time duplicate check to identify existing records at or near the time of data entry for new registration transactions.	Both
NVR-3.3.2	NYSVOTER shall provide the ability to perform ad hoc duplicate checks, on demand based, on a variety of user-defined criteria sets, including phonetic, transposition, and like spelling matches. Such checks may be statewide or customized for specific regions (multi-county) and must be conducted weekly.	NYSVOTER
NVR-3.4	Coding Accuracy Support NYSVOTER (CASS) Standardization	
NVR-3.4.1	NYSVOTER shall provide the ability to ensure that the registrant address used for mailing voter materials conforms to USPS standards for optimum mailing rates. (USPS certifies that the list has been cleaned via NCOA process and, therefore, gets CASS certification.)	Both
NVR-3.4.1.1	NYSVOTER should have the capability to process registrant addresses against USPS CASS to determine standardized address for optimal mailing rates.	Both
NVR-3.4.1.2	NYSVOTER should separately store the CASS (or other USPS) optimized address for mailing purposes (in addition to the registrant's designated residence and mailing address).	Both
NVR-3.4.1.3	Counties should have the capability to access/download/retrieve USPS standardized addresses.	Both
NVR-3.4.2	NYSVOTER shall provide the ability to ensure that in rural areas where USPS standards are not sufficient, a registrant's address conforms to a standard acceptable to the county.	Both
NVR-3.5	Bulk Record Updates	
NVR-3.5.1	NYSVOTER shall provide the ability to process bulk voter registration record updates from counties (e.g., precincting, street name changes, area code and zip code changes) and update the state official voter registration records accordingly.	Both
NVR-3.6	Districting	
NVR-3.6.1	NYSVOTER shall have the ability to track and keep up to date official district information maintained in county VR/EMS.	Both
NVR-4	ELECTION PROCESSING	
NVR-4.2	Voter History Updating	
NVR-4.2.1	NYSVOTER shall store whether a voter voted in an election (state, federal, or local) after it is captured in the county VR/EMS.	Both
NVR-5	REPORTS	
NVR-5.1	Data Analysis and Management Reporting	
NVR-5.1.1	NYSVOTER shall provide the ability to generate predefined and ad hoc queries and reports in formats as needed.	Both
NVR-5.1.1.1	NYSVOTER shall provide a third-party reporting tool (e.g., query by example) for ad hoc reporting requests.	NYSVOTER
NVR-5.1.2	NYSVOTER shall provide standard reports that can be easily selected from a NYSVOTER menu by authorized users.	Both
NVR-5.1.3	NYSVOTER shall provide the ability to filter reports based on key data fields contained in the output (date, county, etc.).	Both
NVR-5.1.4	NYSVOTER shall provide the ability to generate a computerized statewide voter registration list that is single, uniform, official, centralized, interactive, defined, maintained, and administered at the state level and contains the name and registration information of every legally registered voter in the state.	NYSVOTER

NVR-5.1.5	NYSVOTER shall generate the official voter registration list for the conduct of all federal, state, and local elections in the state.	NYSVOTER
NVR-5.1.6	NYSVOTER shall allow state and county users to conduct user-defined searches of the new NYSVOTER database.	NYSVOTER
NVR-5.1.7	NYSVOTER shall allow voter registration staff to establish data views, registrant status information, and statistical calculations to inform the decision-making process.	Both
NVR-5.1.7.1	The NYSVOTER shall provide the county VR/EMS access to its data for the generation of reports by the county system.	Both
NVR-5.1.8	NYSVOTER shall provide the ability to sort voter registrant data by district/county, birth date, and other information (e.g., last name, first name, voter registration number, address order).	Both
NVR-5.1.9	NYSVOTER shall provide the ability to compile and report on voter registration changes by registration source in compliance with National Voter Registration Act (NVRA) requirements.	Both
NVR-5.1.10	NYSVOTER shall provide the ability to compile and report on voter registration statistics by party and political district at specific times, in compliance with NYS Election Law.	Both
NVR-5.1.11	NYSVOTER shall provide the ability to compile and report on registration data for redistricting purposes.	NYSVOTER
NVR-5.1.12	NYSVOTER shall provide the ability to compile and report registration data to judicial districts for use in compiling jury pools according to user defined parameters.	NYSVOTER
NVR-5.1.13	NYSVOTER shall notify the county of all new or updated registrations processed by the state database on a given day (e.g., query by function).	Both
NVR-5.1.14	NYSVOTER shall sync with county VR/EMS prior to county printing of poll books.	Both
NVR-5.1.15	NYSVOTER shall have the ability to produce a report to monitor county file maintenance and resolution of duplicate, felon, mentally incompetent, or deceased voters (refer to business requirement F.3.2.4).	Both
NVR-5.2	Public Service Requests (PSR) Response	
NVR-5.2.1	NYSVOTER shall provide the ability to compile and provide extracts of voter registration data in a variety of formats to qualified users in compliance with NYS Election Law. These may include all or part of the registrant data as appropriate and legally qualified. (For instance, a candidate for a district is only entitled to the registrants within that district.)	NYSVOTER
NVR-5.2.1.1	NYSVOTER shall provide the ability to compile and provide electronic extracts of registrant data as requested by the purchaser.	NYSVOTER
NVR-5.2.1.2	NYSVOTER shall provide the ability to compile and provide extracts of registrants sorted by address (e.g., for district walking lists).	NYSVOTER
NVR-5.2.1.3	NYSVOTER shall provide the ability to compile and provide extracts of registrant data formatted for mailing labels.	NYSVOTER
NVR-5.3	Registrant Inquiries	
NVR-5.3.1	NYSVOTER should allow individuals to access information about themselves, including but not limited to:	NYSVOTER
NVR-5.3.1.2	Registration status	NYSVOTER
NVR-5.3.1.3	Party affiliation	NYSVOTER
NVR-5.3.1.4	Assigned district	NYSVOTER
NVR-5.3.1.5	Assigned polling place	NYSVOTER
NVR-5.3.1.6	Absentee status	NYSVOTER
NVR-5.3.1.7	Whether their provisional ballot was counted for any election, and if not, why not.	NYSVOTER
NVR-5.3.2	Access must be restricted in such a way that only the individual voter can access their own data.	NYSVOTER
NVR-6	Execution of Compliance Test Script	
NVR-6.1	D-14 County Interface Compliance Criteria_v 3.0	VR System
NVR-6.2	D-42 County_Compliance_Test_Script Ver 2_0	VR System
NVR-6.3	MOVE_Acceptance_Test_County	VR System
NVR-6.4	County system must import as described in StatePortalAbsenteeBallotDataFields_V1.2	VR System
NVR-6.5	County system must import as described in VoterSearch_WebSvc_1.2	VR System
NVR-7	Additional Voter Registration Operational Requirements	
NVR-7.1	County system must extract poll site information and the poll site mapping file in the format prescribed by SBOE to be uploaded using the NYSVOTER web application.	VR System
NVR-7.2	County system must extract the affidavit and absentee voter extract file in the format prescribed by SBOE for duplicate check after each election.	VR System
NVR-7.3	County system must demonstrate a report in their application to view a list of all rejected transactions (with at least a date range and transaction type search criteria).	VR System
NVR-7.4	County system must demonstrate capability to submit a rejected transaction.	VR System
NVR-7.5	County system must import as described in VoterSearch_WebSvc_1.2.	VR System
NVR-7.6	County must be able to change or move voter type (federal, military, etc.) during the election period.	VR System
NVR-7.7	County system must be able to find out missing voting history for a given election—if a list is provided by SBOE—and be able to resend that voting history to NYSVoter.	VR System
NVR-7.8	County system must be able to send missing signatures using global update if a list of those voters is provided by SBOE.	VR System
NVR-7.9	County system must be able to schedule and send voter audit if SBOE requests audit for a batch of voters, voters by status, or the entirety of county voters.	VR System
NVR-7.10	County system must provide a screen to manage web service credential so that a county user can view and/or change them. There should not be dependency on the vendor if there is a need to view or change a username and/or password. The username and password should not be hardcoded.	VR System

NVR-7.11	The web service username and password must be encrypted at rest (at storage level).	VR System
NVR-7.12	County system must be able to schedule a voter history transaction using global update.	VR System
NVR-7.13	County system must be able to schedule and send jurisdiction changes (redistricting) to NYSVOTER. This should be done through global update for list of voters and not by voter update transactions	VR System

Security Requirements

Requirement #	Field Name/Description	Election Law/NYCCR Reference	Required or Optional	Required Field Values/Voter Optional
FDEVR-1	Last Name	§6217.4(d)	Required	
FDEVR-2	First Name	§6217.4(d)	Required	
FDEVR-3	Middle Initial	§6217.4(d)	Required	
FDEVR-4	Name Suffix	§6217.4(d)	Required	
FDEVR-5	Residence House Number	§6217.4(d)	Required	
FDEVR-6	Residence Fractional Address Number	§6217.4(d)	Required	
FDEVR-7	Residence Apartment	§6217.4(d)	Required	
FDEVR-8	Residence Street Name	§6217.4(d)	Required	
FDEVR-9	Residence Pre Street Direction	§6217.4(d)	Required	
FDEVR-10	Residence Post Street Direction	§6217.4(d)	Required	
FDEVR-11	Residence City	§6217.4(d)	Required	
FDEVR-12	Residence Zip Code 5	§6217.4(d)	Required	
FDEVR-13	Residence Zip Code plus 4	§6217.4(d)	Required	
FDEVR-14	Indication of non-standard residence address	§6217.4(d)	Required	
FDEVR-15	Mailing House Number	§6217.4(d)	Required	
FDEVR-16	Mailing Apartment	§6217.4(d)	Required	
FDEVR-17	Mailing PO Box Number	§6217.4(d)	Required	
FDEVR-18	Mailing Street Name	§6217.4(d)	Required	
FDEVR-19	Mailing Pre Street Direction	§6217.4(d)	Required	
FDEVR-20	Mailing Post Street Direction	§6217.4(d)	Required	
FDEVR-21	Mailing City	§6217.4(d)	Required	
FDEVR-22	Mailing Zip Code 5	§6217.4(d)	Required	
FDEVR-23	Mailing Zip Code plus 4	§6217.4(d)	Required	
FDEVR-24	Date of Birth	§6217.4(d)	Required	
FDEVR-25	Telephone	§6217.4(d)	Required	Voter Optional
FDEVR-26	Email	§5-500(d)	Required	Voter Optional
FDEVR-27	Gender/Sex	§6217.4(d)	Required	Voter Optional
FDEVR-28	NYS Driver's License Number	§6217.4(d)	Required	
FDEVR-29	NYS Non-Driver's License Number	§6217.4(d)	Required	
FDEVR-30	Last 4 of SSN	§6217.4(d)	Required	
FDEVR-31	Indication of no driver's license number, no non-driver's license, or no SSN	§6217.4(d)	Required	
FDEVR-32	Political Party	§6217.4(d)	Required	
FDEVR-33	Signature	§6217.4(d)	Required	
FDEVR-34	Voter previously registered	§5-500(4)(g)	Required	
FDEVR-35	Last Date Voted	§5-500(4)(g)	Required	
FDEVR-36	Previous Last Name	§5-500(4)(g)	Required	
FDEVR-37	Previous First Name	§5-500(4)(g)	Required	

Requirement #	NYSBOE Voter Registration (VR) Security Requirements	Cloud/On-prem/Both	Response/Artifact Required (X)
SVR-1	Limit the number of individuals with administrative access to the platform and remove default credentials.	Both	X
SVR-2	Ensure that users are greeted with a warning banner (acceptable use, no expectation of privacy, etc.).	Both	X
SVR-3	VR system auditing regarding other CBOE and NYSBOE for duplicates, moving, deaths, felons, etc.	Both	
SVR-4	If offered in the cloud or as a service, vendors shall host voter systems on separate secure network segments from their corporate networks.		X
SVR-5	Vendor must be a member of the Elections Infrastructure Information Sharing and Analysis Center (EISAC).	Both	X
SVR-6	Vendor must disclose its standardized software life cycle management process and time frame for addressing issues that may affect hardware and software components of its system, including, but not limited to: i) end-of-life software and/or hardware ii) unsupported or unpatched software iii) known vulnerabilities and exposures Additionally, Vendor must notify SBOE within 24 months of a hardware or software component manufacturer's product life cycle end date and must submit a plan within three months of such notification	Both	X
SVR-7	Vendor shall provide a system overview and functional diagram of the entire VR system and how each component integrates into it. The description shall include how the system is administered, configured, and managed.	Both	X
SVR-8	The VR system shall support the use of multifactor authentication.	Both	X
SVR-9	The VR system shall employ the principle of least privilege for each permitted role within the system, allowing authorized accesses only for users (or processes acting on behalf of users) who are necessary to accomplish assigned tasks, as well as administrators, and shall limit the number of individuals with administrative access on the platform, including the removal of default credentials. Vendor shall document how incorporated role-based access controls accomplish this	Both	X
SVR-10	Vendor shall describe what configuration item changes can be made by authorized individuals through system-defined Administration role(s).	Both	X
SVR-11	Vendor shall describe the capabilities of the VR system related to automated timeout of inactive sessions and shall provide evidence that the maximum inactivity period is configured for 15 minutes for all user accounts, noting any exceptions.	Both	X
SVR-12	Vendor is required to demonstrate that the VR system shall monitor and support: a. The ability to define groups and role-based access. b. The ability to create, enable, modify, disable, and archive VR system accounts. c. The ability to log and audit the use of VR system accounts	Both	
SVR-13	The VR system shall be required to: a. Enforce a configurable limit of five (5) 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.	Both	X
SVR-14	Vendor shall provide a system architecture diagram for its proposed solution that includes a description of how the solution is architected, addressing on-prem, cloud, hosted, or any combination thereof. If customer systems are needed to host software, information on how those systems must be configured and hardened shall be provided.	Both	X
SVR-15	The VR system 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 visible on the display	Both	
SVR-16	The VR system shall: a. Monitor for and prevent all unauthorized remote access, including wireless where relevant, to the VR system. 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. c. Employ cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Both	
SVR-17	The VR system shall require the use of unique user IDs.	Both	
SVR-18	The VR system shall adhere to password requirements (e.g., password length, password aging, password complexity, etc.) as outlined in PART 6220 - Cyber Security Requirements for Boards of Elections Section (12) Credential Management and Access.	Both	
SVR-19	The VR system shall be capable of providing comprehensive audit logs that can be exported in nonproprietary, human readable format.	Both	X
SVR-20	Vendor shall provide a listing and description of what messages and events generated by the VR system become part of the audit record.	Both	X
SVR-21	The VR system shall require capturing, at a minimum, date- and time-stamped records for actions performed by any user on the VR system, 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	Both	
SVR-22	The VR system shall support the generation of alerts to responsible staff (by role) when a log processing error occurs (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.).	Both	X
SVR-23	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 one another. This shall include the data format(s) the system is capable of importing and exporting.	Both	X
SVR-24	The VR system shall manage and allocate audit record storage capacity and configure auditing in compliance with PART 6220 - Cyber Security Requirements for Boards of Elections to reduce the likelihood of such capacity being exceeded.	Both	
SVR-25	The VR system shall provide the capability to review and analyze VR system audit records regularly for indications of inappropriate or unusual activity. The VR system 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.	Both	X

SVR-26	The VR system shall: a. Use internal system clocks to generate time stamps for audit records, including time generated by an NTP server. b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and are accurate to within 30 seconds.	Both	
SVR-27	The VR system shall protect audit information and audit tools from unauthorized access, modification, and deletion.	Both	X
SVR-28	The VR system shall: a. Support the backup 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.	Both	
SVR-29	The VR system shall support a failover feature to be configured in such a manner as to automatically replicate and securely encrypt a copy of the data at any time. The saved or imported data will be sufficient to restore another VR system in the event of a malfunction.	Both	
SVR-30	The VR system shall be able to recover from the following events: a non-catastrophic failure of a VR system, a power failure, or from any error or malfunction. Recovery from a non-catastrophic failure will mean the restoration of the VR system to the operating condition existing prior to the error or failure, without loss or corruption of data previously stored on the device.	Both	
SVR-31	The VR system shall: a. Conduct automatic backups of user- and system-level information contained in the VR system, in a configurable frequency. b. Protect the confidentiality, integrity, and availability of backup information	Both	X
SVR-32	Vendor shall provide documentation on how its 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 SDLC activities.	Both	X
SVR-33	Vendor shall describe how it employs best practices and methodologies for protecting against supply chain threats to the VR system and its system components. The vendor shall indicate whether any components of the VR system 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. Further, third-party components and dependencies should be provided in a list, including how those components are kept current	Both	X
SVR-34	Vendor shall provide, for any cloud-hosted components, proof that those components have achieved Low, Moderate or High FedRAMP compliance and are hosted by a FedRAMP authorized cloud service provider. Vendor shall provide proof of FedRAMP compliance, as well as documentation of who is responsible for each required security control. These shall be subject to bi-annual review and/or attestation.	Cloud	X
SVR-35	Vendor shall describe what capabilities the VR system has to detect, alert, log, and/or prevent any suspicious software behavior in any part of the VR system.	Both	X
SVR-36	Vendor shall provide documentation and testing results showing that the VR system solution does not exhibit vulnerabilities and weaknesses from sources such as Open Web Application Security Project (OWASP), the Common Weakness Enumeration (CWE) and Common Vulnerability Exposure (CVE). System upgrades shall be subject to the same requirement.	Both	X
SVR-37	Vendor shall provide all documentation needed to identify the full system configuration submitted for evaluation and to develop an appropriate test plan for conducting system testing, collectively referred to as the Technical Data Package (TDP). Minimum TDP documentation: system configuration overview, system functionality description, system hardware specifications, software design and specifications, system maintenance, system test and verification specifications, system security specifications, user/system operations procedures, system maintenance procedures, personnel deployment and training requirements (including security awareness training), configuration management plan, quality assurance program, and system change notes.	Both	X
SVR-38	Vendor shall provide documentation from other election jurisdictions (other states) that have: a. Certified/approved/authorized the proposed VR system. b. Denied certification/approval/authorization of the proposed VR system. c. Withdrawn certification/approval/authorization of the proposed VR system.	Both	X
SVR-39	Vendor documentation shall include recommendations for protecting all VR systems from electrical damage related to power surges, brownouts, lightning, and other transient current and voltage spikes.	Both	X
SVR-40	Vendor shall describe the encryption method and other security measures in place to protect data if the proposed system involves the internet- or cloud-based transmission of data to and from local VR system components.	Both	X
SVR-41	Vendor shall describe recommended or included internet intrusion detection/intrusion prevention and control protocols for any part of the system that involves network connections.	Both	X
SVR-42	Vendor shall provide documentation on a system's nonfunctional qualities, including but not limited to accessibility, performance, availability, reliability, safety, security, usability and auditability	Both	X
SVR-43	Vendor shall describe the security controls used in the development of the system. Such controls include code management to ensure that 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.	Both	X
SVR-44	All VR system data shall remain in the Continental United States (CONUS). Any VR system data stored—including backups—or acted upon must be located solely in data centers in CONUS. Services that directly or indirectly access VR system data shall only be performed from locations within CONUS. Vendor shall provide proof of compliance.	Both	X
SVR-45	Vendor shall provide "User Guide" documentation for each user role that specifies how each user can use the system in a secure and functional manner.	Both	X
SVR-46	Vendor shall describe all recommended controls, processes, and procedures, relevant to the VR system, available to a county BOE to assist them in developing: a. Policy and supporting procedures to facilitate the implementation of security and privacy awareness training. b. Associated security and privacy awareness and training controls	Both	X
SVR-47	Vendor shall describe, when cryptography is required and used within the VR system, the capabilities of the VR system to establish and manage cryptographic keys, including but not limited to key generation, distribution, storage, access, recovery method, and destruction.	Both	X
SVR-48	Vendor shall describe, when cryptographic mechanisms are used, how 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 Level 1 or Level 2, in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards. The vendor shall provide the certificate number. When Cryptographic Module Validation Program (CMVP) validated modules are not used, vendor shall describe details of the encryption that is used, in a manner sufficient to determine how closely the solution	Both	X

SVR-49	The VR system shall support non-repudiation and protection against an individual (or process acting on behalf of an individual) falsely denying having performed a particular action.	Both	
SVR-50	The VR system shall encrypt all data at rest and in transit using FIPS 140-2 Level 1 or Level 2 validated modules compliant encryption. For data in transit, only secure protocols shall be used (e.g., TLS, IPSEC, HTTPS, SFTP).	Both	
SVR-51	The VR System shall use cryptographic hashing and storage for all system credentials.	Both	
SVR-52	Vendor shall describe how it protects and controls digital (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 Level 2), and/or tamper evident packaging.	Both	X
SVR-53	Vendor shall provide the results and supporting documentation related to any third-party or internal testing performed on the VR system. 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 document how any vulnerabilities were mitigated and any that are outstanding.	Both	X
SVR-54	The VR system shall uniquely identify and authenticate defined types of devices that require authentication mechanisms before establishing a connection and that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access.	Cloud	
SVR-55	All VR system data in transit shall remain in CONUS and shall be encrypted in accordance with requirement #S-55 below. Vendor shall provide proof of compliance.	Both	X
SVR-56	Vendor shall describe, for hosted solution offerings, how their incident response plan documentation aligns with NIST SP 800-61.	Both	X
SVR-57	Vendor shall describe how any file to be used within the VR system (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 VR system. Vendor shall describe if its solution achieves this in compliance with Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard.	Both	X
SVR-58	The VR system shall be protected against malware. The vendor shall provide documentation of controls within the system and procedural recommendations relevant to this.	Both	X
SVR-59	Vendor shall describe and notify CBOE/CIT of how it: a. Identifies, reports, and corrects VR system flaws. b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. c. Installs security-relevant software and firmware updates as required. d. Incorporates flaw remediation into the organizational configuration management process	Both	X
SVR-60	Vendor shall describe how remote system administration, software package deployment and system updates are done securely (e.g., secure protocols such as TLS, IPSEC) and require MFA for all remote and administrative access.	Both	X
SVR-61	Vendor shall describe how its VR system solution verifies the integrity of the code base and future software updates (hashing algorithms, digital signatures, etc.).	Both	X
SVR-62	Vendor shall provide, for any cloud-hosted or on-premises components, evidence of any third-party validation of security controls or assessments that have been completed.	Both	X
SVR-63	Vendor shall provide a detailed list of system error messages one might see while using the VR system, definitions of what the messages mean, and actions that shall be taken to address each error.	Both	X
SVR-64	Vendor shall describe how redundancy is built into the VR system to minimize risk of failure or data loss and to ensure high availability.	Both	X
SVR-65	Vendor shall document how the VR system protects the integrity and confidentiality of transmitted information.	Both	X
SVR-66	Vendor shall describe how, if used, public key certificates are issued under an appropriate certificate policy or how public key certificates are obtained from an approved service provider, including certificate renewal.	Both	X
SVR-67	Vendor shall describe how—should the VR system fail from a known secure state—it will preserve the maximum amount of system state information.	Both	X
SVR-68	Vendor shall produce security patches within the service-level agreement (SLA) timelines and shall provide instructions on how to keep their solution up to date.	On-prem	X
SVR-69	Vendor shall describe how software and devices meet the least functionality principle and disable unneeded services such as telnet, SNMP, remote administration (Web Mode), etc.	Both	X
SVR-70	Vendor shall develop, document, and maintain the baseline configuration of the VR system hardware and software components. The vendor documentation shall describe all maintenance activities that are necessary to ensure that the VR system remains in the desired configuration and functioning in a secure manner. This baseline configuration and maintenance procedures document shall clearly identify the software versions that must be in place to maintain the baseline configuration.	Both	X
SVR-71	Vendor shall provide documentation on how the VR 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). Vendor shall also name all standards used and to which component they apply (e.g., servers, mobile devices, wireless). For on-prem or cloud equipment provided by the county, vendor must provide hardening instructions	Both	X