Board of
Voting Systems Examiners
(BVSE)

Ohio **Voter Registration System** Requirements Matrix

Adopted September 17, 2025

TABLE OF CONTENTS

SYSTEM BEING EVALUATED

Vendor: _____

Testing Laboratory: _____

Model: _____

Version: _____

EXAMINATION INFORMATION

Date: _____

Examiner Name: _____

Examiner Signature: _____

For use by the Board of Voting Systems Examiners' examination of Voter Registration Systems submitted for approval and certification in Ohio elections.

For purposes of this matrix, the "acceptable" rating means the voting equipment satisfies the certification requirements established by Chapter 3506 of the Ohio Revised Code and Rule 111:3-9-08 of the Ohio Administrative Code. "Not acceptable" means the Voter Registration System does not meet the requirement.

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
VOTER REGISTRATION FUNCTIONALITY REQUIREMENTS **SECRETARY OF STATE SWVRD, DATA ACT, REPORTING, AND SIGNATURE REQUIREMENTS**			
1. The Voter Registration System (VRS) shall possess the capability to capture and securely store voter registration information, communicate effectively with the state database, and generate reports on voter registration data in compliance with the DATA Act. This capability shall be validated through a successful integration test with the State-Wide Voter Registration Database (SWVRD) FXS system. Such testing must be performed for each software version submitted for certification, demonstrating seamless data exchange, and adherence to established protocols.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
2. The VRS shall have the capability to generate daily point-in-time snapshots of the voter registration database in accordance with the format and data guidelines outlined in the Daily Snapshot File and Data Requirements of current Secretary of State directives and Ohio law.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
3. The VRS shall have the functionality of generating voter lists for the National Change of Address (NCOA) and Supplemental processes consistent with Ohio law that contain at least state ID, and voter first and last names.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
4. The system shall have the functionality of creating a report containing a signature from the county voter registration system and SWVRD.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
5. The VRS shall have the functionality of storing voters' signatures, accepting signatures from the State-Wide Voter Registration Database through the Offline System/Track missing signatures of voters.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
6. The system shall have the functionality of generating a report to compare potential out-of-county duplicate voters. The report shall provide the following available matching criteria from the SWVRD for each voter listed: a. The Ohio Bureau of Motor Vehicles (BMV) number, last four digits of a Social Security number, first name, middle initial, last name, and birthday. b. The last activity date and activity type from the Secretary of State for each jurisdiction, for each voter listed. c. The Ohio voter ID and County voter ID for each county, for each voter listed.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
7. The VRS shall have the functionality of: a. Generating a list of all registered voters by county, precinct, or polling location with a designation for all voters who have already voted in an election. b. Generating a street segment list for all street segments in a county-by-county, precinct, or polling location. c. Generating a report for all voter records not containing a signature.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
8. The VRS shall have the functionality of handling the entry, processing, and disbursement of voter registration data and information to all voters, poll workers, and election administrators within the jurisdiction in which it will be utilized. This must include: a. Voter registration requests. b. Voter registration records. c. Absentee ballot requests. d. Voter history information. e. Voter list maintenance data.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
9. The VRS shall have the functionality of: a. Processing of Data Entry and generation of associated proofing reports. b. Daily processing of online voter registrations and associated report (Online Details Report for in-county voters that move and for incoming voters from outside the county). c. Require notation for confidential voters d. Tracking codes, including Counter, Mail, Online, Reg. Drive, County, etc.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
10. The VRS shall be able to produce reports regarding various election and absentee activities that occur within the system, in a machine-readable, commonly available, and well-known format. This will include the VRS produced reports reflecting the totals and voters for all trackable codes required under the DATA Act.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
11. The VRS shall have the functionality of complying with all DATA Act reporting requirements, including: a. Post-Election applications of Voter History processes (Absentee, Provisionals, and Election Day, as well as application of records in the Voter Hold and Online Modules). b. The ability to set registration and receive dates on voter updates made during the Voter Hold period. c. Clean up reporting as reported by the Secretary of State from the Audit Dashboard (BMV issues, State and Territorial Exchange of Vital Events issues, Date of Birth issues, reg. date issues). d. Voter and absentee snapshots uploaded automatically.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
ADDING AND UPDATING VOTER REGISTRATION APPLICATIONS			
12. The VRS shall have the functionality of processing new voter registration applications. This shall include applications submitted by paper or electronic delivery, and shall be able to process the following information: a. Voter Name (first, last, and MI). b. Former Name Field. c. Suffix. d. Voter Date of Birth. e. Will the voter be at least 18 years of age on or before the next general election? f. Voter Citizenship Status. g. Voter ID (If applicable). h. Voter Address. i. Additional Address. j. Last 4 Digits of a Social Security number. k. Bureau of Motor Vehicles number. l. Voter Signature.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
13. The VRS shall have the functionality of updating existing voter registration records with new information, such as: a. Name changes. b. Address changes. c. Signature changes. d. Political party changes (if applicable).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
DUPLICATE PROCESSING			
14. Upon adding or updating a record, the system shall have the capability to: a. Detect an existing record in the jurisdiction based on existing matching criteria. b. Allow a voter record to be edited without creating voter-initiated activity. c. Keep the County ID number when voters are moving out of the jurisdiction and returning as a new voter, so the history of the voter continues and creates duplicate voters (Active and Deleted).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
15. The system shall have the functionality of allowing a voter record to be edited without creating voter-initiated activity.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
16. The system shall require the county with the oldest voter-initiated activity date to initiate a packet before the county with the most recent voter-initiated activity date.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
CHANGING VOTER STATUS AND DATA DISPLAY			
17. The VRS shall have the functionality of changing a voter status, which can include: a. Active status. b. Inactive status. c. Pending status. d. Canceled status.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
18. The VRS shall have the functionality of displaying voter registration records and the history of said records for use by an election administrator, including: a. Voters (Active, 17-year-old, Federal Post Card Application (FPCA), Confirmation, Deleted). b. Attorney-in-Fact. c. Felons. d. Provisional Only Voter. e. Geo-Political (Address-Street segments/Precincts and Districts). f. Ability to link Precinct to Polling Location. g. Process party affiliation resets in accordance with Ohio law. h. Voting History. i. Registration Voter Counts (by status and party). j. Petitions. k. Precinct Election Officials.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
19. The VRS shall have the functionality of looking up a voter by various voter data points, including: a. Name, b. Date of birth, c. Address, or d. Voter ID number.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
BACKING UP, RESTORING, IMPORTING, AND EXPORTING VOTER REGISTRATION RECORDS			
20. The VRS shall have the ability to export voter registration records in a machine-readable, commonly available, and well-known format. The VRS shall be able to restore the records using the exported data.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
21. The VRS shall have the capability to export voter data in a machine-readable, common data format for import into electronic pollbooks.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
22. The VR System shall have the capability to import voter participation data in a machine readable, common data format exported from electronic pollbooks.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
23. The system shall have the capability to export a list of voters that can be used to create a paper pollbook.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
24. The system shall have the ability to import voter data in a common data format to flag voters identified by the Secretary of State for the purpose of list maintenance.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
ABSENTEE REQUESTS			
25. The VRS shall enable users to process new absentee requests by processing the following absentee data: a. First and Last name of Absentee Voter. b. Absentee Voter Address. c. Absentee Voter Date of Birth (DOB). d. Absentee Voter ID (if applicable). e. Absentee Voter party selection (if applicable). f. Absentee Voter reason for ballot request (if applicable). g. Alternate mailing address. h. Major and Minor party selection by candidate for election, and information for offices and candidates regarding special elections within a specific jurisdiction.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
26. The VRS shall enable users to update current absentee requests with various statuses within the absentee process. This includes: a. Active. b. Inactive. c. Unsent. d. Sent. e. Pending. f. Accepted. g. Rejected. h. Cured. i. Cure Needed. j. Any other absentee status required under Ohio law and regulations.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
27. The VRS shall enable users to display absentee records and history for voters for use by an election administrator.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
28. The VRS shall be able to record and display various data points related to current and past elections occurring within the jurisdiction the VRS operates within. These can include: a. Name and type of the election: 1) Primary 2) General 3) Municipal 4) Special, or Referendums b. Date of the election: 1) Day 2) Month 3) Year c. Appropriate office and office parameters for offices up for election and from past elections. d. Candidates for current and past elections.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
PETITIONS			
29. The VRS shall have the functionality of: a. Petition Verification and the generation of associated reports. b. Tracking Circulator Information. c. Allowing parameters regarding the specific petition. d. Process linked duplicates (a voter can only sign a limited number of petitions for an office). e. Generating parts and line-by-line reports of those who signed; generate related statistics.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
PROVISIONAL DATA			
30. The VRS shall have the functionality of: a. Processing of provisional data and generation of associated reports. b. Standardizing codes for tracking and reporting. c. Interacting with the VR (Voters and GIS).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
ELECTION WORKERS			
31. The VRS shall have the functionality of: a. Assigning election workers to a specific precinct and job assignment. b. Confirming a voter has not been convicted of a felony. c. Linking voters' profiles from Voter Registration (VR) to the Filing Information System (FIS). d. Nominating winners from a primary election to a general election.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
MISCELLANEOUS			
32. The VRS shall require vendors to specify the requirements of data storage for physical/onsite or cloud-based systems.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
33. The VRS shall demonstrate interoperability with certified ballots on demand voting systems, voting systems, and electronic pollbooks.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
34. The VRS shall have the capability to: a. Track all notices sent/received. b. Track undeliverable mail as required. c. Document the processing, indexing, and attaching to the voter record.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
CYBERSECURITY REQUIREMENTS SYSTEM OVERVIEW			
35. The Voter Registration System has been tested by an Election Assistance Commission (EAC) accredited Voting System Test Laboratory (VSTL), and it exceeds the minimum requirements established for use in Ohio.	☐ Acceptable/Yes ☐Unacceptable/No	☐ Yes ☐ No ☐ N/A	
36. The VRS shall provide the capability to configure a warning banner upon logging into the system.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
37. If the VRS is hosted outside of the board of elections data center, it shall be located in the United States at a data center that is SOC 2 Type 2 certified. If a commercial datacenter vendor provides hosting, the system shall be in their US government community cloud.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
38. The vendor shall provide a software bill of materials (SBOM) and dependencies in SPDX, CycloneDX, or other common machine-readable format.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
39. If the VRS is a cloud service, the vendor shall provide a secure communication channel between the customer's on-premise environment and the cloud using contemporary, secure, and authenticated protocols, such as IPSEC.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
40. The VRS shall require all vendors and board of elections employees to use multifactor authentication for logging into the voter registration system. Multifactor authentication shall not be permitted to be disabled.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
CONFIGURATION AND ACCESS MANAGEMENT			
41. The VRS shall employ the principle of least privilege for each permitted role within the system, allowing authorized access only for users (or processes acting on behalf of users) who are necessary to accomplish assigned tasks. Vendor shall document how the VRS role-based access controls accomplish this.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
42. Vendor shall describe what configuration item changes can be made by authorized individuals through the system-defined administration role(s).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
43. Vendor shall describe the capabilities of the VRS related to automated timeout of inactive sessions.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
44. The voter registration system shall have a configurable automated timeout for inactive sessions. This timeout setting can be no longer than 30 minutes of inactivity and cannot be disabled.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
45. Vendor is required to demonstrate that the VRS monitors and supports: a. The ability to define groups and role-based access. b. The ability to create, enable, modify, disable, and archive VRS user accounts. c. The ability to log and audit the use of VRS user accounts. d. Vendor shall provide information about the VRS ability to integrate with a board's identity provider (e.g. Entra ID, Ping).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
46. The VRS shall: a. Enforce a configurable one to five 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
47. The VRS shall have the ability to issue a unique user ID and password to each user.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
48. The VRS shall adhere to password requirements (e.g., password length, password aging, password complexity, etc.) based on NIST standards.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
49. For vendor-hosted or cloud-hosted VRS Systems all VRS data shall remain in the Continental United States (CONUS). Any VRS data stored—including backups—or acted upon must be located solely in data centers in CONUS.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
50. For vendor-hosted or cloud-hosted VRS Systems, as part of the TDP package, document where the systems are being hosted. This shall include the name of the hosting provider, the region of the country in which the data is being hosted.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
51. For vendor-hosted or cloud-hosted VRS Systems, the environment must be dedicated for use by the county. Describe how each county will be hosted in a dedicated hosted environment.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
52. Vendor shall describe how remote support functions such as system administration, software package deployment, and system updates are done securely.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
53. The vendor shall provide local area network (LAN) and wide area network (WAN) connectivity requirements based on the principle of least privilege.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
54. 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
55. Vendor shall describe how the software meets the least functionality principle and disables unneeded services such as telnet, SNMP, and remote administration (Web Mode).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
56. Vendor shall develop, document, and maintain the baseline configuration of the VRS hardware and software components. The vendor documentation shall describe all maintenance activities that are necessary to ensure that the VRS remains in the desired configuration and functions 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
57. Vendor shall provide documentation on how the VRS 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 resources provided by the board of elections, vendor shall provide hardening instructions.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
HARDWARE AND SOFTWARE DOCUMENTATION			
58. Vendor shall 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: a. End-of-life software and/or hardware. b. Unsupported or unpatched software. c. Known vulnerabilities and exposures. Additionally, vendor shall notify the BVSE within 24 months of software component manufacturer's product life cycle end date and must submit a plan within three months of such notification on how to address the affected technology.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
59. 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, including, but not limited to, integrity of the code base. b. Identifies individuals having information system security roles and responsibilities. c. Integrates the organizational information security risk management process into SDLC activities.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
60. 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 VRS 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
61. The vendor shall undergo a cybersecurity maturity assessment of the vendor's software development and cybersecurity practices to provide assurances that these practices are matching the requirements of this matrix and Secretary of State security directives. A copy of the report and remediations steps taken shall be included in the examination.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
62. 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, minimum required hardware specifications, recommended 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
63. Vendor shall provide documentation from other election jurisdictions that have: a. Certified, approved, and/or authorized the proposed VRS. b. Denied certification, approval, and/or authorization of the proposed VRS. c. Withdrawn certification, approval, and/or authorization of the proposed VRS.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
64. 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, quality assurance processes during the development cycle, and any security testing standards.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
65. Vendor shall describe the adoption of a published secure coding standard (e.g., OWASP).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
66. Vendor shall describe their secure coding policy and provide a copy of the policy as part of the technical data package.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
67. Vendor shall describe their code review practices, specifically addressing automated code scanning, the use of AI-generated code, review of AI-generated code and validation, along with manual code review for security. Please provide a copy of this policy and process as part of the technical data package.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
68. Vendor shall describe, as part of their secure by design processes, how the VRS code is immune to some of the most common coding vulnerabilities, including those in the OWASP top ten.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
69. 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
70. Vendor shall describe all recommended security controls, processes, and procedures, relevant to the VRS. This shall include a crosswalk between the Secretary of State Technical Security requirements, including the Vendor Management Security Supplement as described in Directive 2022-38.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
71. Vendor shall describe, for vendor or cloud-hosted systems, how their incident response plan aligns with NIST SP 800-61.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
72. For cloud or vendor-hosted systems, provide the most recent audit report (within 18 months of the date of submission) that evaluates its controls against an established set of trust principles (security, availability, integrity, confidentiality, and privacy). A cloud or vendor-provided SOC 2 Type 2 report will support this requirement, but other documentation may be provided.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
73. Vendor shall provide a shared responsibility matrix documenting which cybersecurity controls are managed by the provider/vendor, and which cybersecurity controls are managed by the county. This matrix shall cover, at a minimum, the following domains (physical security, network and infrastructure security, platform services security, storage encryption, identity and access management, application code, data handling, monitoring, and incident response).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
74. Vendor shall provide evidence of any third-party validation of security controls or assessments that have been completed.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
75. Vendor shall provide a list of system error messages one might see while using the VRS, definitions of what the messages mean, and actions that shall be taken to address each error.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
76. Vendor shall provide a system overview and functional diagram of the entire VRS and how each component integrates into it. The description shall include how the system is administered, configured, and managed.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
77. 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
78. Vendor shall provide documentation on how they are addressing the Secure by Design standards as described by the CISA Secure By Design initiative, specifically addressing each one of the principles outlined in the initiative.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
79. 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 documentation shall clearly indicate the use of AI for creating documentation and how quality control of any AI-generated content is maintained. This shall include the data format(s) the system can import and export.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
80. Vendor shall describe recommended or included network intrusion detection/prevention and control protocols for any part of the system that involves network connections.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
81. Vendor shall provide documentation on a system's nonfunctional qualities, including but not limited to accessibility, performance, availability, reliability, security, usability, and auditability.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
82. The VRS shall demonstrate interoperability with the Statewide Voter Registration Database by passing the most recent validation testing procedures administered by the Secretary of State's office.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
LOGGING			
83. Vendor shall provide a listing and description of what messages and events generated by the VRS become part of the audit record.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
84. The VRS shall record at a minimum, date- and time-stamped events, including but not limited to: a. All user-related events. b. All system administration events. c. Voter registration records events. d. Authentication events.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
85. The VRS shall log to an immutable logging system outside of the VRS. Describe how the logging for items listed above will be stored, and how those records will be kept separately, in an immutable format for a minimum of 180 days.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
86. The VRS shall support the generation of alerts to responsible staff (by role) when a log processing error occurs (e.g., lack of storage space, logging stops unexpectedly). Vendor shall describe what alerting thresholds are configurable and what alerting methods can be used (e.g., email, text, phone call).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
87. The VRS shall manage and allocate audit record storage capacity to reduce the likelihood of such capacity being exceeded.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
88. The VRS shall provide the capability to review and analyze VRS audit records regularly for indications of unauthorized activity. The VRS 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 (e.g., email, text, phone call) if any activity described is identified.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
89. The VRS shall record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC).	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
90. The VRS shall protect audit information and audit tools from unauthorized access, modification, and deletion.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
DATA SECURITY			
91. The VRS shall be able to recover from the following events: a non-catastrophic failure of a VRS, a power failure, or from any error or malfunction. Recovery from a non-catastrophic failure will mean the restoration of the VRS to the operating condition existing prior to the error or failure, without loss or corruption of data previously stored on the device.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
92. Vendor shall describe, when cryptography is required and used within the VRS, the capabilities of the VRS to establish and manage cryptographic keys, including but not limited to key generation, distribution, storage, access, recovery method, and destruction.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
93. Vendor shall describe, when cryptographic mechanisms are used, how the encryption products used have been validated under the Cryptographic Module Validation Program (see www.nccoe.nist.gov/automation-nist-cryptographic-module-validation-program), to confirm compliance with FIPS 140-3 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 adheres to the principles espoused in the CMVP.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
94. The VRS shall encrypt all data at rest and in transit using FIPS 140-2 Level 3 validated modules compliant encryption. For data in transit, only secure protocols shall be used (e.g., TLS, IPSEC, HTTPS, SFTP). Provide as part of your TDP submission confirmation that the modules are compliant. This documentation can be provided from NIST for the modules being utilized.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
95. The VRS shall not have the ability to communicate wirelessly. It shall not contain wireless hardware. Network connectivity, if required, shall use a hard-wired connection.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
96. Vendor shall provide instructions that explain how to verify that wireless functionality is disabled.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
97. The VRS shall use cryptographic hashing and storage for all system credentials.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
98. The VRS shall have the capability to set and modify user permission levels.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
99. Vendor shall document how the VRS protects the integrity and confidentiality of transmitted information.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
VULNERABILITY MANAGEMENT			
100. Vendor shall provide the results and supporting documentation related to any third-party or internal testing performed on the VRS. Supporting documentation shall include, but not be limited to, test plans, test cases, and results from all security testing (e.g., vulnerability, penetration, etc.) that was done on the system. Vendor shall also document how any vulnerabilities were mitigated and any that are outstanding.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

101. For the version being submitted to the BVSE, the Vendor must engage a qualified, independent penetration testing provider that holds industry-recognized certifications such as *CREST* (e.g., CREST Accredited Red Team or CREST Certified Penetration Tester), *ISO/IEC 27001* audit evidence for the testing organization, or *OSCP/OSCE* credentials. The engagement must deliver a full-scope application penetration test covering all externally accessible interfaces of the Voter Registration System, including web services, APIs, authentication flows, and any third-party integrations. The test plan should be based on the latest OWASP Testing Guide (v4) or PTES (Penetration Testing Execution Standard), executed over a minimum two-week period to allow for thorough reconnaissance, exploitation, and post-exploitation analysis. Upon completion, the Vendor must provide a comprehensive report that includes: a. Detailed findings with risk ratings and proof of concept evidence. b. A clear remediation plan specifying actions taken and any outstanding vulnerabilities, with acceptance criteria for each item. c. Evidence of re-testing or verification that mitigations have been effectively applied.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	

REQUIREMENT	ACCEPTABLE/ UNACCEPTABLE	COVERED IN REPORT	QUESTIONS/COMMENTS/EXPLANATIONS
102. Vendor shall describe how it: a. Identifies, reports, and corrects VRS flaws. b. Tests software updates related to flaw remediation for effectiveness and potential side effects before installation. c. Installs security-relevant software updates as required.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
103. 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.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	
104. Vendor shall produce detailed release notes outlining all changes to the system, including any relevant Common Vulnerabilities and Exposures (CVEs) that were remediated as part of this release.	☐ Acceptable/Yes ☐ Unacceptable/No	☐ Yes ☐ No ☐ N/A	