**Table of Contents**

[Appendix B, Part 1: General Information 1](#_Toc499042526)

[Appendix B, Part 2: Voting Machines 9](#_Toc499042527)

[Appendix B, Part 2a: General Election Deployment Data 14](#_Toc499042528)

[Appendix B, Part 3: Electronic Poll Books 14](#_Toc499042529)

[Appendix B, Part 4: Elections Management 23](#_Toc499042530)

[Appendix B, Part 5: Voter Registration 32](#_Toc499042531)

[Appendix B, Part 6: Absentee Voting 64](#_Toc499042532)

[Appendix B, Part 7: DTI Standards 69](#_Toc499042533)

# Appendix B, Part 1: General Information

**Definitions**

1. **Absentee Voting** – the process through which a person who is unable to go to his/her polling place on the day of the election due to a reason specified in the State’s Constitution may cast his/her ballot. These ballots are opened, qualified and counted in accordance with the provisions in Delaware Code, Title 15.
2. **Ballot Building Software** – the software that builds the ballots for one or more voting devices using data provided by the State’s Election Management System.
3. **COTS** - commercial off-the-shelf,
4. **Delaware Election System**– all hardware and software used to register voters and conduct elections by the Department of Elections or in support of federal, state, county, municipal, public school and other elections.
5. **Early Voting** – a defined period before an election when a registered voter may cast his/her ballot.
6. **ED-RD** – the election district name where ED is a number usually between 01 and 19 and RD is a number usually between 01 and 41. The default sort for this data is RD and then ED.
7. **Election District** – a geographic area within a Representative District in which all registered votes are eligible to vote for the same offices. The same as a precinct. Commonly abbreviated ED.
8. **Election Officers** – commonly referred to as poll workers. The people the Department hires to work in polling places on Election Day.
9. **Election Management System** – the software system that holds the necessary data, interacts as necessary with other election system components, and supports all activities necessary to register voters; and to plan, conduct and report the results of an election. This includes but is not limited to registering voters; assigning, hiring and paying poll workers; maintaining and paying polling places; maintaining candidates; maintaining the election structure; maintaining and reporting election results, and providing the information used to build ballots in each of the voting system s used in the State.
10. **Poll Books** - paper or electronic devices used by Election Officers to qualify voters at a polling place or vote center and to record whether the person cast his/her ballot.
11. **Polling place** –a building where one or more election districts vote. It can also refer to the area within a building where one or more elections districts votes.
12. **Representative District** - A geographic area where member of Delaware’s House of Representative lives and represents. Commonly abbreviated RD.
13. **Vote Center** – a physical location where people from various locations within a county may vote. This is typically used at Early Voting sites, but may be used for Election Day voting.
14. **Voter Registration System** – holds the live and historical data of everyone registered to vote in the State. It includes List Maintenance tools to facilitate cancellation of registrations of persons no longer eligible to vote in Delaware; and tools to report information about registered voters in various forms. Absentee voting is a component of the voter registration system and is used to issue and track absentee ballots for an election.
15. **Voting Equipment** – the devices used in a location where a person casts his/her ballot. This includes the devices used to cast and secure the ballot (voting machines) as well as the devices or documents used to qualify a voter and record that a person has voted (poll books whether electronic or paper).
16. **Voting Machine** - the device that a voter uses to cast his/her ballot. Information retrieved from voting machines is used to document and report election results. Voting system – as used in this document, refers to the devices and software enables a person to cast his/her ballot. The voting machines, ballot building software, and results reporting. The machine records and retains an anonymized record of the vote, which may be retrieved and reviewed for audit purposes.

**Overview**

The purpose of this solicitation and any resultant contract is to establish a state-wide solution for voting equipment and an election management system.

The State of Delaware, hereinafter referred to as “the State,” is considering replacing the State’s voting system, election management system with a single, or multi-vendor, integrated voting system allowing for automation and full integration between polling place/early voting site equipment and the absentee, and election management systems. If the project proceeds, the vendor or vendors shall be responsible for complete replacement, installation, training, testing, and maintenance, including bridge maintenance for existing systems, within 8 months. The scope of the project is to include all equipment, training, testing, maintenance of new equipment, and transitioning from the State’s election management system to the new system.

The data storage and management system established through this solicitation may or may not be procured from a vendor also identifying voting equipment as a component of the vendor’s primary product line.

Any contract awarded will be utilized at the State’s discretion dependent on availability of specifically budgeted funds.

Any contracts awarded resultant of this solicitation will be mandatory use for all Covered Agencies with additional availability to municipalities.

It is anticipated that the Department of Elections will be the primary State Agency utilizing the contract resultant of this RFP dependent on availability of funding.

**Background**

Delaware first used Shoup full faced ballot direct recording mechanical lever voting machines in the 1956 elections. Absentee voting at that time was by paper ballot. The county Departments sent voted absentee ballots for each Election District to the Polling Place for the district for Poll Workers to count. The Poll Workers entered the vote totals for each candidate on tally sheets. After the Polls closed, Poll Workers read the totals for each candidate from the back of each voting machine and wrote them onto the tally sheets. We do not know the full history of the process used by the County Departments to collect and report unofficial election results. By 1983, however, Poll Workers reported unofficial results from the Polling Place to the County Departments by telephone. Department staffs compiled the results using calculators and then phoned the results to the State Election Commissioner’s office.1 There were several points of failure in this process that resulted in mistakes that the canvassing authorities would correct.

Delaware began the process of purchasing a new voting system in 1994 or early 1995. The RFP process evaluated several options and resulted in the statewide purchase of the Danaher Controls ELECTronic 1242 full faced ballot Direct Recording Equipment (DRE) machine. The National Association of State Election Directors (NASED) had certified these machines as compliant with the Federal Election Commission’s (FEC) 1990 Voluntary System Standards (VSS).2 The State used these machines for the first time in the 1996 Primary Election and has used them in every election since then. The State continued using paper absentee ballots that Poll Workers counted in the Polling Place. The Danaher machines included the capability for Poll Workers to enter the results of the absentee tally into one of the machines assigned to the Election District. Some Poll Workers had difficulty with the process and at times entered erroneous information that the canvass process corrected. After the Polls closed, Poll Workers took memory cartridges from each of the assigned voting machines in their Election District to zones that read the cartridges and transmitted the results within the State’s firewall to the State’s Election Management System (EMS). The State’s system then uploaded the results to the State’s Web Site. This process greatly sped up the reporting of unofficial results while reducing errors.

The FEC approved updated VSS in May 2002.3 The Help America Vote Act (HAVA) enacted in October 2002 in response to the contentious 2000 General Election. Among other things, HAVA funds to States to upgrade voting equipment, created the United States Election Assistance Commission (EAC), and transferred the responsibility for developing voting system standards from the FEC to the EAC.4

Delaware used HAVA funds to begin the further modernization of the State’s Election System. House Bill 206 with amendments 1 & 2 enacted on July 12, 2005, authorized the Departments of Election to count absentee ballots centrally. The State used another RFP process to purchase central count scanners and absentee ballot preparation software. The winning vendor was Diebold Election Systems.5 Starting with the 2006 elections, the county Departments (now called Offices) uploaded the absentee results to the States EMS shortly after 8 p.m. on Election Night. This further increased the accuracy of unofficial election results.

Concurrently, the State contracted with Danaher Controls to modernize the ELECTronic 1242s to include upgrading the CPU and Power Supply Boards, updating the ballot preparation system, eliminating the Absentee Entry Device, and adding the capability for a person to listen to his/her ballot. NASED certified that the modernized ELECTronic 1242s complied with the 2002 VSS.6

The EAC approved Voluntary Voting System Guidelines (VVSG) 1.0 in December 2005. This was an updated version of the 2002 VSS. VVSG 1.0 that “…significantly increased security requirements for voting systems and expanded access, including opportunities for individuals with disabilities to vote privately and independently.”7 The EAC launched its full testing and certification system in January, 2007.7

The EAC approved VVSG 1.1 on March 31, 2015. The decade-long delay in finalizing this version was because the U. S. Senate did not confirm Commissioners nominated to replace those who had resigned due to uncertainty regarding the future of the EAC. “Version 1.1 provides updates to requirements in the areas of security, reliability, usability, and accessibility. These improvements enhance the testability and clarity of several of the requirements contained in version 1.0 of the VVSG.”8

The EAC is currently testing systems against VVSG 1.0 and VVSG 1.1. The EAC will only test systems submitted for testing after July 6, 2017 against VVSG 1.1.9

Delaware’s voting machines have been durable and very reliable. Unfortunately, Microsoft no longer supports the operating system used in the system that creates the ballots. Delaware’s Department of Technology and Information is also pushing the Department of Elections to move off the State’s mainframe. Additionally, HB 90 currently before the State’s House of Representatives requires the Department to implement Early Voting in 2020 at a minimum of four locations in the State, for at least 10 days before an election ending the Sunday before an election. The Department would need to deploy voting equipment capable of handling Early Voting and Electronic Poll Books in order to effectively manage the election process and prevent those who had voted early from voting on Election Day. The magnitude of these changes suggests that the best solution is to replace the State’s entire Election System – voter registration, election management, and voting equipment (absentee and polling place) as well as procure Electronic Poll Books preferably from a single vendor or from a combination of vendors whose systems “talk” to each other.

The Department of Elections currently uses various systems to conduct elections. It uses the Danaher Controls ELECTronic 1242s for polling place voting along with paper poll lists. It uses Dominion Voting System equipment for both in person and by mail absentee voting. It also uses a Department developed ballot marking system to facilitate ballot delivery and absentee voting by uniformed service members, citizens who reside outside of the United States, and citizens with a disability. The ballot marking system and other tools enabled the County Departments using Emergency Authority in Delaware Code, Title 15, Chapter 55 to provide deployed National Guard and first responders the capability to vote during the aftermath of Hurricane Sandy.

The State developed its voter registration and election management system in the late 1980s. The State implemented the system in 1990. It has undergone many modifications since then.

Delaware’s Superior Court acting as Boards of Canvass in each county certify General and Special Elections using Election District reports from polling places, the absentee system, and provisional ballots to ascertain the true results. The State’s Election Management System provides the tools necessary for Superior Court to compare the results reported on Election night to the results from each voting device, the absentee system and provisional ballot accounting.

House Bill 342 with Senate Amendment 1 enacted on June 28, 2016 established a 12-member Department of Elections Voting Equipment Selection Task Force chaired by the State Election Commissioner. The act designated members because of their State Government position and required House and Senate leaders to appoint four legislators. Due to the change in Administrations that delayed the filling of some positions, the Task Force did not start meeting until after the deadline to submit its report to the Speaker of the House of Representatives and the President Pro Tempore of the Senate. The Act’s synopsis states:

At the recommendation of the Joint Sunset Committee (“Committee”), this Act establishes the Department of Elections Voting Equipment Selection Task Force (“Task Force”). In order to continue its long history of successful election, Delaware must replace its voting equipment by 2018 or 2020. The State Elections Commissioner has started reviewing the numerous options available on the market and requested that the Committee form a task force with legislative representation so that the Commissioner may present 3 to 5 options for purchase or lease. The Task Force’s recommendation is advisory only.10

The Task Force has listened to presentations from vendors who demonstrated various technologies. These include full-faced DRE systems, vote by mail systems, optical/digital scan systems, and electronic poll books. The Task Force has not yet formulated its recommendations.

­­­­­­­­­­­ 1 Personal recollection, Florence Rodgers. She began working at the Department of Elections for New Castle County in 1983.

2 NASED ITA Approved Systems 1-03 to 11-03 (<https://www.nased.org/ITA%20Information/NASEDApprovedSystems1.03.pdf>).

3 CRS Report for Congress, Federal *Voluntary Voting System Guidelines:* Summary and Analysis of Issues, November 5, 2005, p CRS-3.

4 US EAC Web Site, VVSG Fact Sheet (<https://www.eac.gov/voting-equipment/vvsg-fact-sheet/>).

5 Diebold Election Systems changed its name to Premier Election Solutions in 2007. ES&S purchased the company in 2009. In 2010 in response to a Consent Decree, ES&S sold many of the Premier assets to Dominion Voting Systems. (Wikipedia – <https://en.wikipedia.org/wiki/Premier_Election_Solutions>).

6 NASED Qualified Voting Systems 08-14-07 (<https://www.nased.org/NASED%20Qualified%20Voting%20Systems%20FINAL%20rev081407.pdf>).

7 US EAC Web Site, Voluntary Voting System Guidelines (<https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/>).

8 US EAC, 2015 Voluntary Voting System Guidelines, Volume 1, Version 1.1, pg 5.

9 US EAC, Minutes, Public Meeting January 6, 2016, p.10.( <https://www.eac.gov/documents/2016/9/7/1616-eac-public-meeting-minutesdoc/>).

10 HB 342 enacted 28 June 2016 (<http://legis.delaware.gov/json/BillDetail/GetHtmlDocument?fileAttachmentId=48409>).

**Detailed Specifications**

**1. Vendor shall provide the following to ensure strength and viability of the vendor for the duration of the voting system life expectancy:**

1. Financial Statements subject to an independent audit with an unqualified opinion.
2. Five (5) consecutive years of audited financial statements including parent company if any.
3. History of statewide voting system implementation success. The successful vendor shall provide direct history of a minimum of three (3) successfully managed implementations for the main contractor and any subcontractors utilized in the response to this Request for Proposal.
4. Employee Base and Company Size
5. Original equipment manufacturer for any equipment not manufactured by the vendor.
6. Proof of a robust support organization with a nationwide presence.

**2. Vendor or vendors shall provide an integrated voting system that:**

1. Allows for automation and full integration between the State’s polling place equipment, absentee voting system, and election management system.
2. Provides a single-point support system for all aspects of total system.
3. Provides for seamless data exchange between system components.
4. HAVA compliant and must meet all applicable accessibility laws and guidelines.
5. Carries out election processes completely and accurately during the entire system lifecycle
6. Has equipment that is well-built, rugged, easily maintained.
7. Has components that are interoperable and have a data structure with a mechanism that easily exports data in user defined or common data formats (when established by the US EAC).
8. Allows the State to effectively and efficiently audit election results while maintaining secrecy of the ballot.
9. Has strong access controls that authenticates administrators, users, technicians, devices and services before giving access to sensitive functions.
10. Has strong physical security, data protection and software integrity features.
11. Detects, remediates, logs and reports anomalous or malicious behavior.
12. Only exposes physical ports and access points essential to voting operations, testing, and auditing; restricts access to ports based on permissions of the user; and logs all connections to include the identity of the user.
13. Operates on dedicated servers within the State’s network and does not require or permit connection to the internet.
14. Interface with various State financial systems for paying Election Officers and polling places.
15. Generates emails to absentee voters who provide an email address whenever a significant event occurs. This includes receipt of an application, transmitting a blank ballot, receipt of a voted ballot, and whether or not a person’s voted ballot was counted.
16. Integration with other systems, e.g. DMV (for SSN validation, per HAVA), and DELJIS (for Felony checks)

**3. Vendor or vendors shall provide an integrated voting system with demonstrated capability of the following minimum system requirements:**

1. The system must possess the capability to monitor all poll books system-wide on an entire state, county, or local scale, depending upon the jurisdictional boundaries of the election.
2. The system must possess the capability to automatically transmit alerts to selected election administrators or officials when events occur, identified by specific equipment undergoing the event.
3. The system shall be individually marked by unit with integrated identification tags, either sequential numeric or sequential alpha-numeric. Tags shall be configured to indicate ownership by the State. The Vendor shall provide an updated equipment location listing, based upon the integrated identification tags on a daily basis as delivery is implemented.

### Other Requirements:

1. Vendor shall be required to conduct an on-site demonstration of equipment’s capability to provide accommodations for voters with accessibility needs.
2. **Standards and Policies:** The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.
3. **System Logs and Help:**
   1. Must be instrumented to provide monitoring, alerts, notices and information to existing monitoring systems. Additional tools for those areas that require more robust, extensive, and/or interactive monitoring must be included in the Bidder's proposal.
   2. Must provide functionality to allow authorized users to print screen information including application name and screen or function name.
   3. Must provide a comprehensive and context-sensitive electronic help function that can be accessed both from the relevant application function and independently from a help menu.
   4. Must allow an authorized user to access and view help information from an application function without having to exit or close the application function.
   5. The information that the system provides through either the electronic help function menu or in a context-sensitive manner must include field-specific information on required data content and data format as well as general information about each application function and application screen or page.
   6. The system's electronic help function content must be cross-referenced, allowing an authorized user to view and access content on help topics and subtopics that are related to the help topic or subtopic that the user is currently viewing.
   7. Must provide a Help table of contents, multiple (up to 15) index levels, and full text search.
   8. The help index levels, index values, help content and hierarchy of index values and associated help content must be configurable by an authorized administrator for all general, function-specific and field-specific help topics and subtopics.
   9. System functions and features must conform to accessibility standards cited in:
4. Section 508 of the United States Rehabilitation Act: and
5. Web Content Accessibility Guidelines 2.0 (W3C World Wide Web Consortium Recommendation WCAG 2.0 12/2008, Level A & Level AA Success Criteria).
   1. Contractor staff that provide Help Desk and Maintenance and Operations (M&O) support shall use an automated problem-tracking tool to enable staff to record, track, monitor, and report on operational and performance problems (e.g., defects and Deficiencies) detected, prioritized, and resolved during:
6. Pilot and Production operation of the System beginning with Pilot Deployment and Testing and extending through the end of First Year Operations and Close-out; and,
7. Ongoing Production operations and maintenance
   1. The Contractor shall provide and use software tools to scan and monitor the System to ensure that security vulnerabilities are identified and addressed.

**4) Data Conversion:**

1. The contractor is responsible for all aspects of data conversion from the existing system to the new system. The Delaware Department of Elections will be available to provide assistance in data interpretation and participate in testing and evaluation of the results.
2. Based upon the approved recommendation for the phasing of the application, the contractor must develop data-mapping, conversion and migration plan for what files and data are converted and when the conversion will occur. This plan shall include information regarding the synchronizing of data to ensure there is no lost data as the system is phased in. As part of the plan, the contractor must develop a data map that describes each field and/or table in the existing system and how it will be treated by the conversion program.
3. The contractor must provide programs for converting the existing data to the new system. These conversion programs must be functionally tested and pass full regression tests before turning over to the test users for acceptance testing.
4. The contractor is responsible for identifying data anomalies that require “data cleansing” activities and will assist with the needed “data-cleansing”. These “cleansing” activities will ensure that all data is ready for conversion and processing. “Data cleansing” will remain in effect for the length of the agreement.

# Appendix B, Part 2: Voting Machines

**Election Day and early voting machine**

**Current voting machine deployment**

**Polling place voting –** The Department has 1,491 ELECTronic 1242 voting machines. The Department deployed 1,376 machines in 432 Election Districts that were located in 287 buildings for the 2016 General Election. 4,303 poll workers staffed the Election Districts on Election Day. Deployment details by Election District are at Appendix B2a (Voting Machines Deployment). The maximum votes that can be cast on any one voting machine due to equipment limitations is 700. The Delaware Code specifies the following formula for deploying voting machines:

a. In general elections, the polling place for every election district shall be supplied with at least 1 voting machine for every 650 registered voters or majority fraction thereof.

b. In primary and special elections, the polling place for every primary voting district or election district shall be provided with at least 1 voting machine for every 800 registered voters or majority fraction thereof.

Since HAVA the Department has deployed a minimum of 2 voting machines for each Election District except where the number of registered voter is extremely small. Due to current Election Management System limitations, the maximum number of machines that a County Office may deploy in an Election District is five.

Per the Delaware Code, each Election District is normally staffed by an Inspector, two judges, and 2 clerks for each assigned voting machine. The County Offices (or within) the Department may use different terminology for some of their poll workers. They may also assign additional poll workers to serve as greeters or for other reasons.

**Legal requirements -** Delaware Code, Title 15, Chapter 50A

**§ 5001A Requirements.**

(a) Any electronic voting system may be adopted, purchased or used which shall be so constructed as to fulfill the following requirements:

(1) Each voting device shall have a serial number permanently attached to or stamped to the device;

(2) It shall secure to the voter secrecy in the act of voting for or against as many questions as may be submitted;

(3) It shall permit the voter to vote for the candidates of 1 or more parties, or to write in the name or candidate of the voter’s choice for any office;

(4) It shall permit the voter to vote for as many persons for an office as the voter is lawfully entitled to vote for, and the automatic tabulating equipment used in such electronic voting systems shall reject choices recorded on any ballot card or any voting device if the number of such choices exceeds the number to which a voter is entitled;

(5) It shall prevent the voter from voting for the same person more than once for the same office;

(6) It shall permit the voter to vote for or against any question the voter may have the right to vote upon, but no other;

(7) It shall permit each voter in primary elections to vote only for the candidates of the party with which the voter has declared that voter’s own affiliation, and preclude the voter from voting for any candidate seeking nomination by any other political party;

(8) It shall correctly record and accurately count all votes cast for any and all candidates of a political party, and for or against any and all questions, and correctly record the names of all candidates written in by votes;

(9) It shall be provided with means for sealing the vote recording devices to prevent its use and to prevent tampering with ballot labels, both before and after the polls are open or before the operation of the vote recording device for any election is begun and immediately after the polls are closed or after the operation of the vote recording device for an election is completed;

(11) It shall be so equipped that it shall prevent the voter from voting for all the candidates of 1 party by the use of a single mark, punch or other action; however, it shall be provided with a device or method for each party, for voting for all presidential electors of that party by 1 mark, punch or other action.

(b) Every voting device or booth shall be provided with a means of providing sufficient light to enable voters while in the voting booth to read the ballots or ballot labels. All voting devices used in any election shall be provided with side curtains and front shield to insure that no person can see or know for whom any voter has voted or is voting.

**§ 5002A Compliance guarantee.**

Before any electronic voting system is purchased, rented or otherwise acquired, or used, the person owning or manufacturing such voting device must give an adequate guarantee in writing and post a bond accompanied by satisfactory surety with the State Election Commissioner guaranteeing and securing that such voting devices comply fully with the requirements contained in § 5001A of this title and will correctly and accurately record every vote cast and **further guaranteeing such voting device against defects in labor and materials for a period of 5 years from the date of acquisition thereof, or, in the case of rented voting devices, for the period of rental.**

**§ 5005A Printing of ballots; distribution of ballots.**

(a) Ballots shall be printed in black ink on white material of such size as will fit the ballot frame used for all elections and shall be secured in the ballot frame to make tampering or removal difficult. (See D below)

(b) The party emblem which has been duly adopted by such party in accordance with law and the party name or other designation for each political party represented on the voting device shall appear on the ballot if space and layout permits.

(c) Official ballots for voting devices shall be prepared and furnished by the Department in the same manner as provided by law.

(d) Nothing in this section shall preclude the use of an electronic device where the ballot is electronically generated and displayed or which has the capability to generate and display multiple ballots.

**Additional requirements, Delaware Code, Title 15, Chapter 45**

**§ 4502 Form and designation of ballots.**

(a) For each election, the party emblem adopted by each political party and its name shall appear on the ballot with the names of its candidates, arranged in line with the titles of the offices for which they are contesting, along with space for the voter to write in the name of any candidate of that voter's choice, as prescribed in § 5005(b) of this title. In those years in which a President and Vice-President of the United States are to be elected the ballot shall be designated "Presidential, Vice-Presidential, State, County and District Ballot"; in other years the ballot shall be designated "State, County and District Ballot". The names of all candidates of any party shall be placed under the title and device of such party as designated in the certificate filed with the department of elections by such party's authorized agent or agents or, if none is designated, under some suitable title or device to be selected by the department of elections. When a President and Vice-President are to be elected, the names of the candidates for those offices shall be placed at the top of the list of candidates for all offices to be voted upon. The device named and chosen and the lists of candidates of the Democratic Party shall be placed in the first column on the left-hand side of the ballot, of the Republican Party in the second column, and of any other party, and the space for the voter to write in the name of any candidate of that voter's choice for any office, in such order as the department of elections shall decide. The names of unaffiliated candidates shall appear in alphabetical order, under the heading "Unaffiliated Candidates", after the listing of various political parties.

(b) All ballots for the same election shall be of uniform size, of the same quality and color of paper and sufficiently thick that the printing cannot be distinguished from the back. The arrangement of the ballots shall in general conform, as nearly as possible, to the sample ballot set forth in this section.

(c) The ballots prepared in accordance with this chapter shall conform as far as possible to the following design except that the write-in column may be placed on either side of the ballot.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OFFICIAL BALLOT | | | | | | | |
| Presidential, Vice-Presidential, State, County and District Ballot | | | | | | | |
| **WRITE IN** |  | **PARTY EMBLEM** | | **PARTY EMBLEM** | | **PARTY EMBLEM** | |
| **Name of Party** | | **Name of Party** | | **Name of Party** | |
|  | For President | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |
|  | For Vice-President | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |
|  | For United States Senator | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |
|  | For Representative in Congress | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |
|  | For Governor | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |
|  | For Lieutenant Governor | JOHN DOE |  | JOHN DOE |  | JOHN DOE |  |

(d) Absentee ballots may be laid out with candidate names under an office title. If this form is used, party logos shall not be used and the political party of each candidate shall be listed beside or below the name of each candidate. The candidates shall be listed in the order specified in subsection (a) of this section above. Except, that in a primary election the candidates shall be listed in alphabetic order and the political party shall be listed for each office.

(e) If the number of candidates, offices and/or parties to be listed on the ballot preclude the layout of a ballot as specified in this section, the Department of Elections shall obtain approval of the State Election Commissioner to lay out the ballot in a manner best suited to the number of candidates, offices and/or parties eligible to be placed on the ballot.

**Vendor shall provide voting machines for Election Day and early voting that meet or exceed the following requirements:**

a. The US EAC must have certified the voting equipment against VVSG 1.0 standard or higher.

b. Provides all voters the opportunity to privately and independently cast his/her vote.

c. The capability to quickly and accurately build ballots using the State’s standard export from the State’s election management system, e.g. candidates, offices and districts.

d. Shall be scalable – each voting device can handle a minimum of 1,000complex ballot styles for an election, multiple languages, and various election configurations.

e. Voters choices, including write-in votes, shall be reflected on a paper record created by the voter or voting system that a voter with or without disabilities can review before it is cast and that is suitable for a recount.

f. Voting machines used in polling places and early voting sites must be capable of operating in an election district or vote center mode, and report results of each race by election district.

g. Voting machines used in polling places or early voting sites must have a battery capable of operating the device for at least 16 hours, and have a battery that recharges automatically when power is restored to the system. **A system in which the battery requires removing and charging on a separate charging device does not satisfy this requirement.**

h. The voter should be able to activate the voting machines and/or select accessibility features without Election Officer assistance in a manner that results in the display of the correct ballot for the voter.

i. Voting machines that utilizes voter completed paper ballots should possess the capability to determine the intent of voter who does not mark his/her ballot according to the instructions. Further, the system must possess the capability to process normal variations in printing and scanning without requiring adjustment of the mark reading thresholds.

j Voting machines that utilize voter completed paper ballots must possess the capability of processing a ballot with a blank second or back page if no election data flows to the second or back page.

k. Voting machines that utilize voter completed paper ballots shall possess the capability of sorting write-ins, blanks, and over-votes on a high-speed scanning device and reporting write-in votes by race and election district.

l. Voting machines that utilize voter completed paper ballots shall possess the capability of processing ballots up to nineteen (19) inches.

m. Export results by election district, race and candidates onto multiple copies of paper, and onto removable media that can be read by devices at reporting stations and the results securely transmitted to a secure location. This includes the reporting of under votes and over votes (where possible) by race. Transmission must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.

# Appendix B, Part 2a: General Election Deployment Data

****

GSS18809-ELECTION\_SYS

Elections System Solution

# Appendix B, Part 3: Electronic Poll Books

**Minimum Requirements for Electronic Poll Book (EPB) System**

1. **Basic Features**
2. Voter Search and Check-In:
   1. Provide all information necessary to verify voters’ identity.

Note: System shall store answers to these questions as a derived value from a strong key derivation function. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security Standard, and Cryptography Standard.

* 1. Allow for a search based on name, address, or voter ID. Must support predictive text, auto-complete, suggested matches, etc.
  2. Provide capability for the initial lookup step to be limited to just voters in the precinct location where the EPB is located.
  3. EPB shall have the ability to scan various forms of identification for search, e.g. Delaware driver’s license, State ID card, Polling Place Card/Voter ID Card, etc.
  4. EPB shall have the capability of providing the EPB operator with sufficient voter record information for determining a voter’s eligibility to vote, voter status, voted status, absentee status, districts and precinct information, and ballot information, only after the voters identity has been proofed per (a).

1. Usability:
   1. Touch screen capability is required.
   2. EPB shall support user interface customization such as brightness, contrast, text and UI control sizes, User Interface visibility (hide/show, enable/disable), color schemes.
   3. EPB must provide capability to employ the use of hand held devices for voter check in.
   4. EPB shall have the ability to support all DE election types and ballot combinations.
   5. EPB shall comply with all applicable accessibility laws and guidelines.
2. Data Validations:
   1. System must maintain information on voters who have requested absentee ballots, returned absentee ballots, voted by absentee, early voted, etc.
   2. System must identify voters required to show proof of identification or residence.
   3. System shall prohibit the ability for any voter who has participated in one of the elections from participating in any of the other elections held on the same day.
   4. System shall have the ability to display informational prompts and/or warnings based on non-qualifying voter criteria.
   5. Data integrity must be cryptographically protected. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.
3. Voter Registration Data:
   1. Provide a means to capture voter information updates (i.e. completing a voter registration application with electronic signature capture). When Driver License or State ID is used as proof of identification, EPB shall be able to parse the data from the barcode and reduce manual data entry, with the ability for the poll worker to accept or reject the scanned data for each record.

Note: All data must be digitally signed by the inserter and verify that the signing party is authorized on the server side before accepting it (and recording the signature). Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, Key Management Standard, and Electronic Signature Standard.

* 1. Provide a means for updating the Delaware statewide voter registration system.

Note: Must be secure and digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. Support the statewide voter list.
  2. EPB shall support electronic signature capture. Describe how a voter’s electronic signature is captured.

Note: Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, Key Management Standard, and Electronic Signature Standard.

* 1. EPB shall provide polling place information for voters who appear at the wrong polling place and provide a means of directing voters to the correct polling place anywhere in the state, e.g. turn-by-turn directions or generate QR code containing the information.
  2. Ability to capture and store an affidavit (e.g. for non-registered voters during school elections) on the EPB, include capturing of electronic signature.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, Key Management Standard, and Electronic Signature Standard.

1. Data Synchronization:
   1. Where multiple EPBs are deployed at the same voting site, prevent a voter from signing in at different stations.
   2. Be capable of networking multiple EPBs that are located in a single voting location utilizing a secure local area network. Must demonstrate accurate and reliable synchronization between devices so that no voter can vote twice, and no registered voter is denied the opportunity to vote.
   3. Provide a secure means for EPBs to communicate with a central system and vice-versa.

Note: Data must be secured at each level as described in provided security documents. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. If connectivity is available, EPB shall be able to determine if voter has signed in or voted in another location.
  2. Central system shall be capable of supporting more than one election at a time, e.g. simultaneous special elections. The system shall maintain separate unique election records for each election held on the same day.

1. Administration:
   1. Allow for an override of the system if the voter is considered having voted but poll workers know that the voter has not yet voted. Reason for such override shall be captured and logged. The system shall have the ability to require advanced user authentication and authorization to perform the override.
   2. Provide estimates on how long it would take to load an EPB with data.
   3. EPB shall allow for voter history to be quickly and accurately uploaded into the Delaware statewide voter registration system.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. EPB must be able to produce all reports while the election is still underway and after it has closed.
  2. Provide a means for challengers to review checked in voters in real time at every location and from a central location, where connectivity is available.
  3. Allow for review of reports and data from previous elections where EPBs were used.

1. Reporting
   1. Generate interim reports on the screen and printer, i.e. list checked in voters, list of registration updates, etc., without suspending registration operations.
   2. EPB must be capable of providing a list of all validated voters in each respective Election District on an optional EPB printer immediately following the close of the polls on Election Day. Please provide a sample of this list.
   3. Ability to identity double-voting either real-time or post-election.
   4. System must have the ability to conspicuously and automatically display and update the total count of voters checked-in at the precinct. If the EPBs communicate outside of their precinct, then EPB System shall have the ability to prohibit the display and/or combination of poll book counts within any other precinct.
2. Performance, dependability, reliability, availability:
   1. EPBs shall consistently be quick to respond to user actions Example: Search results must be returned quickly or in within reasonable time.
   2. EPB shall redundantly and securely store voter validation data.

Note: Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. Must have sufficient dust, water and drop/shock resistance.
  2. Operate on battery power for up to 16 hours in the case of a power outage.
  3. Shall be capable of automatically switching to a self-contained direct current power source and not interrupt the operation or integrity of the data.
  4. Shall be configured in such a way that the operator is provided indication when the Precinct EPB device(s) is operating on battery power (DC)
  5. Provide a means of quickly recovering data from an EPB that has failed during operation.
  6. EPB shall be able to operate in standalone mode, locally networked (e.g. polling place), and state/public network (e.g. internet).

1. Support, troubleshooting, Survivability:
   1. Provide onsite troubleshooting service on Election Day. Attach current cost figures as well as optional figures to cover day(s) before and after Election Day.
   2. Provide a means to easily deploy security patches for firmware, OS, application, software, etc., to the EPB and its accessories. All electronic devices must be deployed with trusted computing integrity verification in their full stack.

Note: Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. Central system shall have a means to retrieve/report firmware, OS application, software, etc. installed on individual EPBs.
  2. Central system shall have a means to retrieve/report voter registration data version or release date deployed on each device.
  3. EPB accessories, e.g. scanners and printers, must be easily replaceable/serviceable on site with minimal technical experience required.
  4. Hot Swappable: EPB data must be redundantly stored so as not to lose any data, and be able to switch or replace EPB in the event of malfunction. EPBs shall be configured in such a manner to automatically replicate and securely encrypt a copy of the data at all times to a removable/relocatable memory device such as a USB Memory Flash Drive.

Note: A secure key management strategy must be used. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. Hot Introduction: Ability to easily add EPBs into an existing operations, e.g. to support a sudden surge of check-ins, without disrupting ongoing operations.
  2. Scalability: Ability to remove or detach EPBs from an existing operation and transfer devices to another location, i.e. shifting resources based on demand
  3. Ability to generate media required to activate the voting machine.

1. Analytics:
   1. Ability to capture wait times (from clerk 1 searching the voter while in line to clerk 2 searching the voter for check-in)
   2. Ability to captured check-in processing times (from searching the voter during check-in)
   3. Ability to capture stand-by time (times when EPBs are idle)
   4. Ability to generate reports and export raw data captured
2. **Documentation**

As part of this bid, vendors are required to provide formal description and representation of the system, including a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture, and human interaction with these components. The following are required:

1. System Architecture
2. Functional Description
3. User Manuals (System Administrator, Election Administrator, Check-In, etc.)
4. Engineering level Platform Security information (engineering level documentation).
5. Engineering level Cryptographic and Key Management information (engineering level documentation).
6. **Data Transfer, Interfaces and Compatibility**

As part of this bid, vendors are required to provide a means for transfer of data between the Delaware statewide voter registration system and the EPB system. The following are required:

1. The EPB shall provide a simple and timely means of downloading voter and election data from the Delaware statewide voter registration system to the EPB system.
2. The EPB system shall provide a simple means of uploading voter history information to following Election Day to the Delaware statewide voter registration system following Election Day.
3. The EPB shall be compatible and can easily exchange data between EPB and the Delaware statewide voter registration system.
4. **Security**

The system shall provide the following security features:

1. To prevent unauthorized use:

* The EPB system shall provide of record of the following
  + The program and version in use
  + The election file version/release date and time in use
* Describe how security is managed with the EPB including but not limited to:
  + User access control features
  + Data encryption
  + Key Management

Note: Demonstrate compliance to Standards and Policies. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. Be secure from unauthorized access both physical and via wireless against all modern threats.
   1. Compliant with [DoD DISA STIGs](https://iase.disa.mil/stigs/Pages/a-z.aspx)
   2. Does not exhibit common weaknesses enumerated by the [CWE](https://cwe.mitre.org/data/index.html).
   3. D eomization such as brightness,l validation by election officials and an audit trail of determinationsoes not exhibit vulnerabilities enumerated by [OWASP](https://www.owasp.org/index.php/Category:Vulnerability).

Note: Compliant with Standards and Policies. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

1. Shall be configured to ensure controlled, secure logical/administrative access
2. All components shall be configured in such a manner to provide a constant static data encryption methodology that minimally meets Delaware standards and policies, including the security standards and policies provided with this RFP.

Note: Refer to Standards and Policies: The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.

1. Shall be configured and managed in such a manner that all data in-motion maintains the highest level of physical or digital protections per Delaware standards and policies.
2. Shall be configured and managed in such a manner that they may never connect to a publically accessible network
3. Data In-Motion Security: If Precinct EPBs utilize LAN networking connectivity:
   1. All Precinct EPBs must be connected via wired connection (e.g. LAN Ethernet Cable) utilizing a closed and independent switch.  
      -and-
   2. The EPB must support (and require) a VPN connection to a secure location using cryptographic methods in the security and policies provided with this RFP

-or-

* 1. All Precinct EPBs must be connect via a closed wireless non-SSID broadcasting router with encryption methodology employed per Delaware State standards, including and additional filtration scenario to allow only the known Precinct EPB devices the ability to connect to the wireless network.

-and

* 1. The Precinct EPBs shall be configured in such a manner as to only be capable of connecting to the designated wireless networking device.  
     - and -
  2. The EPB must support (and require) a VPN connection to a secure location using cryptographic methods in the security and policies provided with this RFP.

Note: These devices must communicate over a secure layer (e.g. a strong VPN and secure mutual TLS authenticated API connection with good key management). Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

1. Data In-Motion Security: If EPB System and Precinct EPBs utilize WAN networking connectivity:
   1. All Precinct EPBs must be connected via a wireless non-SSID broadcasting router or network with at minimum encryption methodology employed per Delaware State standards (Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information), including an additional filtration scenario to allow only the known Precinct EPB devices within the precinct to connect to the wireless network.

-and

* 1. The EPB System shall be configured in a manner that all data transmission shall only use full tunneling methodology that permits specific routing and approved encryption standards. (VPN)

-and

* 1. The EPB System and Precinct EPBs shall be configured in such a manner that the wireless infrastructure must authenticate each client device prior to access.

-and

* 1. The EPB System and Precinct EPBs shall be configured in such a manner that two-factor authentication is employed.

1. EPBs shall support remote-wipe, local-wipe and have theft prevention and asset recovery features.
2. Ability to detect data tampering

Note: Cryptographically. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. EPB shall have the capability to time stamp most, if not all, activities such as time of voter check in, successful logins, invalid logins, log outs, network connectivity, data transfers, etc. Must have extensive audit logging capabilities.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. Shall be capable of providing accessible and exportable comprehensive audit logs of all transactions to include at minimum, timestamp and transaction/event.
2. Support common and unique user accounts.
3. The EPB system must undergo a security review and assessment by a 3rd party, selected by Department of Elections, and vendor shall provide documentation that all known issues have been addressed and resolved.
4. **Implementation Environment**

As part of this bid, vendors are required to provide separate pricing options for the system to be hosted in the cloud, internally, and hybrid. Regardless of hosting platforms or environments, the vendor solution must comply with the security and policies provided with this RFP.

1. **Accessories and Peripherals**

The Department of Elections may wish the following to be included in the vendor’s base per-unit EPB bid:

1. Electronic Poll Book with barcode scanning and signature capture capabilities
2. Tablet tether
3. Removable memory storage (e.g. Micro-SD Card)
4. Power Banks (battery chargers)
5. 10’ USB power cable
6. Carrying case
7. Stylus
8. EPB software which has been loaded onto EPB
9. Rotating stand for EPB
10. Smart Card Reader/Writer with cable
11. Shipping
12. Acceptance testing

Vendor shall also submit per-unit bids on the following optional equipment:

1. Multi-unit Desktop Charging/Sync Station
2. Thermal Printer with rechargeable battery backup (minimum 8 hours)
3. **Optional Services**

Delaware may wish to enter into an agreement for training, EPB system setup, and election preparation assistance with the winning bidder. Provide current pricing for the following services:

1. Basic training on the EPB system
2. On-site setup of EPB system.
3. Maintenance of the system before, during and after use in elections.
4. Process to upload voter history and other required information to the Delaware statewide voter registration system following an election.
5. Ongoing training for new features.

# Appendix B, Part 4: Elections Management

### Minimum Requirements for Elections Management System

### Note: This section also applies to public school board and referendum elections

1. **Offices and Terms:**
   1. System must provide a central repository of information regarding an elected office for federal, statewide, general assembly (Senate & House), county, municipalities (e.g. City of Wilmington), public school board.
   2. System must have the capability to create and modify office name, jurisdiction type, jurisdictions, terms, base year.
   3. System must allow VP office to be linked to President Office to appear as one ballot choice.
   4. System must have the capability to enter and update the following information about an office
      1. Contact information.
      2. Term of the office
      3. The years that an office is elected
      4. Office filing fee.
      5. Office’s ballot order.
   5. System must provide the capability for flexible, dynamic and overriding office terms.
2. **Candidate Filing:**
   1. System must provide capability to capture the required information for persons who have filed as a candidate for an office, been nominated to run for an office, or have declared themselves a write-in candidate for an office. System must provide real-time updates to candidate and office data ensuring data is synchronized.
   2. System must track changes and history of the changes made to office and candidate records.
   3. System must provide the capability to enter candidate information (e.g. name , address, phone #’s, email, etc.), and upload any supporting documentation
   4. System must provide the capability to pre-populate basic candidate information from the Voter Registration module/system. Note: Candidates for some offices (e.g. school board) are not required to be registered voters.
   5. System must have the capability to capture acceptance or rejection of candidate filings.
   6. System must not allow a candidate to be assigned to an election until the candidate filing has been accepted.
   7. System must allow a candidate to withdraw.
   8. System must provide the capability to verify candidate is a registered voter in jurisdiction of office where required for specific offices.
   9. System must provide the capability to inform other counties of candidate filing (If cross-county office).
   10. System must support offices that have multiple office holders; impacts ballots, declaration of winners.
   11. System must provide the capability to indicate the candidate paid the filing fee or, when appropriate, the candidate filed a supporting petition with signatures.
   12. System must be able to capture the names of the persons who signed the petition. The system must have the capability to verify whether or not the person is registered to vote. Those who are not registered must be flagged as such.
   13. System must provide the capability to verify that the person has only signed the petition once.
   14. The system must be able to count the number of person are valid (e.g. registered to vote in the correct district) and not.
   15. System must enforce deadlines (date and time) and other requirements. Allow authorized staff to override validations, and to capture and store reason(s).
   16. System must provide the capability to publish offices and candidate information to state websites manually or on schedule.
   17. System should allow for export of office and candidate information.
   18. System must allow for county to delete "erroneous" candidates.
3. **Referendums:**
   1. System must maintain a record of Referendums.
   2. System must provide a central location and user-friendly entry mechanism for Referendum
   3. System must provide the capability to enter Referendum text.
   4. System must allow the import and export of Referendum text.
   5. System must support validation requirements for Referendum which may include a super majority for passage (e.g. 60%), or a certain number of ballots cast, or other unique criteria.
   6. System must allow multiple offices and multiple Referendum to be assigned to the same district(s).
   7. System must provide the capability to enter translated text.
   8. System must provide the capability to include or not include a referendum on a ballot.
   9. System must provide opportunity for editing and approval by state or county users before publishing Referendum text.
4. **Elections:**
   1. System must provide the capability to allow submission of candidate and Referendum filing.
   2. System must provide the capability to assign candidate ballot order.
   3. System must provide the capability to import or export election data into ballot production system.
   4. System must provide the capability to calculate ballot styles and ballot types and assign ballot types to voters.
5. **Setup:**
   1. System must provide the capability to setup an election (election date, offices).
   2. All interfaces must leverage strong mutual TLS authentication in compliance with the security standards and policies provided with this RFP.

Note: Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. System must provide programmatic exporting and importing of all election related data. The system must provide programmatic interfaces for data exchange between subsystems and other external vendor systems. Need ability to manually trigger exports and imports as well.
  2. System must provide the capability to import/enter candidates and Referendum and export to ballot production systems.
  3. System must be able to support overlapping elections. The system must allow the user to specify which election they need to work on so that multiple elections can be managed at the same time. Ballots and voters assigned to a specific election shall have a unique ID which is linked to a specific election. A given voter could be in both elections, the voter would have the same voter ID but a unique election ID would be assigned.
  4. System must provide the capability to enter candidate ballot order by guidelines configurable by authorized administrators (e.g. Dems, Reps, Other parties by alpha order).
  5. System must provide the capability to support the maintenance of a county's jurisdiction/representative district/election district data.
  6. System must be capable of producing reports.
  7. System must be capable of producing election management reports including which districts are on which ballot type, ballot type to election district in election district order and sorted by ballot type.
  8. System must provide the capability to calculate Ballot Styles.
  9. System must provide the capability to determine Ballot Types and assign voters.
  10. System must provide the capability to upload ballot styles from the ballot production system.
  11. Public site must consistently and accurately display all elections.

1. **Election Results Reporting:**
   1. System should provide a means of obtaining historical election results by election date readily and easily.
   2. System must provide the capability to upload tabulation file.
   3. System must provide the capability to upload consolidated tabulation system.
   4. System must provide the capability to check for errors.
   5. System must provide the capability to upload/enter/post results in multiple formats to the state’s websites.

Note: Digital signature should be provided. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. System must provide the capability to identify winner.
  2. System must be capable of producing election results and relevant election information for 3rd party organizations, e.g. Associated Press, Voting Information Project. System must support the manual or scheduled programmatic extraction of data in compliance with the security standards and policies provided with this RFP.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard

**Certification and recounts:**

* 1. System must provide the capability to allow state to certify an election.
  2. System must report results by Election District for
     1. Election Day polling places by machine and Election District
     2. Absentee votes cast by voters in an Election District
     3. Provisional votes counted within an Election District
     4. Early voting results by Election District
  3. System must provide the capability to enter and report county and state reconciliation data.
  4. System must provide the capability to record data and report on votes counted, over votes, under votes, etc.
  5. System must provide the capability to allow authorized users to make adjustments to vote counts as a result of Court of Canvass. The changes (before and after), user information, and reason must be logged.
  6. System must provide the capability to generate reports showing the changes and differences between the unofficial election night results against the adjusted post-Court of Canvass results.
  7. System must provide the capability to allow election, official results, and recount results to be locked.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. System must provide the capability to generate certificate of election documents.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. System must provide the capability to publish final results on state websites.

Note: Must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. **Vote Publishing:**
   1. System must publish election results from the entire state or any portion thereof holding an election.
   2. System must include the full reporting of election results.
   3. System must provide the capability to publish result files on state websites.
   4. System must provide the capability to prepare and combine result files for, in and cross-county elections and publish recount results separately.
   5. System must provide the capability to import text, pdf, or csv result files from tabulation systems. Tabulation systems from multiple vendors are/or may be in use.
   6. The system must display results of Referendums along with validation requirements so that a user may determine if the Referendum passed or failed.
2. **Election Officer and Zone Worker Management:**
   1. System must provide the capability to set up class schedule for each specific election.
   2. System must provide the capability to publish class schedule on state websites.
   3. System must provide the capability for potential individuals to apply to be a worker online.
   4. Ability for Election Officers to accept assignment, select class schedule, reschedule class, communicate online, and check payment status.
   5. System must provide the capability to configure custom positions, class size limits, and training requirements.
   6. System must provide the capability to track class vacancies and block the slot when full.
   7. Ability for authorized staff to review, accept, modify and deny applicants.
   8. System must provide the capability to place workers in waitlist, reserve, or on-call status.
   9. Generate assignment letters for applicants/workers that can be personalized by their Department staff with contact and class information, or reason for rejection, re-invitation notice, etc.
   10. Designate positions for each worker.
   11. Ability to input non-voters as workers. These are generally high school students who will become registered voters in the future. When they do register, use existing record to avoid re-entry of data. Also, zone workers for election night reporting do not need to be registered voters or Delaware residents.
   12. Record oath or the ability to upload electronic copies of oath.
   13. Record State of Delaware Dual Employer forms and Zone Worker Bid forms. Ability to upload electronic copies of the form.
   14. Record attendance at training and on Election Day.
   15. Assign county issued cell phone numbers to certain workers when necessary.
   16. Ability to communicate with potential and confirmed workers via text, email, or mail.
   17. Ability to record worker evaluations and recommendations.
   18. Ability to setup pay rate by position and by individual worker for each election.
   19. Ability to set accumulative payment threshold by calendar year or date range. Allow authorized administrators to configure to which positions the threshold shall apply.
   20. Ability to track when workers may exceed payment threshold. Provide visible warnings and prevent poll worker assignment.
   21. Ability to check for “orphan” workers, i.e. not assigned a role or polling place or zone location.
   22. Ability to check for “orphan” polling places or zone locations, i.e. not assigned with workers.
   23. Ability to check for under manned polling places and zone locations, i.e. not assigned with enough workers. Minimum number of workers and roles must be configurable by authorized users.
   24. Ability to generate files necessary for Finance to do payroll. The files shall be securely transmitted to Finance’s file server.
   25. Ability to import payroll result file from finance and update payment status of workers. The files shall be securely transmitted from Finance’s file server.
   26. Ability to manually set status of payment of workers individually or groups of workers at once.

Note: Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Application Security Standard, Web Application Security, Cryptography Standard, and Key Management Standard.

* 1. Ability to store worker working history.
  2. Ability to copy all or select workers from previous elections and assign them new elections.
  3. System should allow for export of worker information.

1. **Location Management**
   1. Ability to add, update and delete election specific locations for early voting Election Day polling locations.
   2. Ability to add, update and delete election specific locations for vote accumulation and transmission, a.k.a. election zones. Provide ability to exclude election zones from getting included in publishing and data export.
   3. Maintain database of all past, current and proposed locations.
   4. System must provide the capability to publish locations by election online. Allow end users to get driving directions.
   5. Ability to copy all or select locations from previous elections and assign them new elections.
   6. Assign election districts to locations.
   7. Support multiple election districts per location.
   8. Store images and accessibility surveys for each location.
   9. Store contact information for each location for delivery and pick up of equipment.
   10. Record serial numbers of equipment sent to each location.

Note: Digitally sign this data. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. Record other equipment to be sent to each location.

Note: Digitally sign this data. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. Automatically generate a Bill of Lading for equipment delivery by third parties.

Note: Digitally sign this data. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. Provide ability to generate files necessary for Finance to pay locations. The files shall be securely transmitted to Finance’s file server.
  2. Support payment of multiple locations to a single account, e.g. payment for multiple schools go to the school district.
  3. Provide ability to import payment result file from finance and update payment status of locations. The files shall be securely transmitted from Finance’s file server.
  4. Provide ability to manually set status of payment of locations individually or groups of locations at once.
  5. Provide ability to scan signed rental agreements and attach to a facility records.
  6. Floor plans and contingency planning information viewable by responders.
  7. System should allow for export location information.
  8. Generate letters for location points of contact that can be personalized by their recruiter, e.g. delivery, pickup, site inspection, connectivity testing, etc.
  9. Sign requirements by type and number for each type.

1. **Voting Information Project**
   1. Ability to create files that comply with Voting Information Project specifications (https://votinginfoproject.org/). Note: At this time 5.1 is the latest version. Refer to <https://votinginfoproject.org/projects/vip-5-specification/>
2. **Data Exchange Policy**
   1. Any Request for Proposal (RFP) and/or Professional Services Agreement that requires a data extract from the Payroll, Human Resources Statewide Technology (PHRST) system must address data classification, protection, integrity and disposal as well as the method of transmission as identified below.

**1. POLICY:**

The PHRST data contained in extract files provided to a vendor is to be used exclusively for the purpose defined in the RFP or Professional Services Agreement. It is not to be used for any other purpose.

**2. CLASSIFICATION OF DATA**

The PHRST data being provided must be classified by PHRST in accordance with the Department of Technology and Information (“DTI”) Data Classification Policy.

b. Data Classification Definitions:

i. State of Delaware Public – Information available to the general public; eligible for public access.

ii. State of Delaware Confidential – Information covered by one or more laws. The disclosure of this information could endanger citizens, corporations, business partners and others. The types of information might be covered under non-disclosure agreements; or safeguarded by a general reference in law or best practices.

iii. State of Delaware Secret – Information that, if divulged, could compromise or endanger the people, or assets of the State; such as Public Safety Information. Data that is specifically protected by law (e.g. HIPAA).

iv. State of Delaware Top Secret – Information that could, if divulged, expose the State’s citizens and assets to great risk.

**3. DEFINITIONS** – PHRST will determine if data being provided to the vendor meets any of the following definitions:

a. Personally Identifiable Information (PII) – Information which can be used to identify or contact a person uniquely and reliably, or can be used with other sources to uniquely identify an individual. Examples include but are not limited to full name, full social security number, full date of birth, street address, telephone number, email address, and fingerprints or other biometric data.

b. Personal Health Information (PHI) – Individually identifiable health information that is maintained or transmitted in any form or medium.

c. Personal Financial Information (PFI) – Individually identifiable financial information that is maintained or transmitted in any form or medium

**4. METHOD OF DATA ACCESS AND TRANSFER**

The file format and method of data exchange must be in accordance with DTI standards. The format and file exchange process must be described in detail; e.g., file placed in folder in PHRST directory on the SFTP server, encrypted file placed on vendor’s SFTP server, etc.

**5. FREQUENCY OF DATA EXCHANGE**

The data exchange frequency must be defined.

**6. RETENTION/LIFECYCLE OF DATA**

Data transmitted pursuant to the awarded contract vendor shall be retained so long as necessary to achieve its intended purpose. The vendor must agree to secure such data until such time as it may be destroyed or deleted. PHRST reserves the right to require a certificate of destruction/deletion.

**7. NON-DISCLOSURE OF DATA**

a. The awarded contract vendor employees or contractors shall not disclose, in whole or in part, the data described in this agreement to any individual or organization not specifically authorized.

b. The awarded contract vendor is required to comply with all applicable confidentiality-related Federal, State and Local laws.

c.  PHRST shall be considered the custodian of the data it provides to the vendor for the purposes of the Delaware Freedom of Information Act, 29 *Del. C.* Ch. 100. All requests pursuant to FOIA for data subject to this agreement in the possession of the vendor must be referred to PHRST. To the extent that the vendor modifies the form or content of data disclosed by PHRST, the vendor shall be considered the custodian of such information for the purposes of the Delaware Freedom of Information Act, 29 *Del. C.* Ch. 100.

**8. DATA BREACH**

Any breach in the security or confidentiality of the data being shared shall be reported immediately to PHRST, to the DTI Security Office, and to the contracting entity’s designated Technology representative or Information Resource Manager (IRM).

**9. BUSINESS ASSOCIATE AGREEMENT**

Prior to release and/or transfer of any data from PHRST to the contract vendor(s), the contracting entity shall execute a Business Associate Agreement (the “BAA) between the contracting entity and the awarded contract vendor. The executed BAA is valid through the life of the contract and any subsequent audit term (5 years or as identified by the State of Delaware contracting entity). If a new Professional Services Agreement is executed, a new BAA must also be executed even if there is no change in vendor

1. **Employee/Location Payment Data Processing**
   1. The file layouts identified below are state required templates established by First State Financials (FSF) for payment vouchers. Vendor proposals are to identify system compliance with providing information compatible with the FSF vouchers.
   2. Payment to Polling Places
      1. DAP001, Vouchers Inbound File Layout
      2. DAP001, Vouchers Log Output File Layout



* 1. Payment to Poll Workers
     1. DAP010, One Time Vendor, Voucher Inbound File Layout
     2. DAP010, One Time Vendor, Voucher Outbound Log File Layout



# Appendix B, Part 5: Voter Registration

**Requirements for Voter Registration System:**

1) **General Requirements & Features:** Pertains to data accessibility, functional applicatioadministration, extensibility, and system access

* 1. The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.
  2. Provide authorized users with read-only access to the data for registered voters within other counties, including historic voter activity data, historic voting participation data, historic affidavit images and historic signature images for registrants.
  3. Provide authorized county users the ability to update the voter registration data for voters within their county.
  4. Prohibit county users from changing data for voters in other counties except to submit a transaction that moves a matched voter from another county into their county.
  5. Automatically send electronic notice to each appropriate county whenever a voter record is added or updated through automatic processes.
  6. Provide the capability for authorized users to search, query and track electronic notices that have been sent to counties. Search, sort, filter and grouping criteria must include county or jurisdiction, notice type, status (resolved or unresolved) and date or date range for notice.
  7. Provide the capability for authorized users to track the source of voter registration applications and to generate report or extract data for reporting purposes, e.g. EAC.
  8. Provide for update and addition of common nicknames, e.g. “Bob” for Robert.
  9. Be able to process voter registration data originating from new sources of voter registration data both internal and external to Department of Elections, with only the addition of a pluggable interface. Note: Department of Elections intends that DHSS-DSS and DOL will be among the potential “new sources” of voter registration data once they are able to plan for and implement a method to provide new voter registration data.
  10. Be able to process voter registration from existing sources. Note: DMV submits registration through their mainframe system as well as self-service kiosks. DMV is in the process of deploying an online drive license and state ID service which is expected to submit voter registrations as well.
  11. Provide extracts of names and addresses for voters in one or more counties for processing by an external service.
  12. System must allow for authorized users to create, edit, and publish changes to webpages in a graphical user interface (GUI) without vendor assistance.
  13. System must allow an incomplete registration to be recorded with an incomplete status, send a verification notice to gather the missing information and deny the registration if missing information is not received in X days. Allow Authorized Administrator to configure X.
  14. System must support Election Day registration, to be used should the State legislature enable Election Day registration.
  15. Where applicable, must support predictive text, auto-complete, suggested matches, etc. to minimize manual entry.
  16. System shall comply with all applicable accessibility laws and guidelines.

1. **Voter Registration - Data:** These requirements list voter registration data elements that must be maintained to comply with HAVA Section 303 requiring that each state implement a “single, uniform, official, centralized, interactive computerized statewide voter registration list.”

Data elements described here include data provided or captured by elections officials’ staff as well as data provided by citizens through online registration via the public access website.

The data elements listed here do not constitute an exhaustive list of required data. Department of Elections expects that during the Design Phase, the Contractor will work with department staff, partner agencies, and vendors to determine all specific data elements necessary to meet all requirements stated in this RFP.

* 1. The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.
  2. Provide functionality that enables authorized users to add new registered voters and to update data associated with existing registered voters.
  3. Be able to capture, store, and display all historical data on every record, including images.
  4. Capture and display all data elements required to support functions and requirements defined in this RFP.
  5. Must allow for capture and storage of voter names including the following discrete data fields:
     1. First name (full or initial);
     2. Middle name (full name or initial);
     3. Full last name (can include hyphenated last name);
     4. Suffix (Sr., Jr., other generations); and
     5. Previous name(s)
  6. Must store a unique identifier (Voter ID) for each registrant.
  7. Must capture and store historic data on voter residence, mailing address, including beginning and ending effective dates of those addresses.
  8. Must provide for capture and storage of addresses (See Voter Registration – Addresses).
  9. Must provide the ability to capture and store a voter’s date of birth. NOTE: Because a voter may have currently effective registrations that predate the requirement to provide date of birth, system must be capable of handling voters without/partial a date of birth.
  10. Must capture affirmation of citizenship status.
  11. Must be capable of capturing and storing the following data that is optional for completion of voter registration:

1. Full Social Security Number
2. Last 4 of Social Security Number
3. Delaware Driver’s License Number
4. Delaware State ID Number
5. Telephone number (up to four different numbers, including type and extension, as separate fields or records);
6. Email address (Must adhere with current internet standards, such as 254 character email addresses).
   1. Must store a voter prior registrations in other states, if any:
   2. State
   3. Full Name
   4. County or Jurisdiction
   5. Voter ID
   6. Residential Address
   7. Mailing Address
   8. Driver License or State ID Number
   9. Must be capable of capturing and storing vote-by mail or absentee voting information. See Voter Registration – Absentee Voting.
   10. Must be capable of capturing and storing a voter’s language preference based on codes that can be defined and modified by authorized Administrators (e.g. [RFC-5646](https://tools.ietf.org/html/rfc5646)).
   11. Must be capable of capturing and storing multiple accessibility/assistance needs for a voter, based on codes that can be defined and modified by authorized Administrators.
   12. Must capture, store and display the status of any voter’s registration, effective dates for such changes and reasons for the change. The status options must include:
7. Active;
8. Inactive;
9. Cancelled/Purged;
10. Pending;
11. Other status (e.g. new registrants during the closed of registration period, under age registrants waiting to be eligible, non-registered election officers)
    1. Must store a voter’s political party preference, based on codes that can be defined and modified by authorized administrators.
    2. Must capture, store and display the following identification information for each voter record:
       1. The voter’s Delaware issued Driver’s License number, if known or provided;
       2. The voter’s Delaware issued State Identification Card number, if known or provided;
       3. The DMV verification status of that number (i.e.., verified, not-verified, or pending verification; and
       4. If verified, the date verified.
    3. Must capture and store the following identification information for each voter record:
12. The 9-digit voter's Social Security Number, if known or provided, which must be accessible for input, query and reporting;
13. The last 4 digits of the voter's Social Security Number (SSN4), if known or provided, which must be accessible for input, query and reporting;
14. The Social Security Administration verification status of that number (verified, not-verified, or pending verification); and
15. If verified, the date verified.
    1. Must capture and store the voter’s current and historical methods of registration (e.g., “by mail,” “walk-in,” “registration drive,” “DMV,” etc.), based on codes that can be defined and modified by authorized Administrators.
    2. Must capture, store and display for voters who register by mail:
16. Whether or not the voter is a first-time voter, subject to the HAVA ID requirement (HAVA Section 303[b]);
17. Whether or not the voter has satisfied the ID requirement and, if so, how; and
18. If exempt from this requirement, the reason for that exemption.
    1. For each voter registration application received, system must capture and store the following discrete data:
    2. Application date;
    3. Date the application was received; and
    4. Effective date of registration for the application; and
    5. The voter registration record that was created or updated based on data in the application.
    6. Must store and display the current and historic images of the full registration applications in a format consistent with either ANSI/AIIM standards or Delaware State standards.
    7. Must store and display the current and historic images of the full registration application with a minimum resolution of three hundred (300) dots per inch (dpi).

Note: Stored data must be digitally signed. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, Key Management Standard, and Document Imaging Standard.

* 1. Must provide the ability to zoom into application and signature images.
  2. Must provide ability to attach🟋 and store🟋 other images to a voter’s record in GIF, TIF, JPG, PNG and PDF formats, such as letters received from the voter. Must allow user to enter comments, and select a category for the image. Categories shall be defined and modified by authorized Administrators.
  3. Must capture🟋, store🟋 and display🟋 an average of fifty (50) free-form text comments and/or notes per voter record with an average size of five hundred (500) characters per comment or note.
  4. Must be scalable to store🟋 an average of one hundred (100) free-form text comments and/or notes per voter record, with an average size per comment or note of one thousand (1,000) characters.
  5. Must allow multiple comments and notes to be stored🟋 for a single registered voter. Each note must have a creation date, and user information associated with it.
  6. Must retain all voter records and associated data, including images for each voter record, such that processes and reports that are generated with an "as of" date correctly reflect the data applicable on the "as of" date.
  7. Must capture and store data🟋 for confidential voters under applicable Delaware laws.
     1. Must allow capability to flag confidential voters.
     2. Must automatically assign non-conventional address (e.g. “Address Withheld”) that are exempt from address validation (e.g. USPS/CASS standard). The non-conventional address will be defined and modified by authorized Administrators.
     3. Must capture and store🟋 the legal basis for which a voter qualifies as confidential (e.g., “court ordered,” “victim of domestic violence,” ) based on user-defined codes that can be defined and modified by authorized Administrators
  8. Must be able to send automated email notification at every step of the application processes, e.g. upon receipt, completed.
  9. Must capture and store a record of list maintenance notices sent to a voter, including the date the extract for mailing label was created or the actual date sent.
  10. Must provide a user interface for authorized Administrators to add and maintain allowable data values for all fields where the set of possible data values is constrained.
  11. Must be able to export voter registration data in compliance with Electronic Registration Information Center (ERIC) data format.
  12. Must be able to import data/reports🟋 from Electronic Registration Information Center (ERIC)
  13. Must be able to import🟋 death data from Delaware Department of Health and Social Services and other authorized state and federal agencies for list maintenance.
  14. Must be able to process voter registration for underage voters (X yr. olds) and automatically activate them once they become eligible. Allow authorized administrator to configure X.
  15. Must be able to process party affiliation changes during a closed period and hold/maintain these changes to be applied automatically when the party change period reopens.
  16. Must be able to process voter registration for new voters during a closed period and automatically activate them once the period opens.
  17. Must be able to import🟋 felon lists from authorized state and federal agencies for list maintenance.
  18. For imported data🟋 for list maintenance:
      1. System must be able to match individual records to existing voters. Search must have confidence match ratings configurable by authorized Administrators.
      2. Facilitate list maintenance with minimum user data entry and manual matching.
      3. For data received in non-electronic format, e.g. paper or scanned copies of paper reports, system must allow for manual data entry.

🟋 Note: Must be digitally signed and/or verified. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. **Voter Registration – Addresses:** These requirements cover addresses.
   1. Must provide for capture and storage of the following discrete data fields related to a voter's address:
2. House number;
3. House fraction number;
4. House number suffix (alphanumeric);
5. Two-character pre-directional code (e.g. S for South., SW for Southwest) \*;
6. Street name (alphanumeric);
7. Street Suffix Abbreviations (e.g. BLVD for BOULEVARD, RD for ROAD, etc.) \*;
8. Two-character post-directional code \*;
9. Unit Type & Number (alphanumeric) \*;
10. City;
11. State\*
12. Zip \*;
13. Zip plus four\* (optional with respect to each voter); and
14. County.

NOTE: \* Must conform to USPS standards

* 1. System must include the capability to standardize residential and mailing addresses against USPS standards.
  2. System must provide a means of overriding address standardizations needed to account for non-traditional residential addresses or non-US mailing addresses. Must be able to capture and store an address in a free-form format as a registered voter's official residence (e.g., the voter's address might be "THREE MILES NORTH OF ACME GROCERY STORE, Alturas, CA" or "Mile Marker 29.5, Hwy 85").
  3. Must provide for capture and storage of multiple mailing addresses for a voter, including permanent mailing addresses, temporary mailing addresses (with beginning and ending effective dates), permanent vote-by-mail addresses, and one-time vote-by-mail addresses.
  4. Must determine whether or not a mailing address is within Delaware based on available data in the mailing address.
  5. Must be able to capture and store a voter’s “Mailing” and “Vote-by-Mail” address using the following fields that can be used with mailing Software:

1. Free-form data entry;
2. Fields long enough to meet US postal, foreign and military mail regulations;
3. Postal codes; and
4. Country code
   1. System must provide the means to identify an address as an “invalid voter address”, e.g. commercial address, private mail boxes, invalid delivery point, etc.
   2. The system must notify the user if a residential address has been identified as an “invalid voter address” and preclude the use of that address as a residential address.
   3. The system must provide for overriding the preclusion of an “invalid voter address” as the residential address of a voter, and capture and store the reason for the override.
   4. The system must provide the capability to remove an “invalid voter address” designation from a voter address.
   5. System must allow for the extraction of addresses.
   6. System must allow for the bulk standardization of addresses.
   7. System must provide a means to export addresses for external validation against CASS certified address standardization software.
   8. System must provide the capability to import and update addresses validated against CASS certified address standardization software.
5. **Voter Registration – Voter Search:** These requirements cover voter registrant searches that will be executed by authorized users or staff.

Users may execute searches to research voter registration issues, resolve list maintenance questions or address other issues.

Requirements listed here include those that are specific to searches that are executed for list maintenance or research purposes, as well as those that are applicable to any search.

* 1. Must allow an authorized user to query and locate an existing record in the system interactively, using any one or a combination of the following criteria:

1. Full or partial first name;
2. Common variances on first name;
3. Full or partial middle name;
4. Full or partial last name;
5. Soundex variations on last name;
6. Full or partial residence address;
7. Full or partial mailing address;
8. Full or partial telephone number;
9. Full or partial Voter ID;
10. Full or partial DL/ID;
11. Full or partial Registration application number;
12. Full or partial SSN4;
13. Full or partial date of birth (DOB)
14. Place of birth;
15. Political party preference;
16. Election District; and
17. Political district.
    1. In response to a search executed for research or list maintenance purposes, system must return all high-confidence matches and all potential matches that exceed the minimum matching threshold (See: Record Matching and Merging).
    2. For any executed search, system must display the following information, at a minimum, for each match:
    3. Full voter name;
    4. Voter ID;
    5. Date of birth;
    6. DL/ID (if available);
    7. SSN4 (if available); and
    8. Residence address
    9. Where they vote
    10. Voter status (e.g. active, inactive, purged to include reason and date, etc.)
    11. For any executed search, system must, upon user choice, display applicable detail for a presented match, including:
18. Historic voter activity data;
19. Historic voting participation data;
20. Historic affidavit/application images and
21. Historic signature images.
    1. For any executed search, system must, upon user choice perform the search
    2. Synchronously; or
    3. Asynchronously. If done asynchronously, provide user a means to know that search has completed.
    4. For any executed search, system must, upon user choice export result to CSV, MS Excel, PDF, MS Word formats.
22. **Voter Registration – Registration Processing:** All voter registration additions and updates from the in-premise Delaware Department of Elections staff will be submitted via this system.

For voter registration transactions, the Delaware Department of Elections staff may optionally begin with a search of records. If the staff executes a search of the database as an initial step, the system will present a single matched record, if available, that meets or exceeds the high-confidence threshold for that search function. The staff may optionally select that matched record for the purpose of pre-populating the data in a new transaction, and then make additions and changes to the data. If the staff does not search for a match, or if the system does not return a single high-confidence match in response to a search, the staff will enter all required data fields for a new transaction.

The process described in these requirements refers to the ID Verification process (which is described in more detail in ID Verification).

* 1. In response to a search that a user executes for purpose of submitting changes to an existing voter registration record, system must display a “match” result only if there is a single match that exceeds the high-confidence threshold.
  2. Must evaluate all submitted registration records against configurable data validation rules, and reject any records that have one or more errors configured as critical severity.
  3. Must provide the capability for authorized users to configure data validations, including adding, modifying, enabling/disabling, and setting severity level.
  4. Must submit registration records that were not rejected for critical severity data validation errors to the ID verification process as described in ID Verification.
  5. If system finds a single, high-confidence match of an existing voter record with the submitted record, system must, upon user choice, update the existing voter registration record with information from the submitted record. (See Record Matching and Merging concerning merge and match requirements.)
  6. If system cannot find a single, high-confidence match of an existing voter registration record with the submitted registration record, system must, upon user choice, create a new record for the voter.
  7. Voter registration applications captured, upon user choice, may remain in partial completion status, until additional requirements are received or authorized users apply the update or create a new voter.
  8. Must determine and indicate whether the voter is required to provide ID when voting in accordance with HAVA Section 303(b) and 42 U.S.C. Section 15483(b)(1), and any other applicable state or federal law.
  9. Once a Voter ID is assigned to a voter record, system must record voter status, according to configurable business rules.
  10. Must determine and assign the voter’s election district. See Voter Registration – Registration Processing – Election District Assignment.
  11. Must provide ability for “Walk-in” applicants to interact with a signature-capturing device, including:

1. Choose from changing or not changing party affiliation
2. Selecting a party affiliation from a list or typing a party name of their choice
3. Accepting and signing the declaration
   1. The signature-capturing device must display existing voter information, newly captured voter information, as well as general information (e.g. closed period for changing party affiliation).
   2. Must provide ability to scan and upload applications from non-walk-in registrants. Facilitate automatic signature clipping.
   3. When a county submits a change in status of a voter’s registration to “cancelled” or “inactive” based on information received locally within the county, system must automatically accept the change in status and the county-supplied reason for the change.
   4. For each new registration, reregistration, or update of name, date of birth, CDL/ID or SSN4 with the resultant new or updated record in “active” status, system must compare that record against available death records for possible matches.
   5. For each new registration, reregistration, or update of name, date of birth, CDL/ID or SSN4 with the resultant new or updated record in “active” status, system must compare that record against available felon records for possible matches. See Felon Research for additional information.
   6. For each new registration, reregistration, or update of name, date of birth, CDL/ID or SSN4 with the resultant new or updated record in “active” status, system must compare that record against all other existing records for possible duplicates.
   7. Must provide ability to segregate deficient voter registration applications.
   8. Capture, store, view all forms and correspondence received from the voter.

Note: Digitally sign and verify it. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

* 1. Flag registrations that provide residence locations that are not shown as dwellings for further investigation
  2. Should also provide for a search by address that provides a list of persons registered at that address, this is useful if the version of the name on the new application is too different from the name of the same person registered at the address.
  3. Must prevent persons registering at a prohibited address (USPS PO boxes, private mailbox facilities, etc., but provide a capability for a supervisor to override and include the reason for the override.

1. **Voter Registration – Registration Processing – Election District Assignment:**
   1. System must automatically assign districts, including election district, based on the residence address provided.
   2. System must have a central repository of addresses, election district and district assignment information.
   3. System must allow an address point or a street segment to be updated.
   4. System must provide tools to facilitate a consistent approach to assigning and maintaining election districts and districts.
   5. System must provide the capability to record election district and district geographic descriptions.
   6. System must provide a method for manually overriding assigned election districts and districts.
   7. System must provide the capability to prepare jurisdiction, district, and election district data.
   8. System must provide the capability to map addresses to unique election districts and appropriate office districts.
   9. System must provide the capability to verify election districts and district records.
   10. System must provide the capability for County to maintain the election districts, district and address data for its own county.
2. **Voter Registration – Registration Processing – Felon Research:** This describes the process of reviewing possible felon matches.
   1. Must provide ability to match against the Delaware Criminal Justice Information System to determine if registrant is a felon.
   2. Must provide the capability for authorized Administrators to enable or disable the felon verification.
   3. Upon determining that registrant is a possible felon, the system must flag the record for further investigation.
   4. Must provide ability for Department of Correction users to review all registrants flagged as possible felons.
   5. Must provide ability for Department of Correction users to view relevant registrant information to determine if the registrant has completed his/her sentence.
   6. Must provide ability for Department of Correction users record the outcome of their research.
   7. Must provide ability to proceed with new registration, reregistration, or update of registration for non-felons and felons who have regained their right to vote (e.g. completed their sentence).
   8. Must provide ability to reject applications for non-eligible felons and to store the reason for rejection in the application.
   9. Must provide ability to generate report, extract date, and create letters of rejections.
   10. Must provide the capability for authorized users to register or deny registration regardless of Department of Correction research outcome. System must capture and store reason and user information for overrides.
3. **Voter Registration – ID Verification:** These requirements describe the ID verification that is to occur for every voter registration or re-registration transaction before it is applied to the voter registration roll.

The process validates a DE driver’s license number, an identification card number or an SSN4 through an interface involving data maintained by Delaware's Department of Motor Vehicles (DMV).

* 1. Must support the DMV ID verification (IDV) interface, which operates on a transactional basis, for SSN validation, per HAVA.
  2. For new voter registrations, re-registrations, and for updates with a change of name, date of birth, DL/ID or SSN4, system must automatically submit the data for validation from the DMV or the Social Security Administration through the IDV interface.
  3. When ID verification cannot be completed at time of receipt of the transaction, the record must be saved with an indicator/flag, and system must automatically retry an incomplete ID verification.

1. **Voter Registration – DMV Change of Address:** Delaware’s current implementation of the National Voter Registration Act (NVRA, or ‘motor voter’) allows for electronic processing of address changes for existing registered voters.

System to provide functionality to support this process, namely:

1. Attempt to match the records against existing voter registration records;
2. Provide such matches for appropriate processing; and
3. Provide unmatched (or below the established confidence threshold) transactions for further research and possible match to a voter.
   1. Must receive voter registration address change data from ERIC, other sources in accordance with the National Voter Registration Act (NVRA).
   2. Must attempt to match change of address (COA) transactions against existing voter registration records using established matching criteria (See Record Matching and Merging for requirements specific to matching criteria.)
   3. For matches of COA transactions against existing voter registration records that meet or exceed the established confidence threshold, system must, either automatically or upon user choice:
4. Update the existing voter registration record with the new voter registration data received; and
5. Update the voter activity history with the basis for registration changes.
   1. For matches of COA transactions that do not meet the established confidence threshold for automatic matching but that meet the established minimum confidence threshold of that match function, system must automatically notify the county that it must make a determination of whether the records match.
   2. When a county verifies that a pre-existing voter registration record matches the COA transaction, system must:
6. Record that information, including the basis for determination, in the voter activity history of the matched voter; and
7. Update the existing voter registration record with the new voter registration data.
   1. If a county determines that the potential match of COA transaction to a preexisting voter registration record is not valid, system must record the determination that the COA transaction was not associated with the record and the basis for that determination.
   2. Must provide authorized users the capability to un-match previously matched COA transactions at any time after such matches have been applied. In such instances, system must correct any changes that were applied to the record as a result of the prior match and handle the transaction as a confirmed non-match for that process.
   3. When a COA transaction cannot be matched against any existing voter registration records, system must send unmatched COA data to the appropriate county.
8. **Voter Registration – Polling Place Cards:** The department must mail voters polling place cards (PPC) following voter registration, reregistration, or updates to the voter record based on a variety of data points (e.g., voter’s notification of an address change).

System must provide the capability to generate an extract to mail PPCs through a third party such as the Department of Technology and Information, Office of Management and Budget: Government Support Services - Printing and Publishing Office.

* 1. Must have the capability to generate a data extract, based on the applicable mailing address for each voter of all required PPC information across the State so that PPCs can be printed by the State through a third-party mailing house.
  2. Must have the capability to generate pre-formatted and pre-populated PPC in PDFs, based on the applicable mailing address for each voter of all required PPC information across the State so that the PDFs can be printed in-house, by the State, or through a third-party mailing house.
  3. Must indicate in the voter record the date that the record was included in a data extract or PDF for PPC mailing.

1. **Voter Registration – Absentee Voting:** These requirements focus on supporting voters that will not be voting in their designated polling place on Election Day. Voters may request for absentee ballots mailed to them or they can walk in to their county office to vote on an absentee ballot in person. Voters may be eligible to vote absentee thru either UOCAVA (Federal law) or and “regular absentee” (Delaware law).

The data elements listed here do not constitute an exhaustive list of required data. Department of Elections expects that during the Design Phase, the Contractor will work with department staff, partner agencies, and vendors to determine all specific data elements necessary to meet all requirements stated in this RFP.

* 1. System must capture Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) flags, whatever Election Administration and Voting Survey (EAVS) and FVAP reporting requirements are.
  2. Must capture and store the following data for every election:

1. Type of application (e.g. Federal Postcard, Federal Write-In, Special Write-In, State defined application/affidavit, etc.);
2. Source of the application (how received);
3. Type of voter: Military, Overseas Citizens, etc.;
4. Date application was requested;
5. Date application was sent;
6. Date application was received;
7. Date application was returned (post marked);
8. Type of elections/ballots requested;
9. Whether or not the application was accepted or denied; and if denied, the reason for the denial. Use codes that can be defined and modified by authorized Administrators.
10. Whether the voter wishes to exercise the permanent vote by mail option;
11. Date vote-by-mail ballot was mailed;
12. Whether the person voted in-person;
13. Manner in which the absentee ballot was transmitted to the voter;
14. When the absentee ballot was received by the elections official;
15. Method of sending absentee materials (e.g., mail, fax, email, etc.);
16. Method of sending absentee ballot (e.g., mail, fax, email, etc.);
17. Method of return of absentee ballot (e.g., mail, fax, etc.);
18. Address to send absentee ballot to.
19. Form of voting (e.g., county absentee ballot or federal write-in vote-by-mail ballot);
20. Date absentee ballot was returned (post marked);
21. Date absentee ballot was received;
22. Whether the ballot was accepted or rejected; and
23. If rejected, the reason for that rejection. Use codes that can be defined and modified by authorized Administrators.
    1. Must capture and store the status of uniformed services and overseas voters that have been identified and fall under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), including the following information:
24. Classification (e.g., Uniformed Services or Merchant Marine on active duty, Eligible spouse of dependent, National Guard member on State orders, etc.); Codes that can be defined and modified by authorized Administrators.
    1. Must capture and store the status of absentee voters (non-UOCAVA), including the following information:
25. Expected location and contact information on election date
26. Reason for voting absentee, based on codes that can be defined and modified by authorized Administrators.
27. Special qualifications
    1. Must support paper and online applications. For applications submitted online refer to State-Level Processes – Website: Voter Portal (Public Access).
    2. Must capture an image of the application (i.e. FPCA, Absentee Affidavit) and attach it to the voter’s record.
    3. Must be able to register new voters and update existing voter registrations from UOCAVA applications (FPCA).
    4. Must be able update voter registration from absentee applications/affidavits.
    5. Must be able to send automated email notification at every step of the absentee voting process, e.g. upon receipt, completed.
    6. Must be able to update and delete applications.
    7. Must be able to change/remove absentee status.
    8. Must be able to capture information for walk-in voters, including electronic signatures for absentee applications.
    9. System must allow for the extraction of absentee voters by election or all elections.
    10. Must be able to accept applications, provide status, mark absentee ballots, etc. online (See State-level Processes – Website: Voter Portal (Public Access)).
    11. Must be able to assign unique ID (a.k.a. voucher number) for every absentee ballot issued, e.g. for walk-in applicants.
    12. Must be able to generate a list of reserved voucher numbers for future absentee ballot issuance, e.g. for paper applications as a backup or alternative intake.
    13. Must be able to assign voucher number by batch, e.g. issue voucher numbers to every voter eligible to vote by absentee for a specific election, by voter type.
    14. Must be able to void, reissue, and make corrections to voucher numbers or a range of voucher numbers.
    15. Must be able to identify whether a voucher number has been assigned, or reserved. If reserved, whether it’s been assigned/used or not.
    16. Must be able to print mailing labels for absentee envelopes.
    17. Must be able to customize and design mailing labels and absentee envelope printing without assistance from the vendor. Support barcoding (e.g. Code39, Code128, QR Code, USPS IMB) of values such as the voucher number, and delivery points.
    18. Must be able to print absentee voter and mailing information directly on envelopes, e.g. a dedicated high-speed envelop printer (Pitney Bowes DA95f).
    19. Must be able to select, apply various filters and sorting absentee voters for data extraction, reporting, printing of labels and envelopes.
28. **List Maintenance – Record Matching and Merging:** These requirements focus on the configuration of criteria for determining matches between records (either duplicate voter records, matches returned in response to a user-initiated search, or matches of voter records with death, felon or third party address change records) and on requirements associated with merging records that are determined to be a “match.”

Though this section is called upon in Registration Processing and matching is referenced DMV Change of Address and other List Maintenance requirements sets, the focus here is the specification of the matching processes and the merge and unmerge processes.

* 1. Must include a user-configurable method for authorized Administrators to:

1. Establish sets of registration record matching criteria;
2. Configure which criteria apply to each type of matching function (e.g., user-initiated registrant search for list maintenance/research purposes, user-initiated search for purpose of submitting data additions or updates, search for existing record upon receipt of a registration transaction, death record matching, felon record matching, duplicate record checks, NCOA matching, etc.);
3. Assign “confidence” levels to each criteria set as it applies to each matching function; and
4. Establish threshold confidence levels required for manual or automatic application of matches for each matching function.
   1. Must allow authorized Administrators to establish one or more bases for matching data in a registration record field, including (where applicable):
5. Exact character match;
6. First “X” characters of the field (where “X” is user configurable);
7. Same characters and order in string, but with spaces and punctuation removed;
8. Soundex match (or alternative method based on phonetic pronunciation);
9. Common nicknames match based on common variations of First Name established by authorized users (e.g., Robert = Bob, Bobby, Rob);
10. “X” matching characters within string; and
11. Same month and year.
    1. Must allow authorized Administrators to identify a set of matching criteria based on combinations of individual field match settings, such as:
12. First Name- with “Common nicknames”; Last Name- first 4 characters; and Date of Birth- same day and month; or
13. DL/ID exact match; First Name- with “Common nicknames”; Last Name- with Soundex.
    1. Must allow authorized Administrators to configure and update whether or not an established matching criteria set is applied to each matching function, including:
14. Registrant searches for purposes of pre-populating a voter record;
15. Registrant searches for list maintenance and research purposes;
16. Searches for an existing record based on the ID;
17. Duplicate registration checks;
18. DMV, DHSS-DSS, DOL transaction processing;
19. Death record matching; and
20. Felon record matching.
    1. Must allow authorized Administrators to individually establish “confidence” values to each established matching criteria set as it applies to each potential matching function.
    2. Must allow authorized Administrators to establish and modify confidence thresholds for each matching function so that matches found that meet or exceed that confidence threshold are automatically applied by the system. For matches that do not meet that threshold, but meet a lower “manual” minimum matching threshold, system must generate electronic notices/lists or flag the records for the appropriate county for match review and resolution.
    3. Prior to merging, system must allow user to select which of the records will be the base for the final voter record, and the option to copy values from certain fields from the other record.
    4. When applying the merge, system must:
21. Record that information, including the basis for determination, in the voter activity history of the matched voter; and
22. Create a voter registration record with the new consolidated voter registration data.
    1. When evaluating voter records to identify potential matches with other voter records (match within the system), DMV transactions, death records and felon records , system must exclude the following from matching results and notices to counties when same match criteria were used:
23. Previously verified matches;
24. Previously verified non-matches; and
25. Previously identified potential matches pending determination.
    1. Must provide the ability for authorized users to batch clear, by date range and/or by the county user ID, match determinations made inappropriately.
    2. Must merge voter registration data into a single registration record when duplicate registrations are confirmed. The voter registration data must include voter activity history and voting participation history and be merged into the record with the most recent date of registration or voter registration update activity.
    3. Must provide authorized users with the ability to un-merge a single voter registration record into separate registration records in the event that registration records were incorrectly merged. The separated voter registration data must include voter activity history and voting participation history and the separate registration records must contain the appropriate registration data.
26. **List Maintenance – Death Records:** Department of Elections receives death records from the Delaware Health and Social Services (DHSS) and ERIC and must utilize this information for list maintenance purposes. The Department also utilizes obituaries for list maintenance.

Department of Elections is responsible for ensuring any confirmed matches of death records with registered voters result in a cancellation of voter registration of the deceased persons.

* 1. Must receive and store death records from different sources, e.g. DHSS, ERIC, obit.
  2. Must match all new death records received against existing voter registration records to identify existing voters that may have died.
  3. For matches with new death records that meet or exceed the established confidence threshold, system must automatically or upon user choice:

1. Cancel the voter’s registration;
2. Record the basis for that cancellation in the voter’s activity record; and
   1. For matches of new death record transactions that do not meet the established confidence threshold for automatic matching but that meet the established minimum confidence threshold of that match function, system must automatically:
3. Note the potential match in the voter’s record; and
4. Provide a method for investigation and resolution of the potential match.
   1. Must allow an authorized county user to enter a determination of the validity of the potential match (valid or invalid).
   2. Must apply authorized county users’ determinations of validity of potential matches and change voter status, if appropriate.
   3. Must provide authorized users the capability to un-match previously matched death records at any time after such matches have been applied. In such instances, system must correct any changes that were applied to the record as a result of the prior match and handle the transaction as a confirmed non-match for that process.
   4. Must allow authorized users to exclude from death record matching processes any death record determined to be incorrect or invalid.
5. **List Maintenance – Felon Data:** In order to comply with applicable laws, system must have the capability to receive felon records from the state and federal agencies, e.g. Delaware Department of Justice (DOJ), Department of Corrections (DOC); to store such records on an ongoing basis; match records to voter registration records, and send electronic notices to counties to confirm potential matches; and, for confirmed matches, update registration status.

When felon data indicate that an individual is no longer under their jurisdiction (i.e., no longer incarcerated or on parole), system must ensure that the record is no longer included in checks for matches of felon records with voter registration records.

* 1. Must be capable of receiving and storing felon records.
  2. Must match all new felon records received against existing voter registration records to identify existing voters that may have become ineligible due to felon status, or may have become eligible to vote due to no longer being under DOJ and DOC jurisdiction (i.e., no longer incarcerated or on parole).
  3. For matches with new felon records that meet or exceed the established confidence threshold, system must automatically, or by user choice:

1. Change the status of the voter’s registration; and
2. Record the basis for that change in the voter’s activity record.
   1. For matches that do not meet the established confidence threshold for automatic matching but that meet the established minimum confidence threshold of that match function, system must automatically note the potential match in the voter’s record.
   2. Must provide the ability for an authorized county user to enter a determination that the potential match is valid.
   3. Must provide the ability for an authorized county user that has investigated and determined that the potential match was invalid to enter that determination.
   4. Must provide authorized users the capability to un-match previously matched felon records at any time after such matches have been applied. In such instances, system must correct any changes that were applied to the record as a result of the prior match and handle the transaction as a confirmed non-match for that process.
   5. Must allow authorized users to exclude from felon matching processes any felon record determined to be incorrect or invalid.
3. **List Maintenance – Duplicate Identification:** The system must have the capability to identify duplicate voter records and take action to ensure there is only one voter record for every eligible voter in Delaware in the official list of voters.
   1. Must provide the ability for authorized user to schedule and run duplicate checks across all voters in the database to identify potential duplicate registration records for the same voter using the criteria established for such matching.
   2. Must automatically, or by user choice, merge voter registration records and assign the voter to the appropriate county when duplicate records are identified based on match criteria sets that meet or exceed the established confidence threshold.
   3. Must, before automatically applying potential duplicate records, check voting participation history for the older registration record. If the older record indicates voting activity in an election after the date of registration in the newer record, the match must not be applied automatically and, instead, system must send electronic notice of potential match to the appropriate county(s).
   4. For matches of potential duplicate records that do not meet the established confidence threshold for automatic matching but that meet the established minimum confidence threshold of that match function, system must automatically note the potential match in both records.
   5. For those records where a potential duplicate was identified with a record in another county, and an authorized county user makes a determination of match validity, system must update the other record with the determination.
   6. System must provide authorized users the capability to un-match previously confirmed duplicate records at any time after such matches have been applied. In such instances, system must correct any changes that were applied to the record(s) as a result of the prior match and store the determination that the records were confirmed non-duplicates.
4. **List Maintenance – Moved out of State:** The system must have the capability to match voters against lists that contain Delaware citizens that have moved out of the state. The lists include those from DMV that list drivers who have surrendered their driver license in another state, as well as from the ERIC cross state report that lists Delaware voters that have registered to vote in another state.
   1. Must provide the ability for authorized users to schedule and run moved out of state checks across all voters in the database to identify potential records using the criteria established for such matching.
   2. Must evaluate the results and reject invalid results - such as address changes previously received.
   3. Must note a potential address change in the voter record and allow authorized users to extract records for mailing notices/confirmations.
   4. When an address update has been determined to be valid where the voter moved outside the State, system must automatically, or upon user choice:
5. Determine the status of the registrant in accordance with configurable business rules
6. Note in the activity history for that registrant that the record was updated because of Moved out of State match.
7. **List Maintenance – Non-U.S. Citizens:** System must allow for cancellation of voter registration for non-U.S. Citizens
8. **List Maintenance – NCOA:** System must provide the capability to process all registered voter records against an external USPS National Change of Address (NCOA) service on a regularly scheduled basis.

Currently, Delaware receives this service monthly from ERIC. System must update the voter record with the potential NCOA match (no change in status) and provide an electronic notice to the county for evaluation and resolution. Administrators must have the capability to monitor all such pending NCOA updates until resolved by the county.

* 1. Must provide authorized users the capability to configure a value ‘X’, such that the extracts created for NCOA processing are broken into multiple files, each containing a maximum of X records.
  2. Must evaluate the results from NCOA processing and reject invalid results - such as address changes previously received and address changes that are older than most recent changes received for a voter - according to configurable business rules.
  3. Must note a potential address change in the voter record and send electronic notice to the appropriate county of the potential address change for determination of validity.
  4. When an NCOA address update has been determined to be valid where a voter has a forwarding address in the same county, system must automatically, or upon user choice:

1. Update the (residence or mailing) address of the registrant;
2. Note in the activity history for that registrant that the record was updated because of NCOA match; and
3. Flag the record for automatic generation and mailing of an Address Verification Card (AVC).
   1. When an NCOA address update has been determined to be valid where the voter has a forwarding address in a different Delaware county or outside the State, system must automatically, or upon user choice:
4. Determine the status of the registrant in accordance with configurable business rules
5. Note in the activity history for that registrant that the record was updated because of NCOA match; and
6. Flag the record for automatic generation and mailing of an AVC.
   1. When an NCOA address update has been determined to be valid where the voter has no forwarding address, system must automatically, or upon user choice:
7. Determine the status of the registrant in accordance with configurable business rules;
8. Note in the activity history for that registrant that the record was updated because of NCOA match; and
9. Flag the record for automatic generation and mailing of a AVC.
10. **List Maintenance – Board Approval Reports:** System must allow for data extracts to be generated for elections board review prior to registration cancellation.
    1. Facilitate the tracking of inactive voters who have had no contact for X period, where X is configured by the administrator.
    2. Generate reports of all cancelled voters
    3. Generate reports of all inactive voters
    4. Generate reports of active to inactive, inactive to cancelled, active to cancelled.
11. **List Maintenance – Pre-Election Polling Place Cards (PEPPC):** System must allow for data extracts to be generated for residency confirmation postcard mailings, or currently known as poll notification card mass mailing.
    1. Must provide the ability to automatically generate a data extract of all required information in any or all counties on a batch basis so that PEPPCs can be printed by the State through a third-party mailing house.
12. **List Maintenance –Address Verification Cards (AVCs):** When the Department receives third-party notice of a change of address, elections officials are required by law to follow up with postcard to the voter alerting them to the actions being taken. For uniformity and list maintenance practices, this section describes system capability to support mailing change of address notices to voters on behalf of counties, if counties choose to have the state conduct mailings for them.
    1. Must provide the ability for authorized users to generate a data extract, based on the applicable mailing address for each voter, of all required information for one or more counties across the State so that AVCs may be printed by the State through a third-party mailing house.
13. **Voter Election Data – Official List of Voters:** As the HAVA mandated official list of eligible voters, the system must provide capability for extracting the official list of voters with respect to any election so that this data can be used to generate and print the polling place rosters and data files for electronic poll book.
    1. Must provide authorized county users the ability to extract the official list of eligible registered voters with respect to any given election.
14. **Voter Election Data – Voting History:** System must maintain voter participation history data that are necessary for to make determination of whether a voter who registers by mail must show ID the first time he/she votes.

Throughout the Election Cycle period, system must capture ongoing data changes related to vote-by mail (See Voter Registration – Absentee Voting) and provisional voting, to support the voter lookup capabilities on the public website and the interactive voice response system (IVRS).

* 1. System must provide the capability to capture vote credit history.
  2. System must allow for the adding of voter   history only when a ballot is valid.
  3. System must provide the capability to edit existing vote history.
  4. System must provide the capability to delete existing vote history. A record of deletion and who deleted must be maintained.
  5. System must change a voter’s registration status from inactive to active when vote history is applied.
  6. System must have capability for the vote by mail module (absentee) to record received ballots and flag as the source for adding vote history.
  7. System must allow for vote history to be added:

1. After an election has been certified;
2. As ballots are processed;
3. To an individual voter; or
4. Through a batch process.
   1. Must maintain historic voting participation for all voters, regardless of the number of elections in which voters might have participated. The history captured and maintained for each voting event must include:
5. State defined code for the election;
6. Election date;
7. Voting district (Election District);
8. How voted (vote-by-mail, early, polling place, or provisional); and
9. Partisan ballot voted (for primary elections).
   1. Prior to an election, system must receive data from the Election Management system or module that enables a user to determine the following data for each registered voter:
10. Voting district (Election District) assignment for the election; and
11. Polling place assignment for the election
    1. For registered voters who vote a provisional ballot in an election, system must capture and store whether or not the provisional ballot was counted and, if not, the reason it was not counted.
    2. Must capture and store the voter participation in school board elections and referendum either by individual voter or mass update (using an input file)
12. **Election Districts and Districts – Mapping:** So that the system can correctly determine the Official List of Registered Voters with respect to political districts, the system must maintain voting district cross reference information.

The information is required for derivation of residence in political district based on the voter’s election district assignment.

* 1. Must be able to identify, from the voter’s election district, the voter’s voting district for State Senate, State Representative, County Council Districts, School Districts, Municipal Districts (e.g. City of Wilmington)
  2. Must capture and store county-defined local districts (e.g., county council, levy court, school districts) and must be able to identify, from the voter’s election district, the voter’s membership in such districts.
  3. Must notify county and administrators of “orphan” election districts (e.g., election districts without voters), and of “orphan” voter registration records (lacking a valid election district assignment).

1. **Election District and Districts – Redistricting:** So that the system can apply new or updated district information to voters after redistricting, i.e. processing of drawing boundaries for electoral and political districts.

New district boundaries data are provided by the Elections Management system or module.

* 1. Must be able to determine voter’s new districts based on imported data (e.g. GIS)
  2. System must be capable of comparing districts assigned to a voter pre and post redistricting to identify potential errors. City, School and Fire District must not change.
  3. Must be able to identify, the voter’s voting district for US Congress, State Senate, State Representative, County Districts, School Districts, Municipal Districts (e.g. City of Wilmington) after redistricting.
  4. Must provide the ability for authorized users to generate a data extract, prior to applying new districts.
  5. Must notify county and administrators of “orphan” voter registration records (e.g., voters without political district assignments).
  6. When update has been determined to be accurate, system must automatically, or upon user choice:

1. Note in the activity history for that registrant that the record was updated because of redistricting.
2. **State-level Processes – Political Party Tracking:** System must have the capability to track voters’ political party data in order to (a) determine voter eligibility with respect to a primary election; (b) maintain uniformity of voter records and data; and (c) support the Voter Registration Report, which is a statistical abstract of party registration by political district.
   1. Must allow authorized users to define and document changes to political parties. For each such party, system must capture and store the following information:
3. State-assigned party code;
4. Whether or not the party is Qualified, Attempting to Qualify, or Non-Qualified;
5. Date of all changes in party status (Qualified/Non-Qualified/Attempting to Qualify;
6. Reason for such changes (if applicable); and
7. Current state party contact information.
8. **State-level Processes – Voter Registration Report (VRR):** The VRR is a statistical abstract of voter registration by election district and partisan affiliation, is published by the department at prescribed times.

The system will need the capability to report on state and county level. The VRR statistics will need to be captured and protected from alteration due to subsequent changes in the underlying voter registration data.

The system must also enable an authorized users to create, on an ad hoc basis, an extract of specified VRR data elements as of an Administrator-specified VRR Date and enable the Administrator to specify/select the internal network location to which the electronic version of the resulting extract shall be routed/stored.

* 1. Must provide authorized users the ability to view VRR completion status (e.g. 'requested', ‘in progress’, 'completed', ‘data extracted’).
  2. Must capture and store VRR statistics of active registered voters by election district and party within a county as of the established VRR date (or run date). System must capture these statistics county-by-county, or for the entire state at one time.
  3. Once a VRR has been deemed published the statistical data cannot be modified.
  4. Must support calculation and production of the following summary statistics for VRR component reports:
  5. Registration By County
  6. Registration By Senate District
  7. Registration By Representative District
  8. Registration By County District
  9. Registration By Political Party (Dem, Rep, Other)
  10. Registration By Minor Political Party (e.g. Natural Law)
  11. Registration By “Other” Political Party (i.e. free text Party Name)
  12. Must provide an authorized user the ability to:

1. Manually initiate a query to extract specified VRR data elements as of a specified VRR Date;
2. Specify the file format for the resulting extract file in accordance with authorized file formats; and,
3. Specify the internal network drive location to which the extract file should be output/stored.
4. **State-level Processes –Voter Registration Data Requests (VRDR):** Requirements below pertain to the need for the system to support workflow and associated data related to investigation, evaluation and fulfillment of VRDRs.
   1. Must allow authorized users to input, track and review Public Voter Registration Data Requests (VRDRs), including:
5. Requestor name;
6. Requestor ID number and type;
7. Requestor organization;
8. Requestor residence and business addresses;
9. Requestor contact information (phone, fax, email addresses);
10. If Requestor is acting as an authorized agent for a qualified party, the name, address and contact information for the party legally qualified to purchase the data;
11. Requestor’s stated purpose/use for the data;
12. Date of application;
13. Date application received;
14. Basis for qualification (election, party, academic, journalist, etc.);
15. Date of application fulfillment or denial;
16. Status of application;
17. Criteria used to select/exclude records for the extract; and
18. Filename(s) and number of records provided in the extract.
    1. Must allow authorized users to log the following items related to processing and fulfillment of a VRDR:
    2. Date the event occurred
    3. Time the event occurred
    4. Free-form text note, averaging fifty (50) characters per VRDR and scalable to one hundred (100) characters per VRDR, of activities and events
    5. Must provide authorized users with a method to select voter registration records for inclusion or exclusion in a VRDR extract based on multiple criteria, with the ability to specify a range or list where applicable, including:
19. County of residence;
20. City of residence;
21. Zip code(s);
22. Home voting district (Election District);
23. Political party affiliation;
24. Current or historic date of registration;
25. Age (before or after a specified date of birth, or within a specified range of dates of birth);
26. Language preference;
27. Voting participation history; and
28. Political district (such as State Senate District, State Representative District, County District, etc.).
    1. In fulfillment of a VRDR, system must be able to produce an extract as a standard text file, with a delimiter (set by the administrator) that includes user-selected data fields, such as:
29. Voter ID
30. Voter Name
31. Date of Birth or Year of Birth
32. Phone Number
33. Residential Address
34. Mailing Address
35. County
36. Districts
37. Party
38. Date of Registration
39. Voting History
40. Date Last Registration Change
41. Code Last Change Voter
42. Status of Voter
    1. System must be able to save user data extract preferences as profiles for later execution. For example users may create a profile based on HB245, i.e. a profile for public requests, candidate and political party requests, and another for the General Assembly, or State, County and local governments.
    2. System must allow users to delete previously saved preferences or profiles.
43. **State-level Processes – Website: Voter Portal (Public Access):** Requirements listed below pertain to the need to provide online voter registration and self-service lookup of registration status and ballot status.

Delaware has adopted a standard for web applications to support mobile devices by optimizing standard browser screen displays via a common look and feel.

Delaware expects that any support the system provides for mobile devices will not require installation any application or other component on those devices. The system will be required to use the common look and feel.

The requirements below include translation of public-facing pages into different languages. Pages and functions to be translated are all of those pages/functions that are used by the public in order to register to vote. Information and features that are not used in order to register to vote (e.g., polling place information) need not be translated.

The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.

* 1. For privacy purposes, the public website must require an individual accessing the website to provide sufficient personally identifiable information to authenticate the individual and to prevent others from accessing that voter's data, and must not provide or confirm any additional private information. The personally identifiable information must be configurable by an authorized administrator, such as: first name, date of birth, house number and zip code, DL/ID.
  2. For privacy purposes, the public website must require the user the option to use two-factor authentication.
     1. Telephone Verification
     2. Email Verification
     3. HOTP/TOTP Software/Hardware Tokens (e.g. Google Authenticator, Authy)
     4. Cryptographic measures not otherwise mentioned.
  3. The public website must allow a voter to determine:

1. Whether he or she is registered to vote;
2. Whether or not voter is registered as a permanent vote-by-mail or one-time mail ballot voter; and
3. Political party preference.
4. His or her elected officials.
5. Other publicly available voter information, voting history
   1. The public website must support online voter registration pursuant to applicable state and federal law, including new registration and updates to an existing registration.
   2. The public website must support online voter functions, including:
6. Submit vote-by-mail (i.e. absentee) requests
7. Submit Federal Post Card Applications (FPCA) for uniformed service and overseas citizens
8. Submit requests for voter registration cancellation for themselves and their close relatives
9. Submit requests for a polling place card
10. View voter-specific sample ballot
    1. The public website must allow a voter to choose the method of signing their requests, including:
11. Use of his or her existing electronic signature with Department of Elections
12. Use of his or her existing electronic signature with DMV. Note: Utilize existing service.
13. Use of a pointing device to draw signature, e.g. stylus, mouse
14. Use of a saved picture of a signature
15. Print, sign and mail the application.
    1. Must provide authorized Administrators a method to configure signature options for each type of application or request.
    2. The public website must allow a voter to determine the status of submitted requests.
    3. The public website must allow a voter to determine:
16. His or her eligibility to vote in an upcoming election;
17. His or her voting election district for an election; and
18. His or her polling place for an election.
19. Driving directions to his or her polling place.
    1. The public website must allow a voter to:
20. View login and logout history
21. View request history
22. Pause and resume completing the application
    1. Must allow members of the public to perform all online voter registration and self-service lookup functions using mobile devices without requiring installation of any application or component on the mobile device.
    2. The public website must allow voters who have voted a provisional ballot to determine if their ballot was counted and, if not, the reason it was not counted.
    3. The public website must allow voters who have voted a vote-by-mail ballot to mark their absentee ballot online.
    4. Must provide authorized Administrators a method to configure vote-by-mail voters that can use the online function to mark their absentee ballot online.
    5. The public website must allow voters who have voted a vote-by-mail ballot to determine:
       1. Date when his or her request was received
       2. Date when his or her ballot was sent
       3. Date when his or her ballot was received
    6. The public website must allow voters who have voted a vote-by-mail ballot to determine if their ballot was accepted and, if it was rejected, the reason it was rejected.
    7. The data on voters’ registration status and ballot status that displays on the public website must be current as of a point in time of the user’s query.
    8. Must allow an authorized administrator to control the updates of public access website data on voters’ eligibility to vote in an upcoming election, election district assignment, and polling place assignment for an election.
    9. The data that are accessible and queried through the public access website must not change during a user’s execution of a query.
    10. All public-facing web pages and functions that a member of the public views or uses in order to register to vote, change voter registration-related data, or look up registration status must be available in two (2) languages (English plus one (1) additional language). These languages currently include English, and Spanish. (Department of Elections will be responsible for providing the required translations.)
    11. Must be scalable and extensible to support web pages and functions that a member of the public views or uses in order to register to vote, change voter registration-related data, or look up registration status in a total of twenty one (21) languages (English plus twenty (20) other languages). Support for multiple language translations must not necessitate recompilation or recoding of the system.
    12. Must provide authorized Administrators a method to configure availability of the public website or select functions.
    13. The public website must have the capability to track voter registration from third party organizations and assign appropriate method of registration codes. Registration of third party organizations shall be defined by authorized Administrators.
23. **State-level Processes – Website: Offsite Registration:** Requirements listed below pertain to the need to provide online voter lookup and registration by authorized users outside of normal business environment, e.g. state fair, naturalization ceremonies.

Delaware expects that any support the system provides for mobile devices will not require installation any application or other component on those devices.

* 1. The website must require an individual accessing the website to provide sufficient personally identifiable information to authenticate the individual and to prevent others from accessing the system.
  2. For privacy purposes, the public website must allow user the option to use two-factor authentication.
  3. The website must provide capability to search voters and determine if they’re registered and to display relevant voter registration information, such as addresses, districts, polling place, etc.
  4. Must provide the capability to submit voter registration applications, including capturing of electronic signature.
  5. Must provide ability for authorized Administrators to setup the events for which users can use the website, e.g. registration drives during the week(s) of the Delaware State Fair.
  6. Must provide ability for authorized Administrators to manage users by event.
  7. Must provide ability to track registration captured by event, and by user.
  8. Registrations captured through this website will be in partial state of completion. This is purely for intake.
  9. Must provide ability for authorized Administrators to configure the types and levels of validations, e.g. ID verification, felon checks, for applications captured through this method.

1. **State-level Processes – Voter Registration Services:** Support real-time voter registration from other state agencies and partners.
   1. Must host services that will securely and reliably receive voter registration transactions (including declinations) from state agencies and partners, e.g. DMV, DHSS-DSS, DOL, etc., in real-time.
   2. Must provide state agencies and partners the capability to:
      1. Determine if their customer is registered to vote;
      2. If not registered, allow the customer to decline to register to vote;
      3. Determine if period of party changes is open;
      4. Retrieve list of political parties
   3. Must support over-the-counter (e.g. DMV associate processing an applicant) and self-service (using kiosks, or using personal devices via the internet) voter registration methods.
   4. Must store and capture data and electronic signature for voter registration. Note: Signature capturing methods use by state agencies and partners are outside of the scope of this RFP.
   5. Must provide capability for county elections staff to review each application prior to creating new voters or updating existing voter registrations.
2. **State-level Processes – Voter Registration Query Services:** Support voter registration queries from users of other state agencies and partners.

Certain citizen services provided by Department of Insurance, Office of the Lt. Governors, Office of the Governor, and General Assembly require them to be able to inquire voter’s registration information, such as address, political affiliation and voting history.

* 1. Must provide authorized Administrators capability to create and manage user accounts for users of other state agencies and partners
  2. Must provide authorized Administrators capability to determine and setup limited access to users.
  3. Queries from users of other state agencies and partners must not update voter registration information.
  4. Must provide state agencies and partners the capability to login to search voters.

1. **State-level Processes – Voting History Match:** System must provide capability to process ERIC data containing possible voting history matches (possible double-voting).
   1. Must provide capability to extract voter registration, absentee information, voting history, and other relevant information to assist in the investigation.
   2. Must provide capability for authorized users to capture and store status/determination of each case. Use codes that can be defined and modified by authorized Administrators.
   3. Must provide capability to generate reports.

**General System Requirements:**

1. **Standards and Policies:** The system must comply with State of Delaware Enterprise Standards and Policies, Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information.
2. **Audit Requirements:** The system must log every action that changes voter registration data, election district mapping data, political party data, or security roles or role assignments. Logs must contain sufficient information for authorized Administrators to reliably reconstruct the chain of events and, where possible, track them back to a specific user.
   1. Must log all creations of and updates to voter registration data that are executed as a result of actions by users and automated processes. The following information must be logged for each such change to voter registration data:
3. Data that was changed;
4. Prior value of the data before the change (if applicable);
5. Date and time of the change; and
6. Source of the change (either an automated process identifier or user ID/name).
   1. Must log all creations of and updates to voter registration data that are executed as a result of actions by members of the public using the public access website. The following information must be logged for each such change to voter registration data:
7. Data that was changed;
8. Prior value of the data before the change (if applicable);
9. Date and time of the change; and
10. Source of the change (i.e., ‘website user’).
    1. Must log all instances of viewing individual voter registration records, searching voter registration records, executing queries and reports against voter registration data, and executing extracts of voter registration data that are initiated by users. The following information must be logged for each such instance:
11. Date and time of the initiation of the view of the record, search execution or query/report or extract execution;
12. Source or performer of the action (user name); and,
13. For searches, executions of queries and reports, and executions of extracts, the data selection and filtering criteria for the search, query/report, or extract.
    1. Must log creations of and updates to election district and political district data (as described in Election District and District-Mapping) by users. The following information must be logged for each such change:
14. Data that was changed;
15. Prior value of the data before the change (if applicable);
16. Date and time of the change; and
17. User name for the individual who submitted the change.
    1. Must log creations of and updates to political party data (as described in Political Party Tracking) by users. The following information must be logged for each such change:
18. Data that was changed;
19. Prior value of the data before the change (if applicable);
20. Date and time of the change; and
21. User name for the individual who submitted the change.
    1. Must log all creations of and updates to security roles, security role permissions, and assignments of security roles to users. The following information must be logged for each such change:
22. Data that was changed;
23. Prior value of the data before the change (if applicable);
24. Date and time of the change; and
25. User name for the individual who submitted the change.
    1. Must provide a graphical user interface for authorized administrators to search, view, and print audit log data including filtering and sorting by any field or combination of fields. Filtering must support wild card searches and range of data where applicable.
    2. Must provide authorized administrators the capability to archive audit log entries prior to a given date of change and to retrieve archived data according to configurable criteria.
26. **Reporting/Querying Requirements:** The solution must include multiple pre-defined reports ready for execution by an authorized user, plus capability to define and execute ad hoc reports and queries.
    1. The solution must provide authorized users with capability and tool(s) to query data and create formatted reports with user-defined sort criteria, filters, and subtotals/totals.
    2. System must include a process for analyzing and reporting voter registration data for federal statistical reporting.
    3. System must provide the capability to generate a report on underage voters in the database.
    4. System must provide the capability to generate a report on new registrations.
    5. System must provide the capability to generate a report on political party changes.
    6. System must provide the capability to generate various voter registration and voting history statistical report. See some publicly available report at <https://elections.delaware.gov/services/candidate/regtotals.shtm> for reference.
    7. System must capture statistics for paper and electronic registrations from referring agencies.
    8. System must provide reporting capability on any and all data fields.
    9. The data that the system displays in response to an executed report or query must be current as of a point in time of report/query execution.
    10. The data extracted during execution of a report or query must not change during query execution.
    11. Must allow authorized users to save created ad hoc report data selection, sort, filter, grouping, and formatting parameters for later re-execution.
    12. Must allow authorized users to manually delete previously saved query/report statements (data selection, sort, filter, grouping and formatting parameters).
    13. Must provide execution-ready versions of the pre-defined reports.
    14. Must, for both ad hoc queries, ad hoc reports and pre-defined reports, allow the user to:
27. Preview/display the report or query results on screen, instead of or prior to printing the report;
28. Print results of the entire report/query or user selected page(s) to a user selected printer in a local network environment; and
29. Export the report or query results electronically to a user specified location external to the system, in multiple formats, including: Acrobat PDF, RTF, comma-delimited text file, and tab-delimited text file. (Report and query output will not be stored within the system.)
    1. For ad hoc queries and reports as well as predefined reports, the system must provide authorized users with a visual “progress indicator” during data extraction and report generation, and must allow users who execute a query or report to cancel execution prior to completion.
    2. For both ad hoc and pre-defined reports, the system must, at authorized user option, include the report parameters and report execution date in report output.
    3. Must make all stored queries and reports available for immediate generation and for batch generation.
    4. Must provide information to authorized users that batch-executed reports are completed.

# Appendix B, Part 6: Absentee Voting

**Vendor shall provide voting equipment for absentee voting that meet or exceed the following requirements:**

**Overview**

1. The US EAC must have certified the voting equipment against VVSG 1.0 standard or higher.
2. Provides all voters the opportunity to privately and independently cast his/her vote.
3. Shall be scalable – each voting device can handle a minimum of 1,000 complex ballot styles for an election, multiple languages, and various election configurations.
4. Voters’ choices shall be reflected on a paper record created by the voter or voting system that a voter can review before it is cast and that is suitable for a recount.
5. The voter should be able to activate the voting device and/or select accessibility features without poll worker assistance in a manner that results in the display of the correct ballot for the voter.
6. Voting machine that utilizes voter completed paper ballots should possess the capability to determine the intent of voter who does not mark his/her ballot according to the instructions. Further, the system must possess the capability to process normal variations in printing and scanning without requiring adjustment of the mark reading thresholds.
7. Voting machine that utilizes voter completed paper ballots must possess the capability of processing a ballot with a blank second or back page if no election data flows to the second or back page.
8. Voting equipment that utilizes voter completed paper ballots shall possess the capability of sorting write-ins, blanks, and over-votes on a high-speed scanning device and reporting write-in votes by race and election district.
9. Voting equipment that utilizes voter completed paper ballots shall possess the capability of processing ballots up to nineteen (19) inches.
10. Export results by election district and race onto multiple copies of paper, and onto removable media that can be read and securely transmitted to a secure location.
11. The absentee system should use standard paper instead of ballot stock and operate on a ballot on demand system using a COTS printer.

**System Requirements, Performance and Capabilities**

The system shall be used to count absentee ballots at central locations in each of the State’s three counties and shall meet the following requirements in addition to those mandated by the State’s legal requirements listed in Appendix B – Part 2 Voting Machines and by the VVSG versions 1.0, 1.1 or 2.0.

1. **Accuracy**
2. Have control logic and data processing methods to detect errors and provide a method for resolving errors on ballots which impede tabulation without human review while still allowing and supporting manual review mechanisms—but which does not require physical remaking of paper ballots;
3. Provide for the tabulation and reporting of write-in votes;
4. Accommodate multi-member districts whereby multiple votes are cast for more than one position in the same election;
5. In the event of the failure of a unit, retain a record of all votes cast prior to the failure; the unit shall provide for the audit of all records retained prior to the failure to determine if the records were affected by said failure.
6. Shall not count overvotes;
7. Shall record and report the number of undervotes and overvotes for each office and/or question on the ballot;
8. Shall count ballots from various Election Districts without requiring the system to be stopped, reset, etc. when encountering a different Election District; and
9. Shall provide a report after each batch of ballots have been counted that shows the number of ballots counted in each batch as well as the number of ballots not counted.
10. **Audit and Security**
11. Provide that each voter’s ballot is secret and the voter cannot be identified by image, code or other methods
12. Provide printed records regarding the opening and closing of the polls and include the following:
    * + 1. Identification of election, including opening and closing date and times;
        2. Identification of each unit;
        3. Verification that all counters are set at zero; and
        4. Identification of all ballot fields and all special voting options.
13. Prevent printing of results before the sequence of events required for closing of the polls are completed;
14. Any programmable memory device shall be sealed in the unit with means of tamper resistant and preventative measures; engineering level information by the vendor must be provided to the State of Delaware;
15. Allow for extraction of data from memory devices to a central host; and

Note: Digitally sign it. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. Provide safeguards against unauthorized tampering of any system component. All components should exhibit trusted computing characteristics and be tamper resistant and preventative.

**3. Building Absentee Ballots (ballot preparation and other services)**

The Central Count Absentee System shall include the hardware and software required to accomplish the functions described below.

1. Absentee Ballot Specifications
2. For each election, the system shall provide each Department of Elections the capability to develop a database containing all necessary records and fields to build the ballots for each Election District in the county for primary, general and school elections. This includes:
3. Election specific data to include global settings as appropriate;
4. Political parties and appropriate logos;
5. Candidates;
6. Offices with links to the appropriate candidates;
7. Referendums with links to appropriate responses;
8. Election Districts with links to the appropriate Offices; and
9. Reporting zone, if necessary (the location from which the results will be reported)
10. The vendor’s system shall provide the capability to create new elections, retain previously defined elections, and reuse previously defined elections. Such systems shall facilitate error-free definition of elections and their associated ballot layouts.
11. The vendor’s system shall provide proof sheets for each record so that the associated information can be verified.
12. Absentee Ballot Process
13. The vendor’s system shall provide a mechanism for defining the ballot, including the definition of the number of allowable choices for each office and contest, and special voting options such as write-in candidates.
14. The vendor’s system shall generate all required master and distributed copies of the voting program in conformity with the definition of the ballot for each Election District. The systems operating the voting program must operate within a trusted computing environment – more specifically the full stack of the computer system must be cryptographically verifiable.
15. The distributed copies, resident or installed in each voting device, shall include all software modules required to monitor system status and generate machine-level audit reports, to accommodate device control functions performed by maintenance personnel, and to register and accumulate votes.
16. Absentee Ballot Validation
17. The vendor’s system shall provide a mechanism for executing test procedures that validate the correctness of election programming for each voting device and to insure that the ballot corresponds with the installed election program.
18. The vendor’s system shall be able to receive data electronically from the State’s Election Management System.

Note: Verify it cryptographically. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. The vendor’s system shall also be capable of transmitting accurate absentee results electronically to the State’s Election Management System.

Note: Digitally sign it. Refer to GSS\_18809\_ELECTIONS\_SYS\_rfp -> Technology requirements -> STANDARD PRACTICES for additional information. Specifically, Cryptography Standard, and Key Management Standard.

1. The vendor’s system shall accommodate multiple languages. The system shall allow local election officials the ability to download information from software used to translate information to the appropriate language or the system should perform translations automatically with controls in place to ensure translations are accurate.

**4. Ballot Printing**

1. The vendor’s system shall provide the capability for the Departments of Elections to print ballots as needed. Each ballot shall have the minimum control information in text and barcode:
2. Ballot style; and
3. Election District.
4. The vendor’s system shall provide the capability to print ballots up to nineteen (19) inches.
5. The voter shall make his/her selections by filling in an oval or rectangle located next to the name of the candidate.
6. Where the column format as shown in voting machine section is not possible, we desire that the system shall print the appropriate party logo to the left of each candidate’s name and/or the candidate’s party under his/her name.
7. Where ballot paper used in the system is not a COTS product, the vendor shall provide the Departments of Elections the capability to purchase the paper directly from the vendor or the vendor’s source.

**5. Back-Up Power**

The system shall have the capability to operate for at least 16 hours during power failures, power surges and other abnormal electrical occurrences. The vendor shall provide documentation of the backup system and its maintenance when not in use for elections. This back-up power capability shall engage immediately with no loss of data in the event of disruption of electrical connection, and power all system components. NOTE: We are willing to discuss alternatives to this requirement.

**6. Speed of System**

A single device (scanner or tabulator) shall count at least 50 ballots per minute.

**7. Election Reporting Requirements**

1. Provide printed results of the absentee votes by election district for each candidate for each office and/or each question, and cumulative results for each candidate for each office in the format specified by the State.
2. Provide a report for each Election District that shows the offices up for election, the candidates for each office and the absentee votes that each candidate receives for use at the Board of Canvas.
3. Provide a report that shows the number of ballots counted along with the overvotes and undervotes for each office and for each office by Election District.
4. Each report shall show the name and date of the election.
5. Provide functionality to transmit election results via Secure File Transfer Protocol to the appropriate server over the State’s wide area network.
6. Provide for the storage of election results in any version of software required, i.e., Access, Excel, PDF, ASCII and HTML.
7. Provide for election results to be produced in such a manner as to allow for easy copying for paper distribution upon request.

**8. System Audit Log**

The system audit log shall contain sufficient information to allow the auditing of all operations related to ballot tabulation, results consolidation, and report generation. It shall be created and maintained by the system in the sequence in which events and/or operations occurred.

**9. Access to Election Data**

Provisions shall be made for authorized access to absentee results after closing of the polls and prior to the publication of the official canvass of the vote. The system may be designed so that results may be transferred to an alternate database or device. Access to the alternate file shall in no way affect the control, processing, and integrity of the primary file or allow the primary file to be affected in any way.

**10. Other Requirements**

1. Devices should be transportable, without damage to internal circuitry;
2. Devices should withstand frequent loading and unloading, stacking, assembling, disassembling, reassembling, and heavy use, without damage to internal circuitry.
3. Devices should provide Election Officials with a method to immediately detect if a voting unit is not operating properly;
4. Devices should be “tamper-proof.”

# Appendix B, Part 7: DTI Standards

**7a. Cryptography Standard**

****

**7b. Key Management (without PARR)**

****

**7c. Application Security Standard**

****

**7d. Web Application Security**

****

**7e. eSignature Policy**

****