OSET Institute Development Group – CoreTeam
Request for Comments: **101**
BCP: N.A.
Obsoletes: NONE
Category: **REQUIREMENTS**

March 2012

The TrustTheVote™ Project
Digital Voter Registration System

Status of this RFC

This Request-for-Comment provides design requirements for the TrustTheVote Project community. This RFC does not specify, but intends to be the basis for proposing a digital voting technology standard with regard to open source voter registration systems. Distribution of this memo is intended to be unlimited but is initially being provided to the Design Congress stakeholder community and other OSET Institute Advisers from who early comment on this preliminary draft is sought. Special thanks go to CA Dep. Secretary of State and State Elections Director Lowell Finley and his team for their excellent work in producing their VoteCal RFP, which served as a catalyst in the original (2009) drafting of this RFC.

Table of Contents

Section I
Introduction

1.1 Purpose of This Request for Comment

The purpose of this Request for Comment (RFC.101) is to solicit advice, comments, and proposed revisions that will inform the TrustTheVote Project (TTV) Core Team (hereafter "Core") final design and specification decisions for the Digital Voter Registration System ("DVRS") architecture and reference implementation. DVRS is an open source single centralized voter registration database that meets applicable Help America Vote Act of 2002 (42 U.S.C. 15301, et seq. HAVA) requirements.

The purpose of this RFC is to provide a thorough understanding of a Digital Voter Registration System and related HAVA requirements. The system as designed is intended to support upload of a state's county or precinct level voter registration data from their own election management systems. The DVRS will interoperate with a future TTV Election Management System (EMS).

The objective is to produce an open source design specification and reference implementation for a DVRS suitable for adoption by any State of the Union pursuant to the final version of this RFC. The goal is to produce an open source result that has the approval and endorsement of the TTV Stakeholder Community.

Note that "approval and endorsement" is for the design and specification of the DVRS and not necessarily a recommendation for adoption of the implementation in any jurisdiction.

1.2 Scope of This Request for Comment

Pursuant to RFC.001, the scope of RFC.100 covers the business functional requirements for DVRS only. References to government codes and regulations should be verified. RFC.100 has been originated on roughly on the requirements for the State of California, although it is intended that DesCon will guide a final specification that represents a hybrid system framework capable of implementation in any jurisdiction albeit with localization requirements.

Generally, an RFC drives two types of design specifications: the External Design Specification (EDS) and optionally an Internal Design Specification (IDS). The EDS is intended to define two of the three "faces" of an interactive system[1]: the "outer-face" or user experience, and the "interface" or the components and services that provide the interoperability between back-end services and data sets and the actions of users. Some systems are sufficiently complex or represent information technology innovations that require specifications of the back-end layer or "inner-face." The IDS document is used for this purpose.

Importantly, in the TrustTheVote Project, an RFC is not a design specification, regardless of type (EDS, IDS), nor can it be a replacement for the same.

1.3 ADA Compliance

To meet and carry out compliance with the nondiscrimination requirements of Title II of the Americans with Disabilities Act (ADA), it is the policy of the OSET Institute and TrustTheVote Project to make every effort to ensure that its designs, specifications, and reference implementations are guided by the needs of persons with disabilities.

[1] See generally, Dr. Aaron Marcus http://www.amanda.com/people/staff/staff_f.html

Section II
Typical System, Challenges, & Opportunities

2.1 Introduction

The objective of this section is to provide an understanding of a typical State's voter registration, election systems, and related needs. In addition, this section discusses the manner and extent to which information technology is typically applied in voter registration business functions within a State system. The TrustTheVote Project has chosen to base a significant portion of its "model" on the voter registration services as they exist in the State of California. As this RFC evolves, it is anticipated that elements of other States' systems may be incorporated for purposes of reference and driving requirements for a general purpose state digital voter registration system.

This section is divided into the following subsections:

- Business Program and Functions
- Challenges and Opportunities
- Constituents and Users
- Typical Technical Environment and Infrastructure

2.2 Typical Functionality

The following overview describes the typical voter registration functions and processes. This overview includes a brief description of the manual and automated processes that support the service. In many cases, particularly for larger states such as CA, "voter files" are maintained separately by the elections official of each of the State's counties.

Voter information is usually keyed or in more modern systems, scanned into county databases. Information in the voter file can be used for a variety of purposes including:

- Determining which precinct and political subdivision the voter is a resident of, based on the voter's declared address;
- Determining a voter's eligibility to participate in a particular election, and the appropriate ballot "style;"
- Processing of absentee and provisional ballots;
- Calculating precinct size and drawing precinct lines;
- Determining district boundaries for political subdivisions within jurisdictions;
- Producing precinct rosters;
- Tracking absentee voters and mailed absentee ballots;
- Providing voter registration information to individuals and organizations eligible to receive this information;
- Conducting county residency confirmation, sample ballot, absentee voter applications, and other mailings;
- Hiring precinct workers who, in many states, must be registered voters;
- Verifying that a candidate is registered with the party they are running under and is a resident of the jurisdiction in which they are seeking nomination/election;
- Verifying signatures on petitions for initiatives, candidate nomination and similar instruments to ensure that the signer is a registered voter for the appropriate jurisdiction, has not already signed
- the same or a competing petition, and that the signature appears to match that of the registered voter.

- Providing lists for jury pool selection; and
- Processing and making notation of miscellaneous communications with voters (e.g., telephone calls, a voter making an office visit, etc.).

The Secretary of State (SOS) typically maintains the official statewide database of all active voters, supported by their voter registration system and service. This system should contain a copy of the county voter records, kept current by regular (preferably daily) updates from the counties (or other district entity). New voter records generally cannot be entered directly into typical voter registration systems today. Additions, changes, and deletion of voter information identified by the system cannot be applied directly to the database. These systems are usually updated once the counties or districts have researched the changes, applied them to their local databases and then sent their extracts to the state system in an update.

Many States' systems have recently been augmented with external automated processes in order to achieve an interim level of compliance with the Help America Vote Act of 2002 (HAVA), as required by agreement with the United States Department of Justice (USDOJ) to avoid threatened litigation for the State's potential failure to meet the HAVA voter registration database requirements by the statutory January 1, 2006 deadline. These augmentations typically included:

- Establishment of interfaces to a State's Department of Motor Vehicles (DMV) and/or Social Security Administration (SSA) to support verification of unique identifiers provided by registrants;
- Implementation of a process to obtain and apply ineligible-felon information from a State's Department of Corrections;
- Enhancement of existing processes to obtain and apply death records from a State's Department of Health & Human Services;
- Creation of new automated processes to identify non-standard and invalid county/district data and to notify counties or districts of required corrections;
- Enhancement of existing processes to support the use of United States Postal Service (USPS) National Change of Address (NCOA) data to check all registered voter addresses on a monthly basis;
- Addition of new data elements to State's databases to store and process information required by HAVA and the National Voter Registration Act (NVRA);
- Modification of current systems to load inactive voter records from counties or districts, and to edit those records;
- Automation of processes to upload county or district's data changes at the end of each business day to ensure daily currency of the State's database; and
- Modification (where possible) of adaptable existing county or district voter registration systems to include new required data elements, to support verification of voter identification through States' Department of Motor Vehicles (DMV) and SSA, to upload active and inactive records daily, and standardize data coding and formats.

All of these augmentations represent characteristics and requirements for the TrustTheVote Project DVRS. Figure 2.x illustrates the current business processes a typical state system.

2.2.1 Current Typical Voter Registration Process

The registration process begins with the individual voter completing and signing an affidavit of registration and delivering it to the county elections official or the SOS by any of several delivery mechanisms, including:

- Personal delivery to the county elections official or the SOS (in some instances SOS delivers to appropriate county);
- USPS delivery to the county elections official or the SOS (in some instances SOS delivers to appropriate county);

- Third-party delivery by registration drive or political campaign staff (e.g., Rock-The-Vote);
- DMV program mandated by NVRA (National Voter Registration Act);
- Registration at federal, state and local agencies providing food stamps, services to the disabled, or through the Aid to Families with Dependent Children, Women/Infants/Children programs; and
- Alternative mail delivery services.

Figure 2.x illustrates the typical steps involved in the voter registration process.

2.2.2. Typical Voter Registration List Maintenance Process

Duplicate, changed and invalid registrations are usually identified using any or all of the following means:

- Residency confirmation mailings;
- Use of the NCOA information provided by the USPS through private vendors;
- Notification from the Department of Health & Human Services and/or the county Registrar of Births and Deaths of the death of a registrant;
- Change of address notification and other voter information from the Department of Motor Vehicles and other state and federal agencies as designated under the NVRA;
- Notification from other jurisdictions that a voter has re-registered in a new location;
- Direct notification from individual voters that they have moved to another jurisdiction or otherwise changed their registration information;
- Notification from Department of Corrections and federal courts of individuals convicted of felonies and sentenced to prison; and
- Receipt of any official mailing returned by the USPS as undeliverable.

Batch processes are used to transfer data files from other State agencies such as the Department of Motor Vehicles, Department of Corrections, Department of Justice, and/or Department of Health & Human Services, to the system and then to convert the files from their native formats to an acceptable format for further processing by the DVRS.

The DVRS then attempts to match each record against existing records in the registration database. Typically the records are parsed into files for the appropriate county together with the registration ID of any matching registrants that are found. These files from the DVRS database are then typically transferred to the counties by way of a batch process where counties must evaluate the notices and make appropriate changes to their voter registration records.

Figure 2.x illustrates the typical steps involved in the voter registration list maintenance process. Actual activities may vary by county and/or State implementation.

2.2.3. Typical Election Processing Activities

Voter registration information is essential to election processing activities conducted by the State and County election officials. Increasingly, States are requiring that this information must be made available to election officials “24x7” basis during critical election cycles that require the mailing of voter information guides and ballot materials, printing of precinct rosters and poll books, processing of absentee ballots, and tracking of voting history.

Figure 2.x depicts the typical steps involved in the election processing activities that most directly relate to the voter registration data. Actual activities may vary by county and/or State implementation.

2.3. Common Requirements and Opportunities

2.3.1. Help America Vote Act (HAVA)

On October 29, 2002, the Help America Vote Act was adopted by Congress and became law. Section 303 of HAVA (Public Law 107-252, 107th Congress) mandates that each state implement a uniform, centralized, interactive, computerized voter registration database that is defined, maintained and administered at the state level. This database must contain the name and registration information of every legally registered active or inactive voter in the state.

The TrustTheVote Project DVRS, unlike most systems deployed today, should constitute the official record of all registered voters. It must serve as the single system for storing and managing the official list of registered voters in the state.
This centralized system must provide a functional interface for counties, which are usually charged with the actual conduct of elections, to access and update the registration data. Additionally, HAVA mandates the voter registration system coordinate electronically with the DMV, the CDPH, and the CDCR for identification and list maintenance purposes.

2.3.2. Current HAVA Requirements

Although States are rapidly brining their legacy systems closer to compliance with HAVA, there remain a number of critical limitations that must be addressed to achieve full compliance. The following are the requirements necessary achieve a compliant DVRS, driven by HAVA, and incorporated into this specification.

Single, Uniform, Official, Centralized, Interactive, Computerized List	HAVA Section 303(a)(1)(A) requires that the State (through SOS) implement a computerized statewide voter registration list that is: single, uniform, official, centralized, interactive, defined, maintained and administered at the State level, and contains the name and registration information of every legally registered voter in the State.
Data Accuracy and Timeliness	HAVA Sections 303(a)(2)(A) and 303(a)(4) require the system to include provisions to ensure voter registration records are accurate and updated regularly. List maintenance shall be performed by, “The appropriate State or local election official” in accordance with NVRA provisions.
Removing Ineligible Voters from the List	HAVA Sections 303(a)(4)(A) and 303(a)(2)(A)(ii) require reasonable effort be made to remove ineligible voters from the voter registration list. For removing ineligible voters from the list, the State shall coordinate with: the DMV Motor Voter for address changes, the Department of Health & Human Services for death notification, and the Department of Corrections and/or the Department of Justice for felony status.
Eliminating Duplicate Records and Ensuring Data Integrity	HAVA Section 303(a)(2)(B) requires list maintenance to be conducted in a manner that insures: All legally registered voters are in the

	computerized list; only voters not legally registered or not eligible to vote are removed from the list; and duplicate names are eliminated from the list. In addition, HAVA Section 303(a)(4)(B) requires the State to employ safeguards to ensure legally qualified voters are not removed in error. List maintenance activities are to be conducted in accordance with NVRA provisions.
Assignment of a Unique Identifier	HAVA Sections 303(a)(5)(A)(i) – (iii) require all new (and renewing) registrants to provide their driver's license number (DL#). If they have no DL#, they must provide the last 4 digits of their Social Security Number (SSN). If they have neither DL# nor SSN, the system must assign them a unique identifier to use as a "voter registration ID number." No registration is valid unless/until the State verifies these ID numbers.

2.3.3. Typical County Practices

There is a tremendous range of practices, procedures and policies amongst the States and their counties across the country. This document attempts to describe some typical practices and conditions, but in no way intends to suggest these are the only (let alone preferred) conditions. This document continues to utilize examples from the State of California. The purpose is to illustrate some of the diverse conditions that exist in terms of integration.

Typically, counties enter voter registration data into their systems either by key entry or by optical scanning with character recognition. Eventually batch files are created by their EMS (Election Management System) and uploaded to their State's system.

Counties periodically create extracts from their system as tab-delimited text files that contain transactions to update the State's system with the changes that have occurred since the previous extract was created. Some county registration systems do not even support transactional update files. In those cases, counties send a complete digital copy of all their registration records, which entirely replaces the records for that county in the State's database.

Any suggested changes to county data identified from any State Agency (e.g., Motor Vehicles, Corrections, Health & Human Services, etc.) and NCOA processing, and from any system duplicate checks, are typically sent to the counties for review and appropriate action. Some counties receive these notices as electronic transactions for direct import, while others receive them as print reports that must be processed manually.

2.3.3. Typical Data Exchange Protocol

Data exchanged between the States' systems and the counties is often sent in tab-delimited text files based on a standard interchange format of predefined fields negotiated with the counties. Data transfers between the States' systems and the counties, as well as other agencies, are often handled by a system of scheduled FTP batch processes.

In California for instance, there are system applications that reside on the system file server that control the flow of files into, and out of, designated directories on the county workstations ("In-Box" and "Out-Box" directories). DVRS System files generally consist of registrant transaction files, voting history files and precinct/district files, which are manually

launched for processing in the DVRS. The designated DVRS System Administrators are the only individuals with authority to process these files into the DVRS database.

2.3.4. Typical Data Characteristics

DVRS must be able to store voter registration data for up to 50 million active and inactive registered voters.

DVRS should capture history of a voter's participation in previous statewide elections. However, the amount of historical data will likely vary from county to county. Some counties may submit data for several years back, while others may not digitally capture or report historical data at all. When a registrant moves from one county to another, all historical data for that voter should be preserved, provided the registrant's move is within the State. If the registrant moves out of State, historical data should be preserved for a period of time defined by the State.

Data field standards should be defined wherever appropriate to support validation services. Fields that should have format standards include:

- Name suffix and prefix
- Gender
- Residence address data
- Mailing address data
- Place of birth

For example, if the street address field is defined to have 70 standards for street name (e.g. Blvd, Rd, Road, St, etc.) there may be up to 350 different variations in the system. Further, depending on the capabilities of a legacy county registration system, many data fields may not be populated and should be resolved by the States' DVRS.

2.3.5. Confidentiality, Privacy, and Security Considerations

Access to the application and capabilities to review confidential data must be strictly controlled by user accounts with assigned roles and enforced with encrypted passwords. A configurable expiration must be enforced on user passwords. Security roles should be fully customizable to ensure individuals are restricted to the appropriate level of information.

Current systems typically rely on private data communications infrastructure including leased lines, and most systems have little to no accessibility from public data networks, even in a secure manner. The TrustTheVote Project DVRS contemplates utilizing public data networks (i.e., the Internet) for certain accessibility requirements using common data security means which may include, but not be limited to virtual private networking (VPN).

2.3.6. Customers and Users

It is useful to understand something about the "customers" of a DVRS. Customers of a State's voter registration system include voter registrants and authorized recipients of the data (those requests for data are typically initiated with public service requests). Users of the State's voter registration program data include customers, internal SOS staff and management, local county election staff, external stakeholders, and partner agencies. Typically, only local county election staff interacts directly with SOS through the DVRS. With the rise of citizen facing online voter registration services, that condition is changing. Likewise, typically interactions between SOS and its other customers and data users rely primarily on data extracts published on digital media such as CDs. Descriptions of customers and users and their need for State voter registration data are provided below.

1. **Customers**
   "Customers" include two types: registrants who rely on county elections officials to process their voter registration affidavits quickly and accurately so that they may vote in

federal, state and local elections; and certain entities who are authorized by law to obtain voter registration data including:

- Candidates for federal, state, and local office
- Political parties
- Ballot measure proponents/opponents
- Journalists
- Academic researchers
- Other government agencies

These "customers" rely on the accuracy and timeliness of current and historic voter registration information for mailings, redistricting, media publications, and academic studies.

2. **Users**

"Users" include the following (although roles and responsibilities in the kind of DVRS contemplated by the TrustTheVote Project may be altered at the requirement of the adopting State):

- **SOS staff** (system end users) **and management** who rely on system information to perform daily work activities in support of mandated voter registration and election management responsibilities. SOS Elections Division managers rely on system information to ensure that voter registration and list maintenance activities are performed in accordance with federal and state laws and regulations. Elections fraud investigators rely on system information to identify and investigate potential violations of voter registration and election law.
- **County Elections staff** (system end users) **and management** who support the mandated official statewide voter registration list by ensuring that data in the DVRS VRDB (Voter Registration Database) accurately reflects the data in the county systems. County elections officials use the state system to verify voter identification information and identify voters whose eligibility has changed due to relocation, death or felony conviction.
- **External Stakeholders** who include the Legislature, judicial districts, and other state and local governmental agencies interested in voter registration information. For example, in California, judicial districts use voter registration data for jury pool creation and processing.
- **Partner Agencies** which can include the Department of Motor Vehicles (DMV), the Department of Health & Human Services (DHS), or the Department of Corrections and Rehabilitation (DCR). For example, DMV and DHS might exchange information with SOS regarding address and death verification information related to voter registrants. A State could use DCR data to identify persons who are ineligible felons as defined by a State's elections laws. And under HAVA provisions a State verifies with DMV the validity of any driver's license identification or, through DMV to the Federal Social Security Administration, the last four digits of the SSN provided by a registrant.

Section III
Voter Registration Business Model

3.1 Introduction

The objective of this section is to provide a description of the business processes (and associated activities) and business requirements that the TrustTheVote Project DVRS should support. The functional and technical requirements are documented in Section IV – Functional and Technical Requirements, while the business processes are defined in this Section as the Voter Registration Business Model.

3.2 Scope

At a minimum the DVRS voter registration database must be fully compliant with all applicable federal and state laws and regulations. The TTV DVRS architecture/blueprint should not be restricted to specific component products, except to the extent that the capabilities and limitations of certain approaches may affect the ability to meet legal requirements.

The major factors driving the design are derived from the requirement to comply with the Help America Vote Act of 2002 (HAVA) requirements, as understood by the TrustTheVote Project. Specifically, the HAVA requirements for a uniform and centralized database to serve as the official list preclude solutions where information in county systems is simply exported to a central database, subsequent to data entry. Yet, the desire to minimize disruption to county business processes precludes any approach that requires initially replacing all existing county systems. So, integration with legacy systems and certain interfaces for the same are also a driving factor. Accordingly, there are four major aspects to the scope of the TTV DVRS project:

1. DVRS Database and Applications
2. Interfaces to external State agencies
3. Modifications to existing county election management systems (EMS)
4. Integration of DVRS with existing county EMS

Herein the descriptions of these aspects:

- **DVRS Database and Applications** – A new open source system solution (database and applications) to serve as the single, official statewide database of voter registration information. Additions or changes to voter registration (VR) records are to be captured as they are entered by state or county election workers. The database application will possess functionality for assigning unique identifiers, detecting duplicate VR records and detecting other types of validation errors. The database will have a user interface for SOS staff to configure and manage the application. The database will be designed and implemented for security appropriate to the sensitivity and privacy of the data. The database will provide complete logging and auditing capabilities, so that all changes to database content are recorded and traceable to the user or function that made the change.
- **Interfaces to External State Agencies** – The DVRS database will need to be connected to external state organizations, including typically the Department of Motor Vehicles (DMV), the Department of Health & Human Services (DHS), and the Department of Corrections and Rehabilitation (DCR) for voter registration identification and list maintenance purposes. These interfaces should be on-line or batch depending on the business function. Because many states are already doing so, the DMV (and through the DMV, the Social Security Administration (SSA)) interface for identification verification should be implemented using XML/SOAP. In many states the DHS, DCR, DMV, National Voter Registration Act (NVRA), and National Change of Address (NCOA) interfaces are

implemented to accept batch files provided by these external agencies. These interfaces can be replaced with interactive solutions, presuming the DVRS architecture/blueprint specifies all changes required on both sides of the interface.

- **Modification to Existing County (EMS or VR) Systems** – In most state implementations, the DVRS architecture/blueprints should assume that county workers will continue to perform most routine data entry and update functions for the processing of voter registration. The existing county EMS will either be adapted or replaced to ensure that county users interact directly with DVRS for all additions and updates to VR information. Updates to VR information may make use of the remediate screens in the county systems, but record updates need to be applied directly to the DVRS database. This will create an information flow wherein any change (i.e., add, change or deletion) to VR information will be applied directly to the DVRS database. Downstream systems, if any, (e.g., county level EMS) will obtain VR information from the DVRS system as the exclusive source. County systems, if used, that require VR information to be stored locally to operate should be adapted to ensure that all VR information is derived from the DVRS.
- **Integration of the DVRS with County Systems** – Middleware or other suitable technology may be used to facilitate connectivity between county systems and the DVRS and to support distribution over a wide area (potentially public) network.

The complete system will be designed and implemented to ensure a high level of availability, and the ability to handle anticipated workloads during periods of peak system usage. It is assumed that an adopting State's future business process will be largely similar to the current business processes. County users may need to adapt business processes to use common data definitions and code tables established by the State for VR information. County business processes may also need to be adapted to deal with exceptions that result from changes to VR information that are initiated within the DVRS database (e.g., assignment of unique number, detection of ineligible voter).

Business processes at the SOS should also remain largely similar to existing processes, but may need to be adapted to accommodate the new DVRS database as well as additional data and business process analysis and oversight. The State may also need to support new integration technologies introduced as a result of adopting the TrustTheVote Project open source DVRS.

3.3 Goals and Objectives

The goals for the TTV DVRS design solution are to [a] ensure that the adopting State's business needs are met and [b] that the HAVA statutory and operational responsibilities and requirements are achieved. In order for the TTV DVRS to bring an adopting State into full HAVA compliance, the DVRS must include the following characteristics:

- Serve as the single system for storing and managing the official list of registered voters throughout a state;
- Contain the name and registration information of every legally registered voter in the State;
- Contain a unique identifier for each legally registered voter in the State;
- Coordinate with other agency databases within the State (DMV, DHS, CDR, etc.)
- Allow any election official in the State, including any local election official, immediate online access to information in the statewide voter registration system;

- All voter registration information obtained by any local election official in the State will be digitally stored in the DVRS System on an expedited basis at the time the information is input by the local official;
- The chief State election official will provide such support as may be required so that the local election officials are able to enter information expeditiously; and
- Serve as the source for the official voter registration list for the conduct of all elections for Federal office in the State.

The TTV DVRS will allow adopting States to comply with HAVA general system requirements. Adopting State's counties will be required to modify their specific EMS and business processes in order to support this new system and comply with federal HAVA mandates[2].

The new DVRS will require immediate update of voter registration data in the central system as it is entered in the counties, which will improve the currency of data in the single database. List maintenance activities will be standardized to improve data accuracy as well. As new voter registration information is entered into the State system, the system will automatically detect duplicate voters and allow staff to update existing records and combine duplicate records as appropriate, reducing the percentage of duplicate/inaccurate records and preserving a voter's historical record in the database as a voter moves from county to county.

The new DVRS will automate the typical duplicate check function, using a unique identifier assigned every voter to detect duplicate records within the database whenever new data is entered. This functionality will standardize the removal of duplicate records from the system and improve data integrity.

3.4 Business Process Benefits

The TrustTheVote Project has identified three strategic benefits that can potentially be achieved by an adopting State through implementation of the TTV DVRS architecture/blueprint:

- Reduce state-wide costs for system support
- Provide flexibility to implement legal and business improvements; and
- Improve timeliness, accuracy, and availability of data and reports for state-wide use

The TTV DVRS will provide the business process as discussed in this section as well as meet the technical requirements in **Section IV**. All of the processes, functions, and requirements are mandatory for a comprehensive adoptable solution. Additionally, the proposed solution will meet all of the HAVA requirements. In summary, the DVRS will:

- **Implement a Single, Uniform, Official, Centralized, Interactive, Computerized List** — HAVA Section 303(a)(1)(A) requires that the State (through SOS) implement a computerized statewide voter registration list that is: single, uniform, official, centralized, interactive, defined, maintained and administered at the State level, and contains the name and registration information of every legally registered voter in the State.
- **Provide for Data Accuracy and Timeliness** — HAVA Sections 303(a)(2)(A) and 303(a)(4) requires the system to include provisions to ensure voter registration records are accurate and updated regularly. List maintenance shall be performed by "the appropriate State or local election official," in accordance with NVRA provisions.
- **Facilitate Removing of Ineligible Voters from the List** — HAVA Sections 303(a)(4)(A) and 303(a)(2)(A)(ii) require reasonable effort be made to remove ineligible voters from

[2] This is an incumbent requirement regardless of whether a State adopts the TrustTheVote open source solution or some other alternative.

the voter registration list. For removing ineligible voters from the list, the State shall coordinate with DMV for address changes, DHS for death notification and DCR for felony status.

- **Eliminate Duplicate Records and Ensuring Data Integrity** — HAVA Section 303(a)(2)(B) requires list maintenance will be conducted in a manner that insures all legally registered voters are in the computerized list; only voters not legally registered or not eligible to vote are removed from the list; and duplicate names are eliminated from the list. In addition, HAVA Section 303(a)(4) requires the State to employ safeguards to ensure legally qualified voters are not removed in error. List maintenance activities are to be conducted in accordance with NVRA provisions.
- **Assign a Unique Identifier** — HAVA Sections 303(a)(5)(A)(i) – (iii) require all new (and renewing) registrants to provide their driver's license number (DL#). If they have no DL#, they will provide the last four digits of their SSN (SSN4). If they have neither DL# nor SSN, the system will assign them a unique identifier to use as a voter registration ID number. No registration is valid unless/until the State verifies these ID numbers.

3.5 Required System Functionality and Constraint

This Section presents the vision for process and functionality of the TrustTheVote Project Digital Voter Registration System.

3.5.1 Summary

The TrustTheVote Project continues to meet with States' elections officials to continue the discovery of requirements for a base DVRS that can meet the majority of consensus needs for the States while supporting individual needs for State-specific requirements. Here is what we know to date, and anticipate the publication of this RFC will catalyze clarification from our Design Congress Stakeholder Community as well as the public interest at large.

The typical SOS is motivated to meet the HAVA Voter Registration Database (VRDB) requirement with an approach that features a functional centralized voter registration system in a hybrid environment. It is anticipated that Counties can participate using a modified version of their current EMS, or they may use a fully featured and integrated voter registration and election management application that is on the road map for the TrustTheVote Project.

3.5.2 County Systems

HAVA requires that SOS establish and maintain a single, statewide automated voter registration list. However, we've determined that most voter registration activities are and will remain the responsibility of county elections offices. Typical counties currently maintain independent voter registration databases that are usually part of more comprehensive EMS. In addition to voter registration, these systems provide functions that are inherently local, such as managing and verifying the eligibility of polling place workers. Moreover, these county EMS implementations vary in functionality, complexity and overall robustness as the county voting populations can vary from less than one thousand to several million.

In recent years, many SOS have achieved "interim compliance" with the HAVA voter registration requirement using a central database that accepts periodic uploads of data from each county system. For the TTV DVRS, to ensure HAVA compliance, SOS will likely require that the interface between a new centralized database and independent county EMS implementations be extended to upload new data such as voter registration card (VRC) images in order, for example, to capture new registrant signatures. Furthermore, the county systems will need to synchronize updates on an individual-record basis so that updates are not completed until a positive response has been received from the central database specifying a unique identification number (UID) to

be used for the new registration. Any potential duplicate records for the same voter in the DVRS will need to be identified for resolution as part of the process.

For counties that cannot continue to use – or choose not to use – their current EMS to integrate with the TTV DVRS, SOS offices TTV has worked with propose to acquire an optional, fully functional county EMS application that would integrate fully with the DVRS centralized database and would include all required local election management functionality, so that counties could migrate to the use of this system instead of their current environment. A new system, in design at the TrustTheVote Project, will provide the capacity and functionality to support counties in this manner. Timing for the TTV EMS project has not been finalized at this writing. And this RFC will be updated to reflect developments on that separate project.

3.5.3 Independent County EMS Support

For counties that continue to participate in a centralized database using their existing EMS, the DVRS central database system will need to provide support for data transfer and synchronization so that all records in the central database are fully standardized. The system will need to accept individual record add, delete and update transactions from each county EMS, and provide near-real-time response to the county system that the record was either accepted and loaded to the database, rejected for failure to meet data standards or verification requirements, or accepted with the requirement that the county address certain deficiencies in the record.

Any fatal or informational deficiencies found in the transactions will be clearly indicated to the county in the response sent to the county. Additionally, the system will be able to apply voter registration changes that do not originate within the county, such as re-registrations in another county or registration through the DMV motor voter program, and notify the county of such changes for automatic update in the county system or for county review and confirmation as appropriate, based on the confidence of the source transaction.

Wherever independent counties are required to interact with DVRS to process notifications or lists or to input data, DVRS may either provide a workstation browser-based interface, or may develop an integration with the independent EMS so that the function can be performed within the EMS. If a function is implemented through a browser interface, the DVRS will also need to provide an XML-based application programming interface (API) so that the independent EMS may independently integrate the function later.

DVRS will also need to generate all polling place rosters and supplemental rosters, and transmit those rosters in formats suitable for either local print by the counties or for use in electronic poll books. DVRS will need to accept and add relevant data received from the counties after each statewide or federal election to registrant voting participation histories.

The county EMS will be required by SOS to upload VRC and signature images with each registration record added or updated, in the format in which they are currently stored at the county; DVRS will need to convert those images as necessary.

Typically, it is envisioned that county EMS systems will create and store, and then periodically (e.g., monthly) upload an audit file to the State DVRS that records when each record was created, modified or deleted, the change made to the record, and the specific user or program, date and time of each change to any voter registration record. Finally, the DVRS interface to counties' election management systems should be implemented as a published, open XML-based format.

3.5.4 DVRS Processing and Functionality

3.5.4.1 Unique Identifier (UID)

DVRS will assign a UID for each new registered voter, and verify and assign a corrected UID for each re-registered voter if the existing UID does not comply with specified rules. The UID

will normally be a State's driver's license number or a State's Identification Card number, known collectively as the DL/ID. Under specified circumstances, the UID may be derived instead from name, date of birth (DOB), SSN4 and address information.

Before either a DL/ID or SSN4 may be used in the UID, those numbers will need to be verified against the DMV and/or the SSA ID validation system. In many States' it is understood this is an existing system, in some cases, using a real-time interactive interface based upon XML. In such cases, all business rules for matching against the DMV and SSA records should be implemented in the DMV/SSA validation system. The DVRS will need to generate a properly formatted query to the DMV/SSA validation system for each new or updated voter registration that does not include a UID based on a validated DL/ID. DVRS will need to accept and appropriately assign the UID based upon the response from DMV/SSA, which will indicate whether a voter-provided or found DL/ID or voter-provided SSN4 is to be used in the UID.

The method for generation of a UID that is not based on the DL/ID should be such that the registered voter can be identified as the same person when the voter re-registers, without requiring that the voter knows or provides that UID.

Only one valid voter registration record may be assigned any UID. When, during registration update or when a new registration appears to require the assignment of an existing UID to a new voter registration record, DVRS must recognize only one such record as valid, and will provide appropriate notifications to help SOS ensure that all such duplicates are resolved in a timely manner.

3.5.4.2. Voter Identity Matching

DVRS will likely receive identification information from a variety of sources, including new or updated voter registrations processed by counties from received VRC, DMV voter registration and address updates, NCOA files, DHS death notifications or county offices responsible for such vital statistics and death notices, local court conviction records, and DCR felon files. Each of these sources will contain different combinations of voter identification information (*e.g., name, address, date of birth, DL/ID, gender, SSN4*) and each source will vary in the reliability of the information.

DVRS will need to provide a highly accurate method of determining when the person described by the external information source matches an existing registered voter. DVRS will also need to provide the ability to identify existing voter registration records that may be for the same person even though they have been assigned different UIDs. Addressing this "exception handling" functionality is an open issue, but the TTV Project anticipates that the process might operate in the following manner:

- For each data value (*e.g., first name, date of birth, address*), SOS administrators would have the ability to specify one or more matching criteria (*e.g., first four characters match, all characters match exactly, all characters match exactly with one pair of characters transposed, etc.*); then
- SOS would assign a confidence level to groups of matching criteria (*e.g., first name, last name and date of birth*). SOS would then assign a threshold confidence level required for automatic and manual match processing for each identity matching function (*e.g., searching for existing registration records when processing a new VRC, matching death notices against existing registration records; searching for potential duplicate registrations within the system.*)
- Matches that meet the automatic confidence threshold would be processed without further operator action (*although a method would be needed to review and reverse such automatic actions.*) Matches that do not meet the automatic threshold but meet the manual threshold would be presented to the appropriate authorized state or county user for evaluation before application or rejection.

3.5.4.3 County Registration Processing

When a new voter registration or re-registration is processed by the county, the record will be sent to DVRS. The registration record may either be sent as an interactive transaction record from an independent county EMS or received directly from a States' EMS (and certainly the TTV Project EMS once built.)

For all registration processing, required notifications and confirmations sent to counties will support both digital messages to independent county EMS and direct communication to a States' EMS. Any EMS must include, and independent counties' EMS will need to be modified by their owners (hopefully through HAVA funding) to provide, mechanisms to correctly process and respond as required to these notices and confirmations.

DVRS will need to provide the ability to compare information from a new registration to existing records, and present a list, in order of match confidence, so that the authorized county user may accept an existing record for update, or may choose to add a new record. The unique

ID will need to be verified with DMV/SSA before either updating or adding a record. If an existing record is selected for update that causes the registration county to change, the prior county, if not using their State's EMS, will be notified to either cancel the record, or reject the update so that the new county creates a new registration instead.

Prior to sending any confirmation of new or updated registration, DVRS will need to attempt to match the new registration data to records in the cumulative ineligible felon and deceased files. If a record match meeting the automatic match threshold is found, the record will be cancelled in DVRS and notice sent to the new county and the prior county, if any, that the registration is cancelled. Both counties will need to have the ability to review and request reversal of cancellation, and SOS administrators will have the ability to review and resolve such requests. If a record match meeting the manual match threshold is found, notice will be sent to the new and prior county, if any, to review the record and either confirm or reject the match. If confirmed, the record(s) will be cancelled; if rejected, the new and existing records will be processed as if no match had been found. Any rejected match will be noted on the record to prevent the same match from being automatically applied again.

DVRS will need to support receipt of new or updated registrations from DMV in either a file or interactive format. Processing will proceed as above, and all notifications should be sent to the appropriate counties and not back to DMV.

3.5.4.4. Confidential Records

DVRS must provide secure support for confidential voter records under various statutes, where portions of the voter's record, such as address and telephone number are confidential. SOS usually require that confidentiality be implemented so that programs and users may access confidential data only with specific authority and with explicit direction. It is not acceptable to implement record confidentiality solely by applying a confidentiality attribute to the record; users and programs that are developed incorrectly or in ignorance of the confidentiality of a record should not be able to access or report confidential data.

3.5.5.5. External Interfaces

Many SOS will likely require that all custom interfaces be open and implemented using XML and Service Oriented Architecture principles, unless the interface partner (e.g., DMV, DHS,) is unable to support XML.

It is also known that in some cases, the interface to the DMV for DL# verification, and through DMV to the SSA for SSN4 verification, has already been developed and implemented using XML. Typically DMV (e.g., California) requires that only a single, SOS source use this interface. DVRS will require a service to accept verification transactions from the county EMS and route those requests to DMV and correctly process the responses. This service will need to

be implemented using secured communications with the county EMS. The service will also need to maintain detailed audit logs of each verification attempted and the result received, with the ability to search and view specific transaction records, and to generate specified summary reports.

States' DCR usually provide a monthly file of persons who have become ineligible to vote because they are incarcerated or paroled felons, and of those persons who have regained their eligibility at the completion of their sentence. DVRS will need to accept and apply this information to create a cumulative file of all currently ineligible felons.

States' DHS also typically provide a periodic list of residents who have passed on since the last report. DVRS will need to accept and accumulate this information for processing, so that a cumulative deceased file is maintained in DVRS.

The DVRS will need to include a service to compare the mailing addresses of registered voters to USPS NCOA data. All registered voters are to be checked against NCOA updates at least once each month. Depending on the confidence level established by the SOS for such matching, the system should automatically apply the match and notify the appropriate county, or shall generate a notice to the county of the potential match for review and resolution by county officials. The DVRS database system will also provide a mechanism for State administrators to monitor and follow-up on any unresolved felon, death and NCOA transactions sent to the counties for review and resolution.

3.5.5.6 List Maintenance

DVRS will need to provide the ability for SOS administrators to initiate a process to compare new or all records in a cumulative "felon file" or cumulative "deceased file" against all existing voter registration records. DVRS will need to automatically cancel, and send notice to the county of registration, when the automatic match threshold has been met. DVRS will also need to send a list of registrations in each county that meet the manual match threshold to the county so that the county may view the match and match confidence level. The county will need to have the ability to process the list so that each match is either accepted or rejected. If a match is accepted, the voter will be cancelled in DVRS and notice sent to the county; if the match is rejected, the record will be updated in DVRS so that the match can be bypassed in future checks.

DVRS will also need to provide the ability to search for *duplicate* voter registration records within the DVRS database. That process will allow the SOS administrator to trigger the process, set the match threshold for that process, and select whether to include or exclude records with validated UIDs. DVRS will then need to send a list of registrations in each county that meet the match threshold to the county with the earlier registration date for each match so that the county may view the match and match confidence level. The county will need to have the ability to process the list so that each match is either accepted or rejected. If a match is accepted, the records will be merged into the record with the latest registration date (*although if the record with the earlier registration data contains voting activity after the later registration date, the match would be suspended and the SOS administrator notified*).

3.5.5.7. Motor Voter Support

States have also suggested that DVRS will need to be designed to accept voter registration data from DMV using an XML service point-based interface. This interface must include all voter registration data as entered on a standard VRC card, plus a TIFF (or other agreed to file format) image of the VRC and a digitized signature. The system will need to attempt to match such registrations against existing voter registration records and to attempt to apply such registration changes, including assignment of a voter to a precinct based on the residence address, based on the general established business rules for processing new registrations and re-registration. Based on SOS established confidence levels for such matching, the system shall either automatically apply such registration transactions and send notices to the

appropriate counties of the registration addition or update, or the system shall send notice of the potential registration transaction for county review and resolution.

3.5.5.8. Public Website

DVRS will need to provide a public website that allows voters to verify the status of their voter registration, including political party affiliation and whether they are a permanent absentee voter. The system will be configured to establish a secure session with the user, request identifying information, and to report the registration status, county, precinct and voting location for that voter. The system will not respond with any private or identifying information.

States contacted have also suggested that DVRS will need to allow voters who have voted by absentee or mail ballot to determine the status of that ballot on an ongoing basis. The system will also need to allow voters who have cast a provisional ballot in an election to determine whether that provisional ballot has been counted and, if not, the reason it has not.

The DVRS public website shall be designed for full accessibility, and will comply at minimum with W3C Level 2 and relevant Americans with Disabilities Act (ADA) guidelines.

3.5.5.9. Images Support

More and more SOS requires that the system be able to capture, search, and retrieve VRCs via a standard web browser interface. The system shall store online for immediate retrieval all such VRC images. It is anticipated that counties will upload the VRC image for all VRCs received on an on-going basis after system implementation.

3.5.6. Additional Design Considerations

3.5.6.1. Continuity of Operations

In a time of heightened concerns about critical infrastructure and increasing demands on operational continuity where more and more public (government) services are going online, it of no surprise that all SOS require fault tolerance in design. Specifically, we find the SOS requires that the complete DVRS system, including all services provided to counties through the secure delivery of application and system data to the county demarcation, be designed so that no event or events with related cause short of a widespread disaster to the SOS facility shall interrupt the full system services to all customers for (on average) more than four (4) hours in any one event or over four (4) events in any six-month period.

To this end, "*widespread disaster*" generally means an event preventing human, power, or network access to at least two dispersed server sites as proposed. Accordingly, the complete DVRS system should be designed, developed, acceptance tested and made available so that recovery to full system functionality from any single-site event is complete in some agreed to amount of time pursuant to an agreed-to average service level agreement.

Another concern, aside from intervening conditions that could cause service disruption, is overload from normal operation caused by high service demands. This occurs particularly during election cycles near the registration deadline. DVRS design should carefully consider high demand availability and provide for scalable capabilities.

3.5.6.2. Security

Data should be encrypted whenever stored in non-volatile memory and whenever in transit over network links or through facilities not contracted directly to SOS (*e.g., public networks*). System access will need to support a requirement for two factors of identification, one of them requiring access to a specific location or possession of a physical object.

All access will need to be controlled so that users and administrators are assigned roles, and that the roles are associated with the rights and access privileges necessary for that role, with sufficient granularity that no user is assigned rights that the user does not need.

All backup copies of data, including images, will need to be encrypted. SOS tend to prefer that back ups be normally taken to spinning hard disk storage, and not to media intended to be portable.

With the exception of public web servers, no component of the system, including end-user workstations and printers should require Internet access for full functionality.

The DVRS system design should ensure that all server components will be configured to the minimum level necessary for their function, with all unnecessary programs and services removed. All servers will otherwise be hardened to industry best practices, and delivered with procedures for server hardening after system upgrade or replacement.

3.5.6.3. Archiving/Purging

DVRS will need to include a mechanism to purge and archive selected registrations records so that they are removed from the voter registration list, but so that the removed records may still be viewed and, if necessary, restored to the system.

3.5.6.4. Audit Logs

Every action that changes the contents of the database in any way should be logged so that the date/time, unique user and program function that made the modification can be identified. Audit logs should be maintained in perpetuity, so a mechanism will need to be provided to periodically purge the audit log and archive the purged logs to long term storage.

3.5.6.5. Access Control

All access to the system, for either administrators or end users, will need to be controlled by user ID and strong password authentication. And States are increasingly requesting that access control for users in the central environment be supported through a lightweight directory access protocol (LDAP) compatible directory.

Section IV
DVRS Functional and Technical Requirements

4.1 Introduction

The objective of this Section is to present the mandatory business and technical requirements that must be addressed by TrustTheVote (TTV) Project Digital Voter Registration System (DVRS). The tables in subsections **4.2** and **4.4** are the core elements of this RFC in addition to the business processes described in **Section III**.

4.2 Functional Requirements

This subsection contains the detailed **functional requirements** that Secretary of State (SOS) offices participating in the TTV Project are informing the OSET Institute will or should be required of a "best practices" DVRS to address the business processes in **Section III**.

Requirement #	Requirement Description
DVRS.F1	**General Features & Requirements**
1.1	DVRS must provide all county users with read-only access to the data for registered voters within other counties.
1.2	DVRS must provide the ability to update the voter registration data for voters within their county (except to move a matched voter from another county into the county).
1.3	DVRS must provide the ability for authorized SOS administrators to view and update all data provided by all counties.
1.4	DVRS must automatically send electronic notice to the appropriate county whenever SOS administrators make changes to a voter record.
1.5	DVRS must support an interface with independent counties that manage voter registration through their own election management systems (EMS). Where identified in specific business requirements, the interface must be interactive.
1.6	DVRS must provide documented application program interfaces for all end user functions.
1.7	Whenever processing requires a "notice" be sent to an independent county, that notice must be sent electronically and must include sufficient data for automatic processing and import of the data into the county EMS.
1.8	DVRS must be designed to permanently store all historic data on each registered voter. Where necessary for system performance requirements, the system may be designed to archive data for voters whose registration has been cancelled for more than ten years such that the data for those cancelled voters can still be retrieved and viewed by authorized SOS and county users.
DVRS.F2	**VOTER REGISTRATION: Registration Data**
2.1	DVRS must provide functionality that enables authorized county and state users to add new registered voters and to update data associated with existing registered voters.
2.2	DVRS must allow for capture and storage of voter names including the following discrete data fields: • Suffix (Sr., Jr., other generations);

	• First name (full or initial); • Middle name (full name or initial); • Full last name (can include hyphenated last name); • Previous name(s); and • Alternate name (such as hyphenated, two last names, multiple-word last names, etc.).
2.3	DVRS must generate and store a unique identifier (UID) for each registrant in accordance with the rules.
2.4	DVRS must capture and store historic data on voter residence, mailing address and domicile county, including beginning and ending effective dates of those addresses.
2.5	DVRS must provide for capture and storage of the following discrete data fields related to a registered voter's residence address: • House number; • House fraction number; • House number suffix (alphanumeric); • Two-digit pre-directional code (i.e. S., SW) *; • Street name (alphanumeric); • "Alias" street name (alphanumeric); • Type (i.e., Street, Road, Lane) *; • Two digit post directional code *; • Apartment or space number (alphanumeric); • Unit Type *; • City; • Zip *; • Zip plus four* (optional with respect to each voter); and • County NOTE: * indicates code must conform to USPS standards
2.6	DVRS 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 "2.5 MILES NORTH OF SKYLINE TAVERN, VERNONIA, OR" or "Mile Marker 38, Hwy 30").
2.7	DVRS must be able to capture and store a voter's "Mailing" and "Absentee" address using the following fields that can be used with mailing software: • Free-form data entry; • Fields long enough to meet US postal, foreign and military mail regulations; • Postal codes; • Country; and • Indicator of whether or not the mailing address is out of state.
2.8	DVRS 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, DVRS must be capable of handling voters without a date of birth.
2.9	DVRS must be capable of capturing and storing the following voter registration data: • Telephone number (up to four different numbers, including type and extension); • Gender; and • Email address.
2.10	DVRS must be capable of capturing and storing the voter's place of birth, both as free-form text and as user-defined codes (States' to provide).

2.11	DVRS must be capable of capturing and storing a voter's language preference, based on codes that can be defined and modified by SOS administrators. (Refer to Bidder's Library for current language codes.
2.12	DVRS must be capable of capturing and storing a voter's accessibility and assistance needs, based on codes that can be defined and modified by SOS administrators.
2.13	DVRS must capture, store and display the current status of any voter's registration, as well as historic changes in status, effective dates for such changes and reasons for the change. At a minimum, the status options must include: • Active; • Inactive; • Cancelled; • Pending; and • Declined
2.14	DVRS must store a voter's current and historic political party affiliation, if any, based on codes that can be defined and modified by SOS administrators.
2.15	DVRS must provide the ability to capture and store the following identification information for each registered voter in separate fields: • The voter's issued Driver's License or State Identification Card (DL/ID) number: • The DMV verification status of that number (i.e., verified, not-verified, or pending verification); and • If verified, the date verified.
2.16	DVRS must provide the ability to capture and store the following identification information for each registered voter in separate fields: • The last 4 digits of the voter's Social Security Number (SSN4), which must be accessible for input, query and reporting: • The Social Security Administration verification status of that number (i.e., verified, not-verified, or pending verification); and • If verified, the date verified.
2.17	DVRS 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 SOS administrators.
2.18	DVRS must determine and store, for voters who register by mail: • Whether or not the voter is a first-time voter, subject to the HAVA ID requirement (HAVA Section 303[b]); • Whether or not the voter has satisfied the ID requirement and, if so, how; and • If exempt from this requirement, the reason for that exemption.
2.19	DVRS must capture and store the current and historical voter registration affidavits for each voter. For each such affidavit, DVRS must capture the following discrete data: • Affidavit number; • Execution date (from the affidavit); • Date the affidavit was received; and • Effective date of registration of the affidavit.
2.20	DVRS must store and display the current and historic images of the full registration affidavit in ANSI/AIIM compatible format.
2.21	DVRS must be capable of displaying the current and historic images of the voter's signature independently from the affidavit.

2.22	DVRS must provide the ability to zoom into affidavit and signature images.
2.23	DVRS must capture and store information related to contacts and attempted contacts with the voter (voter visit to Election Office, phone calls, eMails, etc.).
2.24	DVRS must be capable of attaching and storing other images to a voter's record, such as letters received from the voter.
2.25	DVRS must provide the ability to capture, store and view comments and/or notes to a voter record using free-form text with a minimum of 1,024 characters. During the entry and editing of such notes, DVRS must display a prominent warning that any such notes are a matter of public record.
2.26	DVRS must allow multiple comments and notes to be stored for a single registered voter. Each note must have a creation date, County ID and User ID associated with it.
2.27	DVRS must retain historical registration data (e.g., residence address, registration status, partisan affiliation, home precinct and district assignment, etc.) such that processes and reports that are generated with an "as of" date correctly reflect the data applicable on the "as of" date.
2.28	DVRS must capture, store and manage data for confidential voters such that: • All such voters are required to provide a mailing address; • Such voters are automatically designated as permanent absentee voters; • All restricted information (residence address, phone number and eMail address) about such voters are not displayed unless the user has appropriate and sufficient permissions; • By default, any restricted information about such voters is not automatically included in any reports, queries or data extracts, and can only be included in such reports or data extracts by special action of users with appropriate and sufficient permissions; • Elections officials that create lists, rosters and data extracts from DVRS may optionally chose whether to exclude the voter, or to include the voter but print the mailing address or the word "confidential" for the residence address of such voters; and • The counts of such voters may be included in or excluded from statistical abstracts such as the Report of Registration, based on user selection report options.
2.29	DVRS must capture and store the legal basis for which a voter qualifies as confidential (e.g., "court ordered," "victim of domestic violence," and "public safety officer") based on codes that can be defined and modified by SOS administrators.
2.30	DVRS must capture and store the date of application for confidential status and provide the capability to automatically remove this status at the conclusion of the two-year period plus a user defined grace period if not renewed.
2.31	DVRS must provide the ability for State and county users to automatically generate notices to confidential voters that their confidential status will expire unless renewed.
DVRS.F3	**VOTER REGISTRATION: Registrant Search**
3.1	DVRS must allow an authorized user to query and locate an existing registered voter in the system for update using a variety or combination of criteria, including: • Full or partial first name; • "Smart name" variances on first name; • Full or partial middle name; • Full or partial last name; • Soundex variations on last name; • Full or partial residence address; • Full or partial mailing address; • Telephone number; • DVRS assigned UID; • DL/ID #;

	• Registration affidavit number; • SSN4; • Date of birth (DOB); • Place of birth; • Political party affiliation; • Precinct; and • Political district.
3.2	If DVRS finds more than one person during the search, DVRS must provide a list of voter records that meets the search criteria and allow the user to select a person from the list to display applicable detail.
3.3	DVRS must provide the ability for an authorized user to search and retrieve one or more registered voters by using wild card characters in one or more fields. For example: "Mil*" in the last name field to find all last names starting with "Mil". "*il* in the last name field to find all last names containing "il". "*ler" in the last name field to find all last names ending in "ler". "Mil*" in the last name field and "Har*" in the first name field to find records with last names starting with "Mil" and first name starting with "Har".
3.4	DVRS must accept queries from independent county EMSs to locate and view registrant records that meet specified criteria and must provide, in response, key data (e.g., UID, Registrant Name, Residence address, date of birth, etc.) for each record found that meets the search criteria.
3.5	DVRS must be capable of responding to requests from independent county EMSs for a specific registration record, providing all data associated with that registration record.
3.6	DVRS must provide visual warning to the user before initiation of a registrant search, if that search is likely to take longer than 60 seconds to complete. If more than one person is found during the search, the system must display a list of records that met the search criteria and allowing the user to select a person from the list to display applicable detail.
3.7	DVRS must allow an authorized user to view all data, including historic voting activity data, historic voting participation data, historic affidavit images and historic signature images for registrants that are registered in other counties.
DVRS.F4	**VOTER REGISTRATION: Registration Processing**
4.1	DVRS must capture and store all new voter registrations received from counties or other state agencies, *or* it must update existing registrations if there is a user-verified match.
4.2	DVRS must provide the ability for authorized users to search DVRS for potentially matching records in DVRS by providing the voter's name, DOB and, if provided, the DL/ID and/or SSN4. Prior to matching, DVRS must attempt to obtain a verified ID for the voter through the IDV process.
4.3	If an existing registration record is found for the voter, based on an exact match from the query, the existing record must be presented to the user for confirmation of the match and update of the existing registration record with the new registration information.
4.4	If DVRS cannot find an exact match to an existing record from the query, DVRS must present the user with a list of all existing records that match the record based on the established matching criteria and match threshold for this process so the user may select one for update. The data returned on each potential match must include an indication of the criteria used for the match and the associated confidence level for that criteria set.
4.5	DVRS must provide the user with a method to retrieve and/or view existing data on a potential matching existing registration to determine whether, in fact, the existing voter is the same person who is attempting to register. The retrievable/viewable data for the potential matching voter must include:

	• All data fields available on the voter registration affidavit; • Historic addresses associated with the voter; • Voting participation history for the voter; • Voter activity history for the voter; • Current and historic signature images for the voter; and • Current and historic affidavit images for the voter.
4.6	DVRS must prevent a *new* record from being *added* to the database with the same UID as assigned to another registration record.
4.7	DVRS must notify SOS administrators if the IDV verified DL/ID for a voter is associated with another registration record in the system and an authorized county user has determined is not the same voter.
4.8	DVRS must process transactions from independent county EMS containing new voter registrations and modifications to existing voter registration records, including: • Voter registration data as specified in the DVRS data standards, • Affidavit images; • Signature images; • Voting activity history; and • Voting participation history.
4.9	DVRS must allow authorized county users the ability to enter and refuse registration to a voter who has not signed the voter registration affidavit. DVRS must note in the voter's record the basis for refusal of registration.
4.10	DVRS must validate all new registration records (including re-registrations) to verify they meet legal requirements for voter registration, including: • Valid date of birth • An SOS administrator configurable minimum age at time of registration; • Permanent residence or domicile within the State; and • US Citizenship.
4.11	New voter registrations that do not pass the required validation criteria and result in "Fatal Errors" must be accepted but suspended with a "pending" status until required information is secured and provided, and DVRS must note in the voter's record the basis for the suspense of registration. Electronic notice of the "pending status" and the basis for that action must be provided to the appropriate county. (Voters with a pending status are ineligible to vote.)
4.12	DVRS must provide electronic notice to the county on the suspension of new or modified voter registration data on the basis of an IDV finding of a SSN4 "single match – deceased."
4.13	New registrations that pass validation requirements but do not meet established data standards or have other non-fatal errors must be accepted into the system, but the record must be flagged for needed correction and electronic notice of the data deficiency provided to the appropriate county.
4.14	DVRS must verify that the new or reregistered voter has been assigned to a valid home precinct. Voters that have not been assigned to a valid home precinct must be flagged for county follow-up and resolution, and an electronic notice sent to the appropriate county for investigation.
4.15	DVRS must provide a function to certify address validity to USPS CASS standards. DVRS must provide and confirm all effective mailing addresses to United States Postal Service (USPS) Coding Accuracy Support System (CASS) standards.
4.16	DVRS must flag the voter's record to indicate that the voter must present identification

	the first time the voter votes in a federal election if: • The registration is for a voter that has not previously voted in a federal election in the State, *and* • The voter registered by mail *and* • The system could not verify a DL# or SSN4 for the applicant *and* • The voter is not registered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) and • The voter in not entitled to vote other than in person under federal law.
4.17	DVRS must compare all newly registered voters against historic death records in the system. If a potential match is found based on matching criteria established by SOS, DVRS must automatically flag the record as potentially deceased and send an electronic notice to the appropriate county.
4.18	DVRS must compare all newly registered voters against historic felon records in the system. If a potential match is found based on matching criteria established by SOS, DVRS must automatically flag the record as a potentially felon and send an electronic notice to the appropriate county.
4.19	Upon acceptance of a voter registration, DVRS must: • Set the voter's status to "active"; • Establish the voter's effective date based upon business rules established by the Secretary of State; • Flag the record for generation and mailing of a Voter Notification Card (VNC); • Send electronic notice to the appropriate county of the acceptance of the new registration and provide the county with the UID established for the voter; • Send electronic notice to the county of any non-fatal errors with the registration record; • Send electronic notice to the county that the voter must be contacted if the UID assigned is not based upon either the DL/ID or SSN4 provided by the voter and one or both was provided, or if the UID assigned is based upon a DL/ID and none was provided; and • If the registration is a re-registration where the voter has moved to a new county, DVRS must send electronic notice to the previous county of the voter's move to a new county.
4.20	DVRS must send electronic notice to a county when a new voter has been registered in that county from other sources (such as DMV), or when a voter in another county has moved into that county.
4.21	DVRS must provide the ability for the county, when it receives notice that a voter has been moved out of that county, to review relevant data regarding that transaction and to confirm the change or reverse the change, forcing separate registration records.
4.22	DVRS must provide the ability to accept modifications received from counties to existing voter registration data, such as: • Error corrections; • Change in partisan affiliation; • Change in voter status; and • New Voter activity history entries, such as mailing of address verification notices to registrant or receipt of permanent absentee application.
4.23	After acceptance of registration (or re-registration), DVRS must attempt to locate existing records for the voter based on the established criteria for such matching. If DVRS finds such a record(s), DVRS must notify the appropriate county for the potential pre-existing record for review and resolution of the potential re-registration.

DVRS.F5	VOTER REGISTRATION: ID Verification
5.1	DVRS must support the existing DMV ID verification (IDV) interface on a transactional basis. (States to provide specifications).
5.2	DVRS must, for all new registrations and re-registrations, automatically submit the voter name, date of birth and any provided DL/ID and/or SSN4 for validation from DMV or the Social Security Administration through the IDV interface.
5.3	DVRS must automatically assign the voter a unique ID (UID) based on the DL/ID if: • IDV verifies the provided DL/ID as an exact match, *or* • IDV identifies a DL/ID as a single exact match when no DL/ID was provided, or when a different DL/ID was provided.
5.4	DVRS must automatically generate a unique ID (UID) for the voter based on the SSN4 if: • The IDV verifies the SSN4 as a single exact match or multiple exact match, and • The IDV does not identify a DL/ID as a single exact match when no DL/ID was provided.
5.5	DVRS must automatically generate a unique ID (UID) for the voter based upon an SOS-approved algorithm, if the IDV is unable to either match the provided DL/ID or SSN4 or identify a single exact match to a DL/ID.
5.6	When DVRS generates a UID that is not based on the DL/ID, the algorithm must ensure that if the voter reregisters at a later time with the same information, the system will generate the same UID or base number for the UID.
5.7	When DVRS validation cannot be completed at time of entry due to DMV/SSA verification system unavailability, the record must be saved with a generated UID. DVRS must automatically retry an incomplete ID verification, and if a DL/ID or SSN4 is verified for the voter, the DVRS must: • Reassign an appropriate UID to the voter; • Notify the county of the change in the voter's UID; and • Identify any potential pre-existing records for that voter and provide electronic notice of the potential match to the county of the pre-existing record(s).
DVRS.F6	**VOTER REGISTRATION: "Motor Voter"**
6.1	DVRS must receive new voter registration data and voter registration address change data, including digitized signature images, from the DMV in accordance with the National Voter Registration Act (NVRA)
6.2	DVRS must attempt to match DMV voter registration change of address (COA) and new registration transactions against existing voter registration records using matching criteria established by the SOS.
6.3	For matches of DMV COA and new registration transactions against existing voter registration records that meet or exceed the established confidence threshold, DVRS must automatically: • Update the existing voter registration record with the new voter registration data received from DMV; • Reassign the voter to the appropriate county; • Update the voter activity history with the basis for registration changes; • Flag the voter's record for automatic generation of a VNC; and • Send an electronic notice to the appropriate county(s) of the registration change.
6.4	For matches of DMV COA and new registration transactions against existing voter registration records that do not meet the established confidence threshold, DVRS must

	automatically: • Send an electronic notice of the potential match and address update for the pre-existing voter registration record to the appropriate county for follow-up and determination if the potential match is valid; and • Update the voter activity history of the potential registration change/match from DMV.
6.5	When a county verifies that a pre-existing voter registration record matches the new DMV registration or COA transaction, DVRS must: • Record that information, including the basis for determination, in the voter activity history of the matched voter; • Update the voter's registration record with the new address from the DMV COA transaction; • Reassign the voter to the appropriate county; • Flag the voter's record for automatic generation of a VNC; and • Send an electronic notice to the appropriate county(s) of the registration change.
6.6	If a county determines that the potential match of DMV COA transaction against a pre-existing voter registration record is not valid, DVRS must update the voter activity history accordingly to indicate the determination that the DMV COA transaction was not associated with the voter and the basis for that determination.
6.7	When a new DMV registration does not match any existing voter registration records, DVRS must: • Create a new voter registration record for the voter; • Update the voter registration with the method of registration; • Flag the voter's record for automatic generation of a VNC; and • Send an electronic notice to the appropriate county(s) of the new registration.
6.8	When a DMV COA transaction cannot be matched against any existing voter registration records, DVRS must send electronic notice of the unresolved transaction to the appropriate county for follow-up investigation.
6.9	When a county determines that an unresolved DMV COA transaction cannot be matched against any existing voter registration records, DVRS must flag the DMV COA transaction as a "Non-Match," requiring notice to be sent to the potential voter in the DMV COA transaction.
6.10	DVRS must allow SOS administrators to record whether or not a county wants the SOS to mail notice of DMV COA transaction failures.
6.11	DVRS must allow SOS administrators to generate a data extract on a batch basis so that a third-party mailing house can print the notice of a DMV COA transaction failure.
6.12	DVRS must automatically note in a voter's activity history when a notice of DMV COA transaction failure has been generated by DVRS for that voter.
6.13	DVRS must be capable of receiving electronic notice from a county that the county has generated and sent a county generated written notice to a voter that their DMV COA update was unsuccessful.
DVRS.F7	**VOTER REGISTRATION: Voter Notification Cards (VNC)**
7.1	DVRS must provide the ability for SOS administrators to define and modify the format and content of the VNCs. the VNCs must include the following data: • Full name of the voter; • Mailing address of the voter; • Partisan affiliation of the voter; and • Effective data of registration (or registration change).

7.2	DVRS must provide the option to include the following data on the VNC: • Assigned precinct; and • Assigned US Congressional, State Legislature, State Positions defined on a State-by-State basis.
7.3	DVRS must have the capability to receive and apply electronic notice from an independent county EMS that a VNC has been sent to a voter.
7.4	DVRS must provide electronic notice to the independent county when a VNC has been generated for a voter by the State.
7.5	DVRS must provide the ability for authorized SOS administrators to generate printed VNCs for all newly registered voters in any or all counties, and all voters in any or all counties whose registration has been updated with a change in name, address, partisan affiliation, precinct assignment or political district assignment.
7.6	DVRS must have the capability to automatically generate a data extract of all required information across the State on a batch basis so that VNCs can be printed by the State through a third-party mailing house.
7.7	DVRS must provide the ability for authorized county users or SOS administrators to confirm that a VNC has been successfully printed for a voter, so that DVRS can provide the option to prevent printing of duplicate VNCs.
7.8	DVRS must provide the ability for authorized users to reprint VNCs on an individual or group basis when necessary.
DVRS.F8	**VOTER REGISTRATION: Synchronization for Independent Counties**
8.1	DVRS must provide the ability to compare a list of unique voter registration UIDs and associated voter registration status from an independent county with the data in DVRS and identify differences.
8.2	DVRS must provide the ability for an independent county to generate an electronic list of voter registration records for that county in the DVRS database for comparison and synchronization with voter registration records in the county EMS.
DVRS.9	**LIST MAINTENANCE: General**
9.1	DVRS must provide the capability for SOS administrators to track, by county and issue, unresolved voter registration and list maintenance issues, including: • UID assignment issues; • Fatal errors with voter registration; • Non-fatal errors with voter registration, such as data format errors or precinct errors; • Potential duplicate registrations; • Potential matches with death records; • Potential matches with felon records; • Potential matches with NCOA records; and • Potential matches with DMV COA transactions and registrations.
9.2	Whenever duplicate registrations are confirmed for the same voter, whether through the process of duplicate matching or registration processing, DVRS must: • Effectively merge the registration records into a single registration record, including voter activity history and voting participation history into the record with the most recent date of registration (or voter registration update activity); and • Automatically send an electronic notice to the county(s) whose voter records have been reassigned or merged with the newest registration record.

9.3	Should it subsequently be determined that registration records were incorrectly merged into a single record, DVRS must permanently provide SOS Administrators and authorized county users with the capability to "un-merge" such records into separate registration records and appropriately apply UIDs to the voters.
9.4	DVRS must provide electronic notice to counties of applied changes to the DVRS voter registration data that originate outside of the county (such as applied death record, State mailed Residency Confirmation Postcard (RCP) or State mailed VNCs).
9.5	DVRS must send electronic notice to counties of recommended changes to the county's registered voters for county research and determination (such as potential duplicate registrations identified, potential NCOA updates, potential death record matches, and potential address corrections).
9.6	DVRS must record in a voter's activity history the effective date of cancellation of a voter's registration and the basis for that cancellation.
9.7	DVRS must allow authorized SOS Administrators the capability to designate and modify the content and format of: • Notice of DMV COA transaction failure; • Pre-Election Residence Confirmation Postcards (RCPs); • Alternate Residence Confirmation Postcards (ARCP); • Change of Address Notification (CAN) (all forms); and • NVRA 8(d)(2) notices.
9.8	All DVRS generated notices must be bar-coded to facilitate the ready identification of the voter and expedited processing of a returned notice.
DVRS.F10	**LIST MAINTENANCE: Record Matching**
10.1	DVRS must include a user-configurable method for authorized SOS administrators to: • Establish sets of registration record matching criteria; • Configure which criteria apply to each type of matching function (e.g., new registration matching, death record matching, NCOA matching, etc.); • Assign "confidence" levels to each criteria set as it applies to each matching function; and • Establish threshold confidence levels required for manual or automatic application of matches for each matching function.
10.2	DVRS must provide the ability for SOS administrators to establish one or more basis for matching data in a registration record field, including (where applicable): • Exact character match; • First "X" characters of the field (where "X" is user configurable); • Same characters and order in string, but with spaces and punctuation removed; • Soundex match (or alternative method based on phonetic pronunciation); • "Smart-names" match based on common variations of First Name established by SOS administrators (e.g., Robert = Bob, Bobby, Rob); • "X" matching characters within string; and • Same month and year
10.3	DVRS must provide the ability for SOS administrators to identify a set of matching criteria based on combinations of individual field match settings, such as: • First Name- with "Smart-names"; Last Name- first 4 characters; and Date of Birth- same day and month or • DL/ID#- exact match; First Name- with "Smart-names".

10.4	DVRS must provide the ability for SOS administrators to configure and update whether or not an established matching criteria set is applied to each matching function, including: • New & updated voter registration; • Duplicate registration checks; • NCOA processing; • DMV Motor Voter processing; • Death record matching; and • Felon record matching.
10.5	DVRS must provide the ability for SOS administrators to individually establish "confidence" values to each established matching criteria set as it applies to each potential matching function.
10.6	DVRS must provide the ability for SOS 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" threshold, DVRS must generate electronic notices to the appropriate county for match review and resolution.
10.7	For high-confidence matches that exceed the established threshold for automatic application of the match, DVRS must provide the capability for SOS administrators or authorized county users to configure so that the system, for that county, either: • Automatically applies such registration changes and sends electronic notice of the change to the county; *or* • Applies such a change, but when the change would cause an existing voter registration to be cancelled, does not actually cancel a voter's registration until the change has been accepted by that voter's county.
10.8	For matches of registration records (e.g., existing/duplicate registration, death records, felon records, DMV COA, NCOA, etc.) that meet or exceed the established confidence level for automatic processing of that match function, DVRS must either apply the match and send electronic notice to the appropriate county of that transaction, or must provisionally apply that match until accepted by the county, for matches of registration records (e.g., existing/duplicate registration, death records, felon records, DMV COA, NCOA, etc.) that meet or exceed the established confidence level for automatic processing of that match function.
10.9	For matches of registration records (e.g., existing/duplicate registration, death records, felon records, DMV COA, NCOA, etc.) that meet or exceed the established confidence level for automatic processing of that match function, DVRS must send electronic notice to the appropriate county for review and resolution for matches of registration records (e.g., existing/duplicate registration, death records, felon records, DMV COA, etc.) that do not meet the established confidence level for automatic processing but meet the established minimum confidence level of that match function.
10.10	DVRS must provide the capability for authorized county users to cancel match-based transactions that have been automatically applied, or to not accept such automatic transactions. In such instances, DVRS must reverse any changes that have been applied to the record and handle the transaction as a confirmed non-match for that process.
DVRS.F11	**LIST MAINTENANCE: DHS Death Records**
11.1	DVRS must have the capability to receive the Department of Health Services (DHS) new death records file, as well as to store such records on an ongoing basis.
11.2	DVRS must match all new death records received from DHS against existing voter registration records to identify existing voters that may have died.

11.3	For matches with new death records that meet or exceed the established confidence threshold, DVRS must automatically: • Cancel the voter's registration; • Record the basis for that cancellation in the voter's activity record; and • Send an electronic notice to the appropriate county of the cancellation and its basis.
11.4	For matches with new death records that do not meet the established confidence threshold, DVRS must automatically: • Note the potential match in the voter's record; and • Send electronic notice to the appropriate county of the potential match for investigation and resolution.
11.5	DVRS must provide the ability for an authorized county user to enter its determination that the match is valid into the voter's record and cancel registration of the voter.
11.6	DVRS must provide the ability for an authorized county user that has investigated and determined that the match was invalid to note that determination in the voter's record and remove the indication that the voter is potentially deceased from the voter's record.
11.7	When counties cancel a voter's registration by reason of death from information received locally within the county, DVRS must automatically add that information to the historic death records stored within DVRS.
11.8	DVRS must permanently provide SOS administrators and authorized county users with the capability to undo death record matches that have been applied to a voter.
DVRS.F12	**LIST MAINTENANCE: DCR Felon Data**
12.1	DVRS must have the capability to receive the Department of Corrections and Rehabilitation (DCR) new felon records file, to store such records on an ongoing basis, and to remove the record when notice of completed sentence or parole has been received.
12.2	DVRS must match all new felon records received from DCR against existing voter registration records to identify existing voters that may have become ineligible due to imprisonment.
12.3	For matches with new felon records that meet or exceed the established confidence threshold, DVRS must automatically: • Cancel the voter's registration; • Record the basis for that cancellation in the voter's activity record; and • Send an electronic notice to the appropriate county of the cancellation and its basis.
12.4	For matches with new felon records that do not meet the established confidence threshold, DVRS must automatically: • Note the potential match in the voter's record; and • Send an electronic notice to the appropriate county of the potential match for investigation and resolution.
12.5	DVRS must provide the ability for an authorized county user to enter its determination that the match is valid into the voter's record and cancel registration of the voter.
12.6	DVRS must provide the ability for an authorized county user that has investigated and determined that the match was invalid to note that determination in the voter's record and remove the possible felon flag.
12.7	When counties cancel a voter's registration by reason of felony conviction and sentencing from information received locally within the county, DVRS must automatically add that information to the current felon records stored within DVRS.
12.8	DVRS must permanently provide SOS administrators and authorized county users with

	the capability to undo felon record matches that have been applied to a voter.
DVRS.F13	**LIST MAINTENANCE: Duplicate Identification**
13.1	DVRS must provide the ability for SOS administrators 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.
13.2	DVRS must automatically 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 level threshold. DVRS must then automatically send an electronic notice to the county(s) whose voter records have been reassigned or merged with the newest registration record.
13.3	DVRS 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, DVRS must send electronic notice of potential match to the appropriate county(s) as indicated following in requirement 13.4.
13.4	DVRS must generate electronic notice of potential duplicates to the county(s) with the older date(s) of registration for identified potential duplicate matches that do not meet the established confidence threshold. The notice must include, for each potential registration record in the duplicate set, the following: • Registrant name; • Date of birth; • UID; • Date of registration; and • Basis of match.
13.5	DVRS must flag potential duplicate records that have been verified as not being duplicates so they are no longer reported as unresolved potential duplicates, so that they may be omitted as potential duplicates in subsequent duplicate checks.
13.6	DVRS must provide the ability for authorized SOS users to remove flag(s) that indicate two registrations are not actually duplicate records for the same voter.
DVRS.F14	**LIST MAINTENANCE: NCOA**
14.1	DVRS must provide the ability to compare and match voter registration addresses against the USPS National Change of Address (NCOA) data, identifying registrants who have changed their mailing address.
14.2	DVRS must provide the ability to automatically apply NCOA matches to voter registration records when a predefined confidence level of match is met.
14.3	DVRS must send an electronic notice to the voter's county of all NCOA potential matches that fall short of the threshold confidence level established for automatic matching.
14.4	DVRS must provide the ability for authorized county users to update the voter record on whether the match was valid or invalid.
14.5	DVRS must retain all potential NCOA matches until the county jurisdiction has applied or discarded the matched new address.
14.6	When a NCOA match has been determined to be valid where a voter has a forwarding address in the same county, DVRS must automatically: • Update the (residence or mailing) address of the registrant; • Note in the activity history for that registrant that the record was updated because of NCOA match; and • Flag the record for automatic generation and mailing of a Change of Address Notification (CAN)

14.7	When a NCOA match has been determined to be valid where the voter has a forwarding address in a different county or outside the State, DVRS must automatically: • Change the status of the registrant to “inactive”; • Note in the activity history for that registrant that the record was updated because of NCOA match; and • Flag the record for automatic generation and mailing of a CAN
14.8	When a NCOA match has been determined to be valid where the voter has no forwarding address, DVRS must automatically: • Change the status of the registrant to “inactive”; • Note in the activity history for that registrant that the record was updated because of NCOA match; and • Flag the record for automatic generation and mailing of a CAN
DVRS.F15	**LIST MAINTENANCE: Pre-Election Residency Confirmation Postcards (RCPs)**
15.1	DVRS must provide the ability for SOS administrators to generate pre-election residency confirmation postcards (RCPs) to all active registered voters that have not voted in an election within the past six (6) months in any or all counties at least 90 days prior to a primary election.
15.2	DVRS 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 RCPs can be printed by the State through a third-party mailing house.
15.3	DVRS must provide the ability for authorized SOS administrators to define and modify the format and content for the RCPs.
15.4	DVRS must automatically note in a voter’s activity history when an RCP has been generated.
DVRS.F16	**LIST MAINTENANCE: Change of Address Notification (CAN)**
16.1	DVRS must provide the ability for SOS administrators to automatically generate a data extract of all required information for one or more counties across the State on a batch basis so that CANs may be printed by the State through a third-party mailing house.
16.2	DVRS must automatically generate the appropriate CAN notice for each voter depending on whether the voter has a forwarding address within the county, a forwarding address outside the county, or no forwarding address.
16.3	DVRS must automatically note in a voter’s activity history when a CAN has been generated for that voter.
DVRS.F17	**VOTER ELECTION DATA: Official List of Voters**
17.1	DVRS must provide the ability to generate the official list of eligible registered voters with respect to any given election based on business rules (i.e., 18 years of age on election day, effective date of registration at least 15 days prior to election day, registration status active or inactive).
17.2	DVRS must provide the ability for authorized independent county users to export the official list of registered voters with respect to any election.
17.3	DVRS must provide the ability to import and apply the voting precinct assignment for each registered voter for a given election from the independent county EMS.
17.4	DVRS must provide the ability for counties to generate and locally print precinct rosters (and supplemental rosters) either as indices or as roster indices for each voting precinct from DVRS. Each roster must be printed in one or more (up to 3) accepted formats as defined by the SOS administrator, and must include the following information for each

	voter: • Voter full name; • Voter residence address; • Voter telephone number; • Signature image (at county option); • Voter UID (in bar-coded format only), • Indication if the voter is required to provide identification as a first-time voter who registered by mail; • Voter status (active or inactive); • Ballot style; • Partisan affiliation (primary elections only); and • Indicator if voter has already voted or been assigned a ballot (early or absentee voting).
17.5	DVRS must provide the ability for counties to extract the required data to locally generate and print precinct rosters and supplemental rosters in an alternate format, or to import into an electronic poll book application.
17.6	DVRS must provide the ability to record when voters have been included in a printed roster so that they may be excluded from the subsequent generation of supplemental rosters.
DVRS.F18	**VOTER ELECTION DATA: Voter Participation History**
18.1	DVRS 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: • State defined code for the election; • Election date; • How voted (absentee, early, polling place, or provisional); and • Partisan ballot voted (for primary elections).
18.2	DVRS must automatically clear the indicator in a voter's record requiring the voter to provide ID the first time the voter votes in a federal election based on voting participation history received from a county indicating that the voter has voted in a federal election.
18.3	DVRS must provide the ability to import and apply voter participation history from independent county EMSs after each election, recording each voter that voted in the election and the method of participation (early, absentee or in person).
DVRS.F19	**VOTER ELECTION DATA: Absentee Voting**
19.1	DVRS must record and track current and historic absentee voting status of each voter, including: • Type of absentee: *one-time*, *special absentee* (military and overseas), *permanent absentee*, and *all-mail precinct*; • Type of application (State defined such as on-line, federal form, sample ballot return application, etc.); • Date application received; • Source of the application (how received); • Whether or not the application was approved or denied; and • If denied, the reason for the denial.
19.2	DVRS must be capable of capturing, storing and reporting the following information related to every election:

	• When a voter was mailed an absentee ballot; • When the ballot was received by the elections official; • Whether the ballot was accepted or rejected; and, • If rejected, the reason for that rejection.
19.3	DVRS must permanently retain all historic information related to absentee voting by a registered voter.
19.4	DVRS must provide the ability to import and apply the status of each absentee ballot with respect to each absentee voter, including: • When a voter was mailed an absentee ballot; • When the ballot was received by the elections official; • Whether the ballot was accepted or rejected; and • If rejected, the reason for that rejection.
DVRS.F20	**VOTER ELECTION DATA: Provisional Voting**
20.1	For voters who vote a provisional ballot in an election, DVRS must be capable of capturing, storing and reporting whether or not the provisional ballot was counted and, if not, the reason it was not counted
20.2	DVRS must provide the ability for SOS administrators to configure the reason codes for rejection of a provisional ballot.
20.3	DVRS must provide the ability to import and apply the status of each provisional ballot cast in an election, including the reason for rejection of each provisional ballot not counted.
DVRS.F21	**PRECINCTS AND DISTRICTS: Precinct – District Mapping**
21.1	DVRS must require and store each voter's current and historic home precinct assignment.
21.2	DVRS must be able to identify, from the voter's home precinct, the voter's voting district for US Congress, State legislature(s), municipality of residence if a voter is entitled to vote in that municipality, or if not, that voter resides in the county's unincorporated area.
21.3	DVRS must allow counties to define additional local election districts (e.g., school districts and water boards) and must automatically identify and report a voter's residence within such districts based on voter's "home precinct" assignment.
21.4	DVRS must detect "orphan voters" who do not have a valid home precinct assignment and "orphan precincts" that are not assigned to the required State legislature(s), County Supervisory, and municipality/unincorporated area districts.
21.5	DVRS must provide the ability to accept and apply political district and precinct data from independent counties so that DVRS contains a replica of the political district and precinct data maintained in the independent county EMS. The replica must be stored in a standard format for DVRS so that DVRS can determine the political district memberships for each registered voter.
21.6	DVRS must provide the ability to accept and apply batch updates of voter registration data from independent counties for specific global data updates (e.g., reassigning home precincts) after authorization by SOS administrators.
21.7	DVRS must detect and notify the independent county and SOS administrators if changes in political district or precinct data have created orphaned voters, precincts or political districts (i.e., voters without a home precinct or without required political district assignments and home precincts without required political district assignments).
21.8	DVRS must provide electronic notice to the county of invalid changes to precinct and political district data that have been submitted to DVRS by the independent county.

21.9	DVRS must provide the ability for SOS administrators to track unresolved errors with county submitted changes to the precinct and political district data.
21.10	DVRS must provide the ability for independent county users to review and export the precinct and political district data stored within DVRS for that county.
DVRS.F22	**ELECTION MANAGEMENT: Absentee & Mail Ballot Management**
22.1	DVRS must provide SOS administrators with the capability to define and modify the reasons for rejecting absentee and mail ballots and the associated reason codes.
DVRS.F23	**SOS PROCESSES: Political Party Tracking**
23.1	DVRS must allow SOS administrators` to define political parties. For each such party, the system must track and report the following information: • SOS assigned party code; • Whether or not the party is Qualified, Attempting to Qualify, or Non-Qualified; • Date of all changes in party status (Qualified/Non-Qualified/Attempting to Qualify; • Reason for such changes (if applicable); and • Current state party contact information.
DVRS.F24	**SOS PROCESSES: Registration Report (RR)**
24.1	DVRS must generate and print the Report of Registration (RR) in the currently established format
24.2	DVRS must provide the ability for each county to indicate to the system that they have completed entry of all voter registrations applicable to a specific RR.
24.3	As of a user-specified date, DVRS must calculate and report the number of active registered voters by county and political districts (Congressional, State legislature(s), incorporated City and County districts) within the county. The registration totals must be broken down by qualified political party affiliation within each district.
24.4	DVRS must provide the ability for SOS administrators to define and modify the format and content of the RR reports. DVRS must generate each finalized RR in .PDF, MS Excel and tab-delimited text file formats
24.5	DVRS must calculate and report the number of active registered voters by county that are affiliated with each party attempting to qualify as of a specified date.
24.6	DVRS must provide the ability for authorized SOS administrators to input and store the estimated number of persons “eligible to register to vote” for each county as of a specified date for each RR and keep the data permanently.
DVRS.F25	**SOS PROCESSES: Voter Information Guide (VIG)**
25.1	DVRS must generate State “ballot pamphlet” or Voter Information Guide (VIG) mailing lists of registered voters eligible to vote in an upcoming election that meets the established specifications for this mailing list.
25.2	DVRS must capture and store a voter’s request to not be mailed the VIG. DVRS must automatically exclude all voters who have so “opted out” from any VIG mailing lists generated.
25.3	DVRS must “household” the mailing list files so that if multiple registered voters with the same last name and language preference reside at the same address, DVRS only generates one mailing label for that address/language preference that is addressed to “ [last name] Residence.”
25.4	DVRS must generate the mailing list so that all addresses in the mailing list conform to US Postal Service standards and the list is presorted to obtain bulk-mailing rates.

25.5	DVRS must identify any registrants with a mailing address that could not be made to conform to the established USPS mailing standards. Such registrants must be excluded from the State VIG mailing lists and electronic notice must be provided to the appropriate county of the address deficiency for county correction and mailing.
25.6	DVRS must update the voter activity record for each voter for whom a VIG address label (individual or household) was generated, indicating the date that label was generated.
25.7	DVRS must provide the ability for SOS administrators and authorized county users to generate mailing lists (or extracts of data for mailing lists) for all eligible registered voters that were not included in the State VIG mailing, including voters: • With a mailing address outside of the State; • Whose address could not be normalized to the established standards; or • Are eligible to vote in the upcoming election but have an effective date of registration after the election
25.8	DVRS must update the voter activity history for each voter when a county has generated a VIG mailing label for that voter.
DVRS.F26	**SOS PROCESSES: Public Voter Registration Data Requests (PVRDR)**
26.1	DVRS must allow authorized SOS administrators and authorized county users to input, track and review Public Voter Registration Data Requests (PVRDRs), including: • Requestor name; • Requestor organization; • Requestor residence and business addresses; • Requestor contact information (phone, fax, email addresses); • 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; • Requestor's stated purpose/use for the data; • Date of application; • Date application received; • Basis for qualification (election, party, academic, journalist, etc.); • Date of application fulfillment or denial; • Status of application; • Criteria used to select/exclude records for the extract; and • Filename(s) and number of records provided in the extract.
26.2	DVRS must allow authorized SOS administrators and authorized county users to log the date, time, and administrator ID of activities and events related to processing and fulfillment of a PVRDR
26.3	DVRS must provide authorized SOS administrators and authorized county users with a method to select voter registration records for inclusion or exclusion in a PVRDR extract based on multiple criteria, with the ability to specify a range or list where applicable, including: • County of residence; • City of residence; • Zip code(s); • Home precinct; • Political party affiliation; • Date of registration; • Age (before or after a specified date of birth, or within a specified range of dates of

	birth); • Gender; • Language preference; • Voting participation history; and • Political district/jurisdiction (e.g., Congressional District, State Assembly District; County Supervisory District; local school district, etc.).
26.4	In fulfillment of a PVRDR, DVRS must be able to produce an extract in a tab-delimited text file that includes the following data fields for each voter: • County of residence; • Full name; • Residence address; • Mailing address; • Party affiliation; • Phone numbers; • Email address; • Language preference; • Gender; • Home precinct; • Date of registration; • Date of birth; • Place of Birth; • Registration status; and • Registration method.
26.5	In fulfillment of a PVRDR that requests inclusion of voter participation history for each voter, DVRS must be able to produce an extract in multiple related tab-delimited text files that includes the following files/data: • Voter registration data (all fields identified in 26.4); and • Voting participation history, including each relevant election in which each selected voter has voted and the method of voting (i.e., absentee, early, or in person). The extracted files must include key data fields to appropriately relate/join the data in each file, so that the extracts can be imported into a relational database.
26.6	In fulfillment of a PVRDR that requests inclusion of voter political district assignment for each voter, DVRS must be able to produce a extract in multiple related tab-delimited text files that includes the following files/data: • Voter registration data (all fields identified in 26.4); and • Political districts to which each voter is assigned. The extracted files must include key data fields to appropriately relate/join the data in each file, so that the extracts can be imported into a relational database.
26.7	DVRS must include the ability for authorized SOS administrators to insert one or more fictional registration records into each PVRDR extract to “seed” the data extract so that improper use of the data can be traced to the particular PVRDR data release.
26.8	DVRS must provide the ability to record the seeded record(s) associated with each PVRDR.
DVRS.F27	**SOS PROCESSES: Jury Wheel Extracts**
27.1	DVRS must provide authorized SOS administrators and authorized county users with a method to select voter registration records for inclusion or exclusion in a Jury Wheel extract based on multiple filtering criteria, with the ability to specify a range or list where

	applicable, including: • County of residence; • City of residence; and • Political district/jurisdiction (e.g., Congressional District, State Assembly District; County Supervisory District; local school district, etc.).
27.2	DVRS must be able to further select records based on a formula that starts with the Nth record and selects every N^{th} record thereafter, where "N" and "M" are variables provided by the applicant (e.g., select every 39th record after record #17).
27.3	DVRS must provide the ability for SOS administrators to track requests for Jury Wheel Extracts (JWEs), including: • Requestor name and contact information; • Requestor address; • Requestor specifications for the extract; • Date of request; • Date request received; • Date request fulfilled (or denied); and • Filename and number of records in the extract.
DVRS.F28	**SOS PROCESSES: Affidavit Issuance Tracking**
28.1	DVRS must allow an authorized SOS or county user the ability to record the issuance of blank voter registration affidavits to an individual or organization from SOS, including: • The name and contact information of the person who requested and received the ballots; • The name of the organization if any; • The date of issuance; and • The range of affidavits issued.
28.2	DVRS must provide a method for an authorized SOS or county user to input a specific affidavit number and determine the person or organization to which the affidavit was issued.
DVRS.F29	**SOS PROCESSES: Public Access Web Site**
29.1	DVRS must provide a public web site for voters to verify the status of their voter registration and other election related information without compromising private information.
29.2	For privacy purposes, the DVRS public web site must require an individual accessing the website to provide sufficient personal identification data to prevent others from accessing that voter's data and must not provide or confirm any private information.
29.3	The DVRS public web site must allow a voter to determine: • Whether he or she is registered to vote and if not then provide for the ability to prepare a voter registration application online to be printed with a signature field for affidavit purposes and a means to track the application process thereafter; • Whether or not voter is registered as a permanent absentee or mail ballot voter; • Political party affiliation; and • His or her eligibility to vote in an upcoming election.
29.4	The DVRS public web site must allow a person to determine the assigned polling place for a residence address.
29.5	The DVRS public web site 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

29.6	The DVRS public web site must allow voters who have requested an absentee ballot or voted an absentee ballot to determine the status of that ballot
29.7	The DVRS public web site must be fully accessible for voters with disabilities; e.g., Americans with Disabilities Act (ADA) Level 1 & 2 compliant, U.S. Rehabilitation Act including Section 508, Subpart B Priority 1 and 2 level check points of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0 "AA" Conformance Level) development by the World Wide Web Consortium (W3C).
29.8	All DVRS web content and functions provided to meet these requirements must be available in Spanish as well as English.

4.3 Architectural Goals

The TrustTheVote Project seeks to produce an open source digital voter registration system that meets or exceeds the broadest consensus of States' requirements. However, it is impossible to meet every State's individual state-specific needs. Therefore, an over-arching goal is to produce a solution that is highly extensible and easily modifiable. In addition, at the encouragement of planned and prospective users of DVRS, the following architectural goals are to be considered in developing specifications and building the reference implementation.

- **Completeness.** The architecture shall aspire to meet all of the functional and performance requirements and business goals as stated herein.
- **Elegance.** The architecture and reference implementation shall aspire to achieve clarity and simplicity of design, minimization of components, direct and non-recursive data communications paths, and optimization of hardware and software components without excessive fragmentation of tasks.
- **Flexibility.** The architecture and reference implementation shall aspire to accept modifications to business rules and data elements and to extend functionality, capacity and performance at the lowest possible cost (in development time) and complexity.
- **Legacy EMS Compatibility.** The architecture and reference implementation shall aspire to minimize modification requirements of existing State and/or county EMS systems in order to support DVRS application program interfaces, and ensure the ability for users to employ DVRS interfaces without excessive task duplication or complication.
- **Maintainability.** The architecture shall aspire to ensure the system can be maintained by personnel with commonly available skills; the use of commodity hardware, and the ease with which necessary changes and updates can be implemented.
- **High Assurance.** The architecture and reference implementation shall aspire to deliver very high availability, including the tolerance for common system component failures and the ability to perform routine maintenance without interrupting service.
- **Interoperability.** The architecture and reference implementation shall ensure ease with which the system can exchange data or obtain services from external systems, and the appropriate use of independent national and international standards
- **Recovery.** The architecture and reference implementation shall ensure the ability to recover the system to full functionality with all data intact following an event that destroys or renders unusable the primary system facility at SOS.
- **Security and Privacy.** The architecture and reference implementation shall provide for comprehensive mechanisms to prevent accidental or malicious use, destruction, of modification of system resources or data, and specific mechanisms including, but not limited to, those required by applicable State or Federal statute or regulation, to ensure

that private and confidential data are not disclosed or exposed for disclosure to unauthorized entities.

- **Stability.** The architecture and reference implementation shall aspire to support above-average workloads, and other abnormal stresses.

Moreover, the DVRS should support a robust reporting service. Therefore, the TrustTheVote Project also has the following goals with regard to reports.

- **Completeness.** The architecture and reference implementation shall aspire to ensure DVRS meets all current and foreseeable future reporting requirements.
- **Elegance.** The architecture and reference implementation shall aspire to ensure the use of common components to support reporting functions throughout the system, and the use of components for their normal purposes without excessive fragmentation of tasks.
- **Performance.** The architecture and reference implementation shall aspire to provide reasonable turnaround on the creation of large or complex reports without degrading the performance of other system components and functions.
- **Usability.** The architecture and reference implementation shall aspire to ensure ease of use of the reporting functions, including the ease with which staff can be trained to produce reports, the ability to modify existing reports and to add new reports by trained end users without programming support, and the degree to which the user interface is easy and intuitive without excessive manual tasks or complexity.
- **Adaptability and Extensibility.** The architecture and reference implementation shall aspire to support reporting requirements beyond those specified in this proposal without significant system modification.
- **Familiarity.** The architecture and reference implementation shall aspire to use commonly-used reporting tools or languages, so that personnel can be recruited and trained to perform reporting tasks, including both the generation of existing reports and the creation of new and modified reports.

4.4 Technical Requirements

This subsection contains the detailed **technical requirements** that Secretary of State (SOS) offices participating in the TrustTheVote (TTV) Project are informing the OSET Institute will or should be required of a "best practices" digital voter registration system (DVRS) to address the business processes in Section III.

Requirement #	Requirement Description
DVRS-T1	**SECURITY AND PASSWORDS**
1.1	DVRS access must be controlled by two-factor authentication, including user ID/password as one factor and either restricted physical access (e.g., to a specific workstation) or possession of a physical device (e.g., single-use password generator) as the second factor.
1.2	DVRS access must provide a security function that allows the establishment of roles and allows SOS administrators to define the specific functions that can be performed by users assigned to each role.
1.3	Except where otherwise specified, SOS administrators must be able to be assigned access through defined SOS roles to data for all counties; authorized county users must be restricted to add, modify and delete data for their counties only.

1.4	DVRS must provide the ability for delegated security administration, allowing SOS administrators to define county security administrators, who will have the ability to define county users with roles that give them permissions to perform functions within that county.
1.5	DVRS must provide the ability to enforce strong passwords that include non-alphabetic and non-numeric characters of a minimum length that can be configured by SOS administrators.
1.6	DVRS must allow SOS administrators to set and enforce the number of intervening passwords that must be used before a password can be reused by an authorized user.
1.7	DVRS must allow SOS administrators to force users to change password at next logon or at a prescribed interval (e.g., after XX days or XX number of logons).
1.8	DVRS must enforce mandatory password changes after a specified number of days that can be configured by SOS administrators. DVRS must provide a visual warning of imminent password expiration to authorized users at logon starting at a specific number of days prior to their expiration of their password that can be configured by SOS administrators.
1.9	DVRS must provide the capability for SOS administrators and designated county security administrators to establish a specific expiration date for a user account.
1.10	DVRS must provide the ability for SOS administrators to revoke a user's access to the system and, in such instances, must apply the revocation immediately, even if the user is currently logged onto the system.
1.11	DVRS must provide SOS administrators the ability to configure the number of invalid logon attempts after which a user account is automatically disabled. For invalid logon attempts, DVRS must display a generic error message that does not indicate the precise nature of the failed information. DVRS must allow SOS administrators to configure the text message displayed for invalid logon attempts.
1.12	DVRS must store user passwords in the system in an encrypted manner such that they cannot be viewed in plain text by any authorized user and must not be stored in any manner on the client side (e.g., cookies, hidden form elements, etc.)
1.13	DVRS must allow SOS administrators to configure a timeout period such that inactive user sessions that exceed the timeout are automatically logged off DVRS.
1.14	Access control for users in the central environment shall be through a Lightweight Directory Access Protocol (LDAP) compatible directory
1.15	DVRS must prevent data caching of confidential voter registration data on user systems.
1.16	All DVRS servers must be hardened to industry standards; hardening procedures must be well documented.
1.17	DVRS must encrypt all data in transit using Secure Socket Layer (SSL) between servers and between servers and workstations.
1.18	DVRS must encrypt all private data whenever stored in nonvolatile memory.
DVRS.T2	**INTERFACES**
2.1	All DVRS interfaces with external systems must be implemented as service points except where that architecture is not compatible with the external system.
	All DVRS interfaces must be implemented using XML; a removable converter must be used to communicate with non-XML partners.
DVRS.T3	**AVAILABILITY AND OPERATIONAL RECOVERY**
3.1	DVRS must be implements so that the primary server equipment is housed at SOS,

	with a backup server environment installed at a physically remote state facility. The equipment at the two facilities should be configured to support the required availability by establishing near-real-time synchronization of data between the two facilities
3.2	DVRS must be implemented with full data replication and synchronization between at least two central server sites, so that all functions can continue without interruption in the event of the unavailability of any one site. The second and subsequent site may be configured to support 50% of peak workload; however, the alternate site(s) must be able to assume full peak capacity workload through the addition of hardware and/or software licenses only and within one day of the onsite availability of any required hardware
3.3	DVRS must be designed and tested to complete restoration to full, multi-site operation following the failure of any single site with no more than 12 hours of system unavailability.
3.4	DVRS must be designed and tested to complete restoration to full, multi-site operation following the scheduled shutdown of any single site in less than one hour.
3.5	DVRS must be designed and tested so that all central server system software and hardware maintenance can be performed at one site while the remaining site(s) continues in operation.
3.6	DVRS must be designed and tested so that no routine process that requires system unavailability requires more than six (6) hours to complete.
3.7	DVRS must be capable of operating for at least eight (8) weeks without interruption for routine scheduled activities.
DVRS.T4	**PERFORMANCE AND CAPACITY**
4.1	DVRS must ensure that routine transactions, including all user system activities functions involved in adding, deleting or updating a voter registration record, complete in less than one (1) second. Searches for records based on criteria that do not include the Unique ID must complete in less than two (2) seconds. DVRS EMS functions not related to voter registration must complete in less than two (2) seconds. All performance requirements are exclusive of network transit time, to be measured at the external interface of the WAN boundary firewall. Performance requirements are also exclusive of the round-trip time for response from the DMV/SSA interface, also to be measured at the external interface of the wide-area network (WAN) boundary firewall.
4.2	DVRS must support two thousand (2000) concurrent users, and must support peak usage of two hundred (200) routine transactions per second while meeting all other performance requirements previously stated.
4.3	DVRS must support up to thirty (30) million active and inactive and cancelled voters as implemented under this contract, and must support up to one hundred (100) million active and inactive voters with the addition of hardware only. DVRS must provide capacity for up to fifty (50) years of voter activity and voter participation history for each voter, and an average of ten (10) affidavit and signature images for each voter, with a maximum of at least one hundred affidavit and at least one hundred signature images for individual voters
4.4	DVRS must allow the ability to archive cancelled voter records older than an age specified when the archive process is run. An index of all archive records must be maintained so that archived records may be searched by name, date of birth and unique ID, and any or all such records restored to the database.
DVRS.T5	**PUBLIC INTERNET ACCESS**
5.1	All public web content must provide equivalent functionality, form and content through any Internet web browser, including the current version and at least two integer releases.

5.2	All public web content must conform to the Priority 1 and 2 level checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0 "AA" Conformance Level) development by the World Wide Web Consortium (W3C).
DVRS.T6	**AUDITING**
6.1	DVRS must log all user and system activity with the application, including logon attempts, data viewed, queries and reports generated and errors encountered. Such system logs must contain sufficient information for authorized administrators to reliably reconstruct the chain of events and track them back to a specific user.
6.2	DVRS must capture and store for all changes of data, at the record and field level, the following data for audit and review: • Data that was changed; • Prior value of the data before the change; • Date and time of the change; and • Source of the change (down to actual user, where known to the system).
6.3	DVRS must provide a mechanism for authorized SOS administrators to search, view and print DVRS audit log data that can be filtered and sorted by: • Date (or range of dates); • Jurisdiction (where applicable); • Data field changed; • Record that was changed; and • Source of the change (to the actual user when known to the system).
6.4	DVRS must provide the capability to archive and purge audit log entries prior to a given date.
6.5	DVRS must be designed so that all audit log data is secure from manipulation and tampering.
6.6	DVRS must be capable of receiving and storing audit log data regarding changes to voter registration data from county EMSs. DVRS must provide a mechanism for SOS administrators to search, view and print audit data that can be filtered and sorted by: • Date (or range of dates); • Jurisdiction (where applicable); • Data field changed; • Record that was changed; and • Source of the change (down to the actual user where known to the system).
DVRS.T7	**ERROR AND EXCEPTION HANDLING**
7.1	Error and exception handling routines must be implemented within DVRS to catalog and chronicle all error messages.
7.2	All log files for errors and exceptions must capture all relevant information for each event, including: • Date/time; • User name; • Source; and • Error description.
7.3	DVRS must provide a mechanism for administrators to search and review error logs.

7.4	DVRS user interfaces must provide user error messages that clearly communicate the following to the user: • Simple, clear explanation of the error; • Identification of the source/location of the error (e.g., module, error code, etc.) for troubleshooting by SOS and TrustTheVote Project staff; and • What the user can do to correct the error (if applicable). As an example of unacceptable messages: standard error messages as served by HTTP servers (e.g., "404 Page Not Found").
7.5	DVRS must provide a mechanism for real-time alerts to administrators and support staff (e.g., email, pager alert, etc.) of critical system failures and errors (not including user errors such as login failure and data entry error.)
DVRS.T8	**REPORTING**
8.1	DVRS must provide the capability for users to generate and print the reports
8.2	DVRS must, where applicable for pre-defined reports, allow the user to configure report parameters for: • Selecting data detail to include in the report; • Constraining or filtering the data on which the report is based; and • Establishing the data grouping and sorting for the report.
8.3	DVRS data must be appropriately indexed for rapid generation of all pre-defined reports
8.4	DVRS must provide the user with a visual "progress indicator" during data extraction and report generation, and must allow the user to cancel reports prior to completion
8.5	DVRS must at user option, include the report parameters and report date in each report for pre-defined reports
8.6	DVRS must support a general-purpose report writer that allows authorized users on an ad hoc basis to extract data from the DVRS database and create formatted reports using the extracted data with user-defined sort criteria, filters, and subtotal/totals.
8.7	The ad hoc report writer tool must present logical, pre-defined views on the data such that users can generate reports without understanding of the underlying technical data structure
8.8	The ad hoc report writer tool must allow authorized users to save custom defined reports for later re-use
8.9	DVRS must make all reports available for immediate generation and for batch generation
8.10	DVRS must, for all reports, allow the user to: • Preview/display the report on screen, instead of or prior to printing the report; • Print the entire report or user selected page(s) to a user-selected printer in a local TCP/IP network environment; and • Export the report data electronically to a user specified location, in multiple formats, including: Acrobat PDF, MS Word, MS Excel, and tab-delimited text file
8.11	DVRS Reporting must provide the capability to print postcards or mailing labels of all or selected voters, filtered by any criteria stored in the database
8.12	DVRS must, at user option, sort and generate all address data for bulk mailings to obtain discounted postal rates
DVRS.T9	**GENERAL TECHNICAL**
9.1	DVRS must provide tools to monitor the system and database performance

9.2	DVRS graphical user interfaces shall employ entry tools such as default values, combo boxes that can select value based on successive character entry, check boxes, radio buttons, pick lists and context-sensitive right-click or command-click menus
9.3	DVRS must provide at least four (4) user customizable fields, such that the fields can be assigned names that the field names will automatically display with the field in the user interface and the data type can be configured by SOS administrators, for each of the following data sets: • Voters; • Precincts; and • Political districts
9.4	DVRS must provide a user interface and workflow that facilitates minimizing keystrokes during data entry; in other words, the user interface must support a variety of user styles from management casual browsing to production-intensive data entry operations.
9.5	DVRS must provide an intuitive graphical user interface (GUI) using screen navigation via pointing device or keyboard at user option and use standard function keys across all components (e.g., F1 always is the same function).
9.6	DVRS must provide functionality for data entry errors to be identified at the time of entry with descriptive and instructional messages in non-technical terms (e.g., real-time field-level verification).
9.7	DVRS must provide consistent menus and screens with a common look and feel throughout the application with a screen title and unique screen identifier on every screen.
9.8	DVRS must provide a standard real-time processing indicator (e.g., the hourglass found in Microsoft Word or a progress bar found in a web browser) that will enable the user to visually assess that the application is processing and not frozen.
9.10	DVRS must provide comprehensive on-screen context-sensitive help function that can be accessed both from the function in question and independently from a menu
9.11	DVRS EMS must support commercially available scanners, including automated sheet fed scanners and bar code reading devices.

4.5 Standard Reporting Requirements

The DVRS needs to support the following standard reports.

4.5.1. Voter Registration

4.5.1.1. Individual registrant detail:

- With or without voter participation history;
- With or without voter activity history; and
- Audit log of changes to voter record.

4.5.1.2. Individual voter affidavit image

4.5.1.3. Current and historic registration statistics/counts:

- By county;
- By political district (category and individual);
- By age;
- By partisan affiliation;
- By category of UID (i.e., DL# based, SSN4 based, or generated);
- By registration status;
- By registration date;

- By confidentiality status/type;
- By absentee status/type;
- By language requirements;
- By accessibility requirements;
- By combinations of above.

4.5.1.4. Voters with an effective mailing address that cannot be CASS certified

4.5.1.5. Current and historic statistics/counts for voters who voted in an election:

- By county;
- By political district (category and individual);
- By age;
- By partisan affiliation;
- By registration status;
- By registration date;
- By confidentiality status/type;
- By absentee status/type;
- By language requirements;
- By accessibility requirements;
- By voting method (*i.e.,* Early, Absentee, Polling Place, Provisional);
- By combinations of above.

4.5.1.6. Absentee voting status: statistics/counts on absentee ballot status (e.g., mailed but not returned; returned and counted; rejected by reason):

- By county;
- By political district (category and individual);
- By age;
- By partisan affiliation;
- By registration status;
- By registration date;
- By confidentiality status/type;
- By absentee status/type;
- By language requirements;
- By accessibility requirements;
- By voting method (i.e., Early, Absentee, Polling Place, Provisional);
- By combinations of above.

4.5.1.7. NVRA report of registration changes for a specified period by source of the registration change

4.5.1.8. ROR status report indicating that the counties have completed entry of voter registrations for a specific ROR

4.5.2. Investigations

4.5.2.1. Voters who have voted more than once in an election

4.5.2.2. Voters (by address) when more than “X” voters are registered at the same address

4.5.2.3. Voters who are registered at an address designated “commercial” (or non-residential)

4.5.3. Political Party

4.5.3.1. Political party detail (with or without history)

4.5.3.2. Political parties listing (including status and assigned system code)

4.5.3.3. Political parties contacts

4.5.4. Address – Precinct – District Mapping

4.5.4.1. Precincts by district (all or selected districts)

4.5.4.2. Districts by precinct (all or selected precincts)

4.5.4.3. Orphaned addresses (not assigned to a precinct)

4.5.4.4. Orphaned precincts (not assigned to one or more required districts)

4.5.4.5. Orphaned districts (no precincts assigned)

4.5.4.6. Alias to street name translation

4.5.4.7. Street names and associated aliases

4.5.4.8. Alias to city name translation

4.5.4.9. Cities and associated aliases

4.5.5. Voter Registration Processing and List Maintenance

4.5.5.1. Detailed listing of unresolved registration issues over "X" days of age:

- By county;
- By type (e.g., data validation error, fatal "pend," potential move out of county, potential duplicate, potential death record match, potential felon match, potential DMV match, potential NCOA match).

4.5.5.2. Summary statistics of unresolved registration issues over "X" days of age:

- By county;
- By type (e.g., data validation error, fatal "pend," potential move out of county, potential duplicate, potential death record match, potential felon match, potential DMV match, potential NCOA match).

4.5.5.3. Voter registration activity statistics within a specified date range:

- By county;
- By type of transaction (e.g., new registration, re-registration within county, re-registration in new county, change of party, cancellation, inactivation, etc.);
- By status of transaction (e.g., completed/active, pending).

4.5.5.4. Voter registration activity error statistics (error count, resolution time) within a specified date range:

- By county;
- By type of transaction (e.g., new registration, re-registration within county, re-registration in new county, change of party, cancellation, inactivation, etc.);
- By type of error;
- By resolution type

4.5.5.5. Voters who have not been mailed a VNC after X days (count by county)

4.5.5.6. Statistics/counts on voters mailed a pre-election RCP by county

4.5.5.7. Statistics/counts on voters mailed a Change of Address Notification (CAN) by county

4.5.5.8. Statistics/counts on voters, by county, who have not voted in "X" years and have not been sent an RCP or an ARCP,

4.5.5.9. Listing of voters, by county, who have not voted in "X" years and have not been sent an RCP or an ARCP,

4.5.5.10. Statistics/counts by county on voters who have had an "inactive" status and not voted since "X" date.

4.5.5.11. Listing of voters, by county, who have had an "inactive" status and not voted since "X" date.

4.5.5.12. DVRS duplicate identification performance statistics (match count, valid match rate, resolution time) within a specified date range:

- By match criteria;
- By match status (e.g., not resolved, match confirmed, non-match verified);
- By county of residence.

4.5.5.13. NCOA performance statistics (match count, valid match rate, resolution time) within a specified date range:

- By type of notice (e.g., individual, family);
- By type of move (e.g., in-county, new county, out-of-state, no forwarding address);
- By match criteria;
- By match status (e.g., not resolved, match confirmed, non-match verified);
- By county of residence.

4.5.5.14. DHS Death Record matching performance statistics (match count, valid match rate, resolution time) within a specified date range:

- By match criteria;
- By type (*i.e.*, new registration validation versus new death notice against existing registration records);
- By match status (e.g., not resolved, match confirmed, non-match verified);
- By county of residence.

4.5.5.15. DCR felon matching performance statistics (match count, valid match rate, resolution time) within a specified date range:

- By match criteria;
- By type (*i.e.*, new registration validation versus new felon notice against existing registration records);
- By match status (e.g., not resolved, match confirmed, non-match verified);
- By county of residence.

4.5.5.16. DMV Motor Voter performance statistics (match count, valid match rate, resolution time) within a specified date range:

- By type of transaction (e.g., new registration, in-county move, move between counties);
- By match criteria;
- By match status (e.g., not resolved, match confirmed, non-match verified);
- By county of residence.

4.5.5.17. DMV ID verification performance statistics (match counts, valid match rate, turnaround time):
- By type of verification requested (*i.e.,* DL#, SSN4, no ID);
- By type of verification response;
- By county of residence

4.5.6. .Election Management

4.5.6.1. List of elections defined in system (including status, election date and assigned codes)

4.5.6.2. Detailed definition of individual election (all associated data, for proofing)

4.5.6.3. List of defined voting precincts and associated voter registration counts for a specific election:
- By county;
- By political district;
- By political party affiliation;
- By registration status (e.g., active, inactive, absentee, permanent absentee, early voted

4.5.6.4. List of rosters not printed for a specific election:
- By county;
- By voting precinct

4.5.6.5. Summary statistics of roster printing for an election:
- By county;
- By date printed;
- By roster type (e.g., active voters, inactive voters, supplemental).

4.5.6.6. Voter Turnout in a specific election:
- By county;
- By political district;
- By age;
- By partisan affiliation;
- By language preference;
- By type of participation (*i.e.*, absentee/mail, early, in-polling place, provisional)

4.5.7. Registration Report
(Covered in business requirement DVRS.F24)

4.5.8. Voter Information Guide (VIG) Mailing

4.5.8.1. Summary statistics of voters selected for mailing:
- By county;
- By language selected.

4.5.8.2. Summary statistics of “household” mailing addresses generated/extracted:
- By county;
- By language selected

4.5.8.3. Summary statistics of eligible voters not selected or rejected:
- By county;
- By reason (e.g., invalid mailing address, out-of-state mailing address).

4.5.9. Public Requests for Voter Registration Data

4.5.9.1. List of all applications/requests for voter registration data (including date requested, applicant, and status of application):

- By date range of application;
- By date range of fulfillment or denial;
- By status (i.e., pending, fulfilled, denied);
- By applicant;
- By basis for qualification (*e.g., political party, candidate, journalist);*
- By type of data requested

4.5.9.2. Individual PRVRD detail, including investigation log, data requested and seeded registration records

4.5.9.3. Listing or index of PRVRD and salted registration records

4.5.10. Jury Wheel Extracts

4.5.10.1. List of all applications/requests for jury wheel extracts (including date requested, applicant, and status of application):

- By date range of application;
- By date range of fulfillment;
- By status (*i.e., pending, fulfilled, denied*);
- By applicant.

4.5.10.2. Individual jury wheel request detail, including requestor information and data requested.