# Contents

# 1. Introduction

This document details the technical requirements for the DOR-MVD System. These requirements cover aspects of the DOR-MVD System outside of the requirements for the specific business areas. The users of the system include all agency staff and external users including but not limited to County Treasurer staff, dealer staff and other (e.g., law enforcement) as identified by the state.

Any references to policies and associated links refer to the most current version. Offerors shall be responsible for reviewing, understanding and complying with all such policies.

## 1.1 User Interface Requirements

- **Multiple Browser Support** - UI must support all major browsers including but not limited to Edge, Chrome, Firefox, Safari. Public facing web applications shall be browser independent.
- **Mobile GUI Support** - UI must provide a single responsive GUI (Graphical User Interface) that runs on mobile devices as well as desktop devices (preferrable to include laptop/monitor touchscreen interactions).
- **Consistent Layout** - UI must have a consistent layout across modules including warnings, alerts and other prompts and must have consistent controls and buttons across modules.
- **Internal and External Users** - UI must consider audience of users from internal (DOR staff & BIT) and external users (customers).
- **ADA Compliant** - UI must be ADA compliant.
  - Preferrable that ADA features are togglable.
- **Guided Design** – Must have a simple clean design, be intuitive, and should guide the user through the process.
- **Required Fields** - UI must visually identify the mandatory input fields (i.e., requiring user input).
  - UI must also consider dynamic mandatory input fields.
- **Field Masking** - UI fields must support a format mask that will enforce mandatory formatting for data entry such as: dates, SSN, phone numbers etc.
- **Masked Passwords** - UI password fields must be masked on typing.
- **Data Validations** - UI must validate that all mandatory data fields have been completed when a user attempts to submit information.
- **Breadcrumb Navigation Displays** - UI should display breadcrumbs and allow users to move forward and back to prior screens to adjust data before submission and guide user navigation to required screens.
- **User Save Prompts** - UI must prompt user to save data before exiting screens as needed.
- **Real Time Error Messaging** - UI must interactively inform the user of errors based on real-time validations performed as the user enters data or as soon as the remote system check is completed.
- **Copy/Paste Support** - UI must support the ability to copy/paste data from one application GUI to another.
- **PII Security** - UI must adhere to security measures/specifications to prevent bulk PII loss.
- **Tabbing Navigation** - UI should allow tabbing/typing through fields.

- **Navigation Focus** - Focus should go to the next logical field.
- **Dynamic Dropdowns** - UI should have dynamic dropdowns that can be filtered/narrowed down by typing.
- **Branding** – Complying with South Dakota branding standards as defined by the State
- **Current Version of Windows** – The system shall be developed, deployed, and maintained to be compatible with the latest version of MS Windows and, as possible, be capable of running in the three most current versions of Windows.
- **Multi-Lingual Support** – The system shall support default language is English, but shall also support other language translation for Spanish, French and others.

## 1.2 Hosting

DOR is seeking a cloud-based solution with the following requirements:

- **SaaS** – The Vendor will bid a solution that is generally proposed as a COTS (Commercial-Off-The-Shelf) product on a hosted platform delivered as a SaaS (Software as a Service) solution.
- **FedRAMP** – The solution must be hosted on a FedRAMP certified hosting platform. The State's prefers to have the solution hosted in the State's FedRAMP certified platform.
- **Primary & Secondary Sites** – The Vendor shall provide a Primary Data Center location and a Secondary Site that runs redundantly serving both as a fail-over and a Disaster Recovery site. This Disaster Recovery location shall be separated from the primary data center location and shall not be within sixty (60) miles of the primary location. All locations and sites must be within Continental United States.
- **Off-Site** – The Vendor shall provide a hosted or third-party hosted Primary Site and Secondary Site that shall not reside on South Dakota state property or a South Dakota state managed facility. All locations and sites must be within Continental United States.
- **Compliance** – The hosting platform must meet State and Federal compliance requirements. State compliance requirements may be found in the BIT Security Policies at this link: https://bit.sd.gov/bit?id=bit_standards_vendor_client_sec_req
- **Connectivity** – The vendor shall supply network connectivity between the Primary and Secondary sites to sufficiently keep the systems in sync and able to meet all disaster recovery and failover requirements. The vendor shall provide supply network connectivity between these locations and the State of South Dakota's network to sufficiently support all requirements in this RFP. The vendor shall ensure that the entire system has enough network and data throughput capacity to support all requirements in this RFP.
- **Storage** – The hosting solution shall include all storage and processing capacity to support all the requirements in this RFP.
- **Supporting Software Components** – The hosted solution shall include all software components and associated licenses necessary for the system to fully function and necessary to manage and maintain the system. This includes but is not limited to database software, operating systems, infrastructure management tools, rules engines, and workflow tools.

## 1.3 Security

### 1.3.1 General Requirements

The DOR-MVD System shall meet all physical and logical security requirements including those found at https://bit.sd.gov/bit?id=bit_standards_vendor_client_sec_req and as noted below:

- **Legislation & Policy** – Complying with and maintaining compliance with appropriate State and federal legislation, regulations, and policy.
- **Security Requirements** – Complying with State and Federal security requirements and safeguard requirements including but not limited to:
  - Incident Reporting and Breach of Security Protocols.
  - Record Disposition/Destruction Security Controls/Standards.
  - Third Party Data Security Controls/Standards.
- **Fail Secure** – Adhering to the principle of "Fail Secure" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.
- **Secure System Boundaries** – Monitoring and controlling communications at key internal boundaries (for example Web servers, Application servers, Database servers) within the DOR-MVD System.
- **Secure Logs** – Not recording sensitive data in debug logs or other application logs created by custom code or COTS components unless the DOR-MVD System encrypts the PII data.
- **Protect Data** – Prevent corruption or loss of data already accepted into the DOR-MVD System in the event of a system failure.
- **Secure Components** – The Vendor shall not deploy any application to production that contains known security vulnerabilities.
- **Scanning** – The DOR-MVD System shall be subject to DOR and BIT security and vulnerability scanning. The Vendor shall remediate any non-compliant results in an agreed upon timely fashion as defined and agreed upon in the Operations and Maintenance section of this RFP.
- **Encryption** – Apply encryption to all data both at rest (stored) and in transit.
- **Trusted Networks and Nodes** – Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems supporting the DOR-MVD System from unsolicited and unauthenticated network traffic.
- **Configuration Reviews** – Review at regular intervals the network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary. Reviews shall be conducted at least twice annually.
- **Organized & Well Managed Hosting** – The Vendor shall implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry practices, such as the current Control Objectives for Information and Related Technology (COBIT) framework or similar applicable industry standards for information security, and shall ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of, and disclosed comply with applicable data protection and privacy laws as well as the terms and conditions of this RFP.

- **Hardening Procedures** – Apply hardware and software hardening procedures, which may include, but not limited to, removal of unnecessary software, disabling or removing of unnecessary services, the removal of unnecessary usernames or logins, and the deactivation of unneeded features in the System configuration files, as recommended by the manufacturer to reduce the System's surface of vulnerability.
- **Data Isolation** – Ensure that State data is not comingled with the Vendor's other clients' data through the proper application of compartmentalization security measures.
- **Security for All Environments** – All DOR-MVD system environments such as the Test and Training environments shall be subject to the same security requirements as those for production environment.
- **Use of Production Data in a Non-Production Environment** – Precautions must be taken when copying data from a production environment to a non-production environment. A non-production environment can be, but is not limited to, conversion, staging, development, or test environments. State data in non-production environments must be stored securely and must have DOR approval before moving any protected production data to a non-production environment. Prior to moving production data from the State's environment to the Contractor's system there must be a security scan. This scan must be done by the State or a BIT approved third-party. This scan can be done up to three months before the data is moved. If there is a third-party scan the scan results must be provided to the State contact.
- **Data Breach Management** – In the event of a Data Breach (e.g., Unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a customer or partner), the DOR-MVD System and Vendor shall:
  - Immediately notify the State with information regarding the breach (e.g., time, customers effected, data compromised, etc.)
  - Isolate all systems used by the attacker to prevent further issues with the data or network.
  - Separate or disable the breached user accounts.
  - Assess the damage and identify and close all breach points.
  - Provide the capability to notify impacted parties in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law. enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. Note, there may be delays in notification if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.
  - Identify and implement an approach to safely restore data.
  - Conduct penetration testing – Depending on the breach, the State and vendor will determine which environments will require penetration testing.
  - Update the system recovery and disaster recovery plans
  - Comply with Appendix Q - BIT Standard Contract Terms: Cyber Liability Insurance, Handling of Security Incident, and Adverse Event.

### 1.3.2 Access Security

- **Single Sign-On Requirements** – The DOR-MVD System shall comply with the State of South Dakota's standard identity management service single sign-on (SSO) which enables custom control of how internal and external users, referred to as "non-privileged" access, sign up, sign in, and manage their profiles, as part of the State's Identity and Access Management (IAM) strategy.

  The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0 (preferred). This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all non-privileged application Administrators and may be required for other users. Microsoft's official documentation on the identity provider the State has implemented can be found at https://docs.microsoft.com/en-us/azure/active-directory-b2c/ and https://docs.microsoft.com/en-us/azure/active-directory-b2c/integrate-with-app-code-samples.

  The Offeror shall provide single sign-on and identify management services for all "privileged" accounts. Privileged accounts refer to those accounts that perform development, maintenance, support or other functions required for the operation of the Offeror's solution.
- **Multiple Role Types** – The DOR-MVD System shall accommodate access to customers and State employees having many roles: Vehicle owner, state employee, etc.
- **Personally Identifiable Information (PII)** – The DOR-MVD System must protect the security of and user access to personally identifiable information collected pursuant to Driver Privacy Protection Act (DPPA).
- **Secure Customer and Partner Access and 2 Factor Authentication** – The DOR-MVD System shall allow Clients to log into a Web Based Transaction Center (see functional requirements, Web Based Transaction Center) using a secure ID and password. As required by the DOR for some or all access, the system shall implement Two Factor Authentication. The vendor shall comply with State's single-sign on policies and procedures.
- **Failed Login Attempt Lockout** – The DOR-MVD System shall enforce a configurable limit of consecutive invalid access attempts by a user and implement appropriate protections to protect against further, possibly malicious, user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for a configurable time period, or delays the next login prompt according to a configurable delay algorithm) and support defined DOR and BIT policy.

  All requirements noted will be administered, for non-privileged accounts, through the State's SSO framework. Requirements noted shall be administered by the Offeror for privileged accounts.
- **Warning Banner** – The DOR-MVD System shall display a configurable pre-login banner or warning (e.g.. "System shall only be accessed by authorized users") prior to accessing any PII. If the DOR-MVD System does not support pre-login capabilities, the DOR-MVD System shall display the banner immediately following authorization.
- **Anti-Virus Compatibility** – The DOR-MVD System shall ensure operation of the DOR-MVD System on workstations configured with anti-virus software per State of South Dakota (DOR or BIT) standards.

- **Access Logging** – The DOR-MVD System shall have appropriate logging parameters enabled to automatically monitor and record:
  - Authorized and failed access attempts
  - Critical information security events as recommended by the operating system and application manufacturers
  - PCI and information security standards
  - User access activities
  - System exceptions

  All requirements noted will be administered, for non-privileged accounts, through the State's SSO framework. Requirements noted shall be administered by the Offeror for privileged accounts.
- **Inactive User Session** – The DOR-MVD System upon detection of user inactivity shall prevent further viewing and access to the DOR-MVD System by that user/session and terminate the session or initiate a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. (The length of inactivity shall be configurable).
- **Password Rules and Access Configuration** – The DOR-MVD System shall be configurable to enforce the following rules regarding personal access:
  - Minimum Password Length (example = 8)
  - Failed login Lockout Threshold (example = 3)
  - Not Reusable Password History (example = 24 )
  - Password complexity (example = specific mix of numbers, letters, special characters)
  - Lockout duration (example = 33 minutes)

  All requirements noted will be administered, for non-privileged accounts, through the State's SSO framework. Requirements noted shall be administered by the Offeror for privileged accounts.

### 1.3.3 System Security

- **FedRAMP** – The DOR-MVD System shall implement FedRAMP security standards. The solution should include compliance with CJIS security requirements and NIST 800-53.
- **Certifications** – The Vendor shall maintain security certifications for sites used to host the DOR-MVD solution and provide the list of these certifications to DOR and BIT.
- **System Audit** – The Vendor shall submit the DOR-MVD System to a security audit (i.e., SOC2 Type II) annually, cooperate in State audits, and make past audit results available for evaluation purposes. The State of South Dakota will determine the scope of the audit.
- **Regular Testing** – Establish policies and procedures to implement and maintain mechanisms for regular vulnerability testing of operating system, application, and network devices to identify:
  - Device or software misconfigurations
  - Missing software patches
  - Outdated software versions
  - Validate compliance with or deviations from the Vendor's security policy
- **Vulnerability Analysis** – Vendor shall evaluate all identified vulnerabilities for potential adverse effect on the system's security and integrity and remediate the vulnerability

promptly or document the reason why remediation action is unnecessary or unsuitable. Vulnerability testing shall be conducted twice annually or more frequently as specified by other agency requirements and standards.

### 1.3.4 Security Log/Audits/Reports

The DOR-MVD System shall:

- **Log All Necessary Activity** – Through configuration, all DOR-MVD System components shall have appropriate logging parameters enabled to automatically monitor and record user access activities, authorized and failed access attempts, system exceptions, and critical information security events necessary to implement and achieve security, business operation monitoring, system performance, and other standards.
- **Log Data** – The DOR-MVD System shall support event logging based on selectable event criteria and producing audit reports that include, at a minimum, the following:
  - Date and time of the event
  - Identity/logon ID of the user associated with the event
  - Source of the event
  - Success or failure of the event
  - Type of event
  - Retaining (for a configurable retention period) the logs necessary to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation
- **Protect Data Logs** – Any recording of sensitive data in debug logs or other application logs created by custom code or COTS components must be protected by encryption like all other data.
- **Log Retention** – Retaining (for a configurable retention period) the logs necessary to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation.
- **Important Log Data** – The log shall support collection of security related data including the following:
  - Capture and store audit records for all security-relevant events, including all security, DBA, and system administrator accesses.
  - Capture and store audit records and transaction logs for indications of unusual activities, suspicious activities, or suspected violations.
  - Capture and store audit records and transactions logs for authorization of system level changes based on criteria defined by DOR/BIT.
- **Usage and Performance Reports** – The Vendor shall provide security reports to the State in a mutually agreeable format which shall include latency statistics, user access, user access IP address, user access history, and security logs for all State files related to the DOR-MVD System.

## 1.4 Backup/Recover/Fail-Over

The Vendor shall develop, document, and implement a system continuity and backup/recovery strategy that addresses the requirements below. The strategy shall address and identify all aspects of the DOR-MVD System relevant to creating continuity and recovery capabilities and

any considerations internal or external to the DOR-MVD System necessary to support or execute the recovery strategy.

- **Entire System** – The DOR-MVD System shall support backup of all system data, configuration files, metadata, server images, and other artifacts as required to recover the DOR-MVD System.
- **Supporting Environments** – The strategy must include recovery and failover for all environments such as Development and Test and although the RPO and RTO can be less than that of production and the parameters can be mutually agreed upon.
- **Disaster and Failure Events** – The DOR-MVD System continuity and recovery strategy and plan shall include considerations for recovery from both disaster, non-disaster (e.g. hardware failure), and backup events.
- **Data Integrity** – The DOR-MVD System continuity and recovery strategy shall specifically address data integrity, account for data dependencies across subsystems, and ensure data integrity when recovering from disaster or non-disaster events.
- **Consistent State** – The strategy shall implement a backup and restore solution to restore a consistent state across all system subsystems.
- **State Standards** – The DOR-MVD System continuity and recovery strategy shall be consistent with DOR and BIT Disaster Recovery Standards.
- **Operating Procedures** – The Vendor shall document all supporting procedures including those to be followed:
  - During normal operations
  - When errors or failures are identified
  - When transitioning to another environment or facility
  - When transitioning back to the primary facility and environment
  - When testing the backup, recovery, and failover functions
  - Post recovery
- **SLA & Approval** – All operations regarding failover and recover will comply with established service level requirements and include coordination with and approval by the State.
- **RPO & RTO** – Vendor will work with DOR and BIT to establish Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) with the following metrics:
  - RPO:  A maximum of 15 minutes
  - RTO: Four (4) hours for read-only access for Law Enforcement users and interfaces
  - RTO: Twenty-four (24) hours for full system access by all internal DOR and County users and web self-service clients
  - RTO: Forty-eight (48) hours for full system access by all users and clients, including third party interfaces.
- **Point In Time Recovery** – Vendor's strategy shall support point-in-time and point-of-failure recovery.
- **Lost Data Logging** – In addition to requirements for logging, documented elsewhere in the RFP, the Vendor shall ensure that sufficient logging is done so that the DOR and BIT can take action to notify affected individuals of any transactions that may not be recoverable as a result of the RPO.
- **Encryption** – The DOR-MVD System shall encrypt all backups using a shared key.

- **Backup Inventory** – The DOR-MVD System shall retain Daily Backups based on agreed upon business requirements.
- **Off-Site Storage** – The Vendor shall store Daily backups off-site.
- **Periodic Testing** – The Vendor shall test the fail-over, backup, and recovery processes at least semi-annually.

## 1.5 System Management

The DOR-MVD System shall include all of the administrative tools and capabilities that are needed to fully manage, monitor, and configure every aspect of the system, including but not limited to:

- **User Maintenance** – includes creating users, managing user roles, monitoring user activity, and administering all other attributes of users. This shall be integrated with appropriate authentication services which are part of the complete system.
- **Customer Information Maintenance** – includes all administrative functions for managing customer information and business transactions.
- **System Administration** – includes all aspects of monitoring and overseeing system functions.
- **System Configuration** – includes all aspects of viewing, changing, checking, and managing the available system configuration information.

## 1.6 Performance

The DOR-MVD System shall be sufficiently sized and appropriately configured in terms of memory, disk capacity, processors, network capacity and other resources to meet the performance requirements specified below. The system must meet the peak loads as well as the average load information provided.

### 1.6.1 Response Time

The system shall meet the response time requirements from the viewpoint of the business user. The DOR-MVD System shall be built and configured to support these requirements. DOR will work with the Vendor to define the appropriate boundaries and limitations for measuring system response time.

User interface response times are categorized as follows. User interface actions that are long running and result in response times that exceed 5 seconds should provide continuous feedback on the status of response (e.g., a percent complete progress indicator)

| User Interface Response Time Requirements | | |
|---|---|---|
| **Category** | **Response Time (t)** | **Examples** |
| Same Screen User Interactions | t < 0.1sec | Switching between tabs on a same screen; field-level validation; screen-level validation |
| Unique Record Retrieval | t < 2 sec | Search for person, vehicle or record based on unique identifier |

| User Interface Response Time Requirements | | |
|---|---|---|
| **Category** | **Response Time (t)** | **Examples** |
| Customer Search | t < 2 sec | Search for person record based on attributes (e.g., name) |
| Retrieve Customer Records | t < 2 sec | Retrieve and display full person record (e.g., identifiers, demographics, photo) |
| Screen Transition | t < 1 sec | Move from one screen to another screen of a transaction |
| Save Customer Record or Transaction Information | t < 2 sec | Save or submit a customer transaction |
| Refresh Customer Web Screen | t < 2 sec | Customer submits information or links to another web page |

### 1.6.2 System & Transaction Volumes

The DOR-MVD system must support the State's current user population, data, and transaction volumes and be capable of supporting reasonable growth. DOR's current system supports the following user community:

- 66 County Offices with about 450 County Users
- DOR-MVD Central office and branch offices with 250 Agency Users
- About 1,325 Motor Vehicle Dealerships (Including Watercraft/Boat and Snowmobile)
- About 171,000 Active Online Users (which has been steadily increasing about 2,000 a month)
- Other users include law enforcement agencies, citizens, and lending institutions.

DOR's current system contains the following record counts:

- More than 3 million Individuals
- Nearly 12,000 Trusts
- About 250 thousand Companies
- About 6.8 million Vehicles
- About 175 thousand Watercrafts/Boats
- About 260 thousand Disability Placards
- About 295 thousand Lien Holders

Document imaging volume is approximately 4.5 TB of data and includes 100 million documents.

The Vendor shall load all documents from the existing document imaging system into the DOR-MVD System as necessary to support current customers and necessary research. DOR will collaborate with the Vendor to identify documents which can be archived.

The following represent the current volume of system transactions.

| Transaction | Annual Volume | Peak Weekly/Daily |
|---|---|---|
| Self-Service, Online Registration Renewals | 120,000 | 900 Daily/ 4,400 Weekly |
| Self-Service, Kiosk Registration Renewals | 200,000 | 2,300 Daily/ 8,000 Weekly |
| Vehicle Titles Issued | 450,000 | 4,500 Daily/ 15,000 Weekly |
| Vehicle Registrations Renewed | 500,000 | 4,100 Daily/ 15,600 Weekly |
| Specialty License Plates Issued | 30,000 | 1,750 Daily/ 7,650 Weekly |
| Chats | 7,000 | 240 Daily/ 950 Weekly |
| Debt Collections | 3,600 | 75 Daily / 160 Weekly |
| Telephone Calls | 70,000 | 660 Daily/ 2,500 Weekly |
| Lien Holder Electronic Notifications (ELT) | 230,000 | 2,000 Daily/ 6,100 Weekly |

## 1.7 Interfaces

The DOR-MVD System shall exchange data with a variety of other computer systems including the Federal government, AAMVA, national entities (e.g., Organ Donor Tracking), South Dakota State agencies, Counties, Data Warehouses, and third parties (e.g., VINtelligence).

### 1.7.1 Interface General Requirements

- The DOR-MVD System shall initiate data exchanges both on specific system events and scheduled times including real-time.
- In general, the State will broker interfaces with existing state systems, resources, databases, etc.
- The DOR-MVD system shall adapt to business necessary interfaces using widely adopted open APIs and standards. Software services shall be available/exposed with published documentation that would enable third-party developers to interface other business applications.
- The DOR-MVD System shall support existing processes that currently interface with the existing systems not targeted for replacement. To reduce the development and maintenance effort associated with these interfaces, DOR requires that the system use, where feasible, a standard interface facility or utility. It is DOR's intent to reduce the overall number of interface programs, to streamline interface processes, and to use newer technological standards (EDI, web services) where feasible, to exchange data.
- The DOR-MVD system shall act upon data received from external systems and must extract and send data to external systems as mutually agreed upon.
- The DOR-MVD System shall provide automated interfaces to and from other internal systems and external systems to maintain and synchronize dependent data.
- The DOR-MVD System shall ensure security of all data transmitted through an interface.
- The DOR-MVD System shall include automatic validation processes with all interfaces to ensure that the number of records sent or received is consistent with the other node.

- The DOR-MVD System shall provide APIs and/or business rules to all interface partners ensuring that data sent to or sent by DOR-MVD meets all validation rules.
- DOR may, at its discretion, choose to interface with an existing system even when the core functionality is part of the Vendor's system (e.g., state's Explorer system, which provides IRP and IFTA functionality will not be replaced, but will be interfaced with).
- The Vendor shall recommend whether existing interfaces and extracts shall remain as they exist today, or potentially become display screens or reports in the DOR-MVD System.
- The Vendor shall develop an Interface façade for interface and exchange processing. This façade shall allow other systems to access information without directly accessing the DOR-MVD internal database.
- The DOR-MVD System shall support encrypted and key based integrations as part of its APIs.

### 1.7.2 Interfaces to a DOR Data Warehouse

As part of this project, the Contractor will implement a hosted Data Warehouse and the DOR-MVD System must interface and support the Data Warehouse. The State's prefers to have the data warehouse hosted in the State's FedRAMP certified platform.

### 1.7.3 Interface List

Please see Appendix J for a list of current and desired future state interfaces.