# Appendix 11 – Technical Requirements



See the RFP Section 1.2 and Task Order, Section 1.2 for a complete list of all abbreviations and acronyms.

# 1. Overview

The MVA expects to use DIWS 2 for other functions that are not currently included in DIWS 2 requirements. It is desirable that foundational subsystem functionality allows the MVA to build other base and business components in a common and consistent fashion.

As part of representing the full set of DIWS 2 requirements for the MVA, these Technical Requirements act as the desired set of technical requirements to be met by the Contractor's proposed solution. This appendix affords the Contractor with the opportunity to provide specific technical details of its proposed approach to meeting DIWS 2 requirements in each area.

The MVA requires a state-of-the-art solution that adheres to industry best practices and employs generally accepted industry frameworks, approaches and patterns. The proposed solution should balance the requirements presented in this appendix to provide a secure, reliable, flexible, enterprise level solution that is cost effective and realistic.

Proposals will be evaluated based on the completeness of the technical solution and, in the context of the overall solution, the extent to which expected and desired technical requirements are met.

# 2. General Requirements

To support the general requirement features and capabilities, **DIWS 2 shall**:

1. Include table driven configuration for multiple language support.
   - This refers specifically to the user interface(s) provided by DIWS 2. Multiple language support for content renditions is addressed in Appendix 5, Section 4.1 Content Creation.
2. Allow the user to interact using the user interface in the following languages:
   a. United States English
   b. Spanish
   c. Korean (desired, but not required)
3. Provide help text in the same language as the user interface.
4. Provide error message text in the same language as the user interface for those error messages originating from the ECM software.
   - For the purpose of this requirement, it is not necessary to translate error messages that originate from prerequisite software or the operating system.
5. Provide the ability to capture and present values, using the user interface or programming interfaces, that contain:
   a. single-byte characters
   b. double-byte characters
   c. multiple-byte characters
   - Consistent with a spirit of inclusion, the MVA prefers to have the option of being able to capture the information presented by its customers and partners with minimal transliteration.
   - An example is a DIWS 2 user interface that allows a user to enter Korean symbols, containing a mix of single and double-byte characters, into indexing fields. These values should be stored and properly displayed when retrieved. Searches for names containing these symbols should also be return the correct results.
   - A second example is an external application that captures information (e.g., names and notes) containing a mix of Swedish, German, Portuguese, French, and Chinese single and double-byte characters. The application uses the interface described in Appendix 10 External Systems Integration to store, search, and retrieve this information in DIWS 2.

# 3. Authentication, Access and Permissions

To support authentication, access and permissions, **DIWS 2 shall**:

1. Support access control via MS Active Directory (AD).
2. Authenticate users before allowing access to functionality requiring a login and validate that a user is authorized before displaying any information or allowing information to be changed or supplemented in any way.
3. Require that all passwords used in authentication are encrypted when stored in a database and ensure passwords are not revealed on a screen when typed.
4. As stated in Appendix 5, Section 6.4 Integration, Requirement 31, support a user authentication mechanism that offers single-sign-on access to all DIWS 2 functionality that requires user authentication or authorization.
5. Support an authentication mechanism that complies with State security requirements.
6. Support an authentication mechanism that accommodates users operating within the MVA network domain as well as users remotely accessing DIWS 2.
7. Allow definition of separate roles for a user accessing data from within the MVA network domain versus from outside the network domain.
8. Identify the location of a user that is authenticating inside the MVA network. Location shall include the:
    a. IP address
    b. Unique identifier associated with the physical hardware if available.
9. Be able to associate permissions with a user using one or more of the following access controls:
    a. User-based (access rights assigned to each user),
    b. RBAC; users are grouped by role and access rights assigned to these groups),
    c. Rule/Context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.).
10. Be capable of operating within an RBAC infrastructure conforming to ANSI INCITS 359-2004, American National Standard for Information Technology (NIST) – Role Based Access Control.
11. Enforce the most restrictive set of rights/privileges or accesses needed by users/groups or processes acting on behalf of users, for the performance of specified tasks.

12. Provide a mechanism to limit access to view/update information identified in the following sections based on user role, access rights and program rules:
    a. Appendix 5, Section 3 Capture Functionality Requirements
    b. Appendix 5, Section 4 Common ECM Requirements
    c. Appendix 5, Section 5 ECM Advanced Requirements
13. Provide central management of user account access privileges.
14. Ensure all roles are unavailable to users until explicitly granted.
15. Allow for a user's access to be temporarily or permanently blocked.
16. Allow the creation of temporary and emergency accounts, which are automatically disabled after a period of time defined by the administrator.
17. Not delete users from DIWS 2 to ensure history of user's identity and past actions.
18. Provide session management abilities such as session timeout, prevention of duplicate logins, remote logout and location-specific session timeouts.
19. Provide audit reports to identify inappropriate access to DIWS 2 within the constraints of captured audit data and State defined criteria.
20. Enforce role authorizations that control system access and the flow of information within DIWS 2 and between interconnected systems.
    - These are roles and authorizations for certain functionality. For example, a HR user should be allowed to access HR functionality and be prevented from accessing AP functionality.
21. Support uniquely identified users, devices, and processes using the assignment of unique user accounts/Logon ID.
22. Validate users (or processes acting on behalf of users) using standard authentication methods such as passwords, tokens, smart cards, or biometrics.
23. Provide a mechanism to prevent unauthorized devices from accessing the application.
    - An example would be restricting access to DIWS 2 by mobile devices such as smartphones and tablets to those known to the MVA. These devices may be allowed to access other non-DIWS 2 applications. Similarly, auditors and other infrequent visitors that are provided credentials for accessing DIWS 2 from an MVA desktop, may be prevented from accessing DIWS 2 from a laptop that they bring with them that is allowed on the network for other purposes.

24. Limit DBA permissions in a manner consistent with the principle of least privilege.
    a. Restricting the operations a DBA is allowed to perform to those specifically required to perform the tasks they are assigned.
    b. Limit the number of users who can have DBA permissions.
    c. Differentiating DBA roles appropriate to the tasks being performed (e.g., installation, maintenance, diagnostics).
25. Prevent database administrators from seeing the data in databases they maintain.
26. Support security using database access controls.

# 4. Interoperability and Integration

To support interoperability and integration, **DIWS 2 shall**:

1. Support a wide variety of synchronous and asynchronous messaging patterns including, but not limited to, the following:
    a. Data look-up and retrieval,
    b. Data look-up with services provided by other applications,
    c. Simple bulk data transfer to/from other systems,
    d. Non-repudiation
2. Provide a highly available infrastructure that will withstand and automatically recover from the failure or unavailability of individual technology components, including the network connection and database.
3. Interface requests shall employ store and forward features when an interface is unavailable.
4. Ensure the DIWS 2 interfaces are scalable to accommodate changes in scale including changes in:
    a. User population,
    b. Transaction volume,
    c. Throughput,
    d. Geographical distribution,
5. Support the ability to make changes to the interface data elements/layouts without coding and easily test those changes.
6. Implement a modular interface architecture so that, throughout the implementation and over time after the system is in production, interfaces can be added in a consistent manner by defining an XML schema, mapping to the database, and definition of the source service.
7. Ensure DIWS 2 interfaces are implemented using enterprise integration middleware and an enterprise service bus.
8. Provide the ability to integrate with legacy systems using point-to-point methods and secure file transfer.
9. Perform source to destination file integrity checks for exchange of data and alert appropriate parties of issues.
10. Publish services and related data to be used by different types and classes of service consumers.
11. Protect all DIWS 2 communications and messaging by at least 2048-bit encryption with the capability to upgrade in the future.
12. Base all DIWS 2 message and data formats on logical representations of business objects rather than native application data structures.

13. Ensure all DIWS 2 data transformations are to and from normalized formats.
14. Ensure DIWS 2 implemented SOA services are attributed with one of the following SOA Lifecycle Status values: Candidate, Justified, Defined, Designed, Implemented, Operational, or Retired.
15. Ensure DIWS 2 SOA-related messages are formally defined with XML Schema Definition (XSD).
16. Implement DIWS 2 SOA-related services hosted using .Net.
17. Support creation and extension of service interfaces through the use of Web Services Description Language (WSDL).
18. Ensure DIWS 2 WSDLs developed for the project conform to the WSDL Development Standards.
19. Ensure DIWS 2 implemented services rely on Web services-Policy configurations for message reliability (Web services-Reliable Messaging).
20. Ensure DIWS 2 metadata attributes are tracked for all services in the services catalog: name, lifecycle status, class, description, owner, version, revision history, release frequency, versioning policy, deprecation policy, message exchange patterns, compensating transaction support, availability requirements, volume, max message size, security attributes, SLA, logging requirements.
21. Be designed, built and deployed with enterprise architecture best practices including substantial reliance on highly configurable SOA components and provide the flexibility to add new environments as needed by the MVA.
22. Provide reliable, once-only delivery and in-order delivery/receipt of messages and allow messages to be configured for guaranteed delivery, as required.
23. Provide functionality that provides reliability for applications, services and message flows to include any of: load balancing, high availability, fault tolerance, automated failover, transaction support (ACID; atomicity, consistency, isolation, durability), execution prioritization and message prioritization.
24. Have the capability to integrate with enterprise service bus technology to perform syntactic and semantic hub-based transformation of messages, including: support of taxonomy, reusable transformation maps, built-in transformation functions, and extending the transformation function with custom-coded logic, as needed.

25. Integrate with other applications/systems via a SOA and event-driven architectures in a manner similar to one or more of the following implementation strategies: Web Services: Web Services Interoperability (WS-I). Organization-compliant implementation of basic Web services standards, including SOAP, WSDL and Universal Description, Discovery and Integration (UDDI), as well as higher-level Web services standards, such as WS-Security, Representational State Transfer (REST). Support for both XML and JSON-based messages and processing along with HTTP, HTML 5 and XHTML.

26. Support, as business requirements dictate, storage of data locally while DIWS 2 is offline and synchronization of that data with the remote server once DIWS 2 is back online.

27. Track all messages from origin to destination (inside a firewall), and allow an authorized user to inquire on the status of any message and address exceptions (e.g. resend the message if a target times out).

28. Have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP.

29. Work with the security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing).

# 5. Regulatory and Security

To support the regulatory and security needs of MVA, **DIWS 2 shall**:

1. Comply with and maintain compliance with appropriate State or federal legislation including:
    a. The sub-parts of Section 508 of the Americans with Disabilities Act (ADA)
    b. Driver's Privacy Protection Act of 1994 (DPPA)
    c. The Privacy Act of 1974, 5 U S C § 552 a, Public Law No 93-579,
    d. Federal Information Security Management Act of 2002 (FISMA),
    e. Maryland State Gov't Code such as Ann §§10-1301 – 10-1308 (protection of personal information) and other Maryland law pertaining to security and safeguarding.
    f. Maryland State Gov't Code such as 45 CFR 85 and all State of Maryland accessibility requirements.
    g. Code of Maryland Regulations (COMAR) 14.33.02.00-12 – , http://www.dsd.state.md.us/comar/SubtitleSearch.aspx?search=14.33.02.*
2. Remain in compliance with new or changed laws.
    a. The Contractor shall be responsible for staying abreast of State and federal legislation in order to keep DIWS 2 in compliance with new or changed laws.
3. Comply with security requirements and safeguards of the following agencies/entities:
    a. Maryland Department of Transportation (MDOT),
    b. MDOT Office of Transportation Technology Services (OTTS),
    c. MDOT Motor Vehicle Administration Office of Information Resources (MVA/OIR),
    d. Maryland Department of Information Technology (DoIT),
    e. National Institute of Standards and Technology (NIST).

4. Comply with all applicable State security policies and adhere to all legal, statutory, and regulatory requirements, as determined by Maryland leadership and detailed in:

    a. State of Maryland Policy,
    b. MDOT Security Policy,
    c. MVA Security policies,
    d. The State of Maryland System Development Life Cycle (SDLC) methodology at: www.DoIT.maryland.gov - keyword: SDLC,
    e. The State of Maryland Information Technology Security Policy and Standards at: www.DoIT.maryland.gov - keyword: Security Policy,
    f. The State of Maryland Information Technology Non-Visual Standards at: http://doit.maryland.gov/policies/Pages/ContractPolicies.aspx,
    g. Nonvisual Access Guidance: Regulation .05 Web-based intranet and internet information and applications at http://doit.maryland.gov/policies/Pages/NVAReg05.aspx,
    h. The State of Maryland Information Technology Project Oversight at: www.DoIT.maryland.gov - keyword: IT Project Oversight

5. Comply with MDOT Incident Reporting Policy and MVA Breach of Security Protocol.

    - For more information, see DIWS 2 RFP, Main Body, ATTACHMENT A, Section 16.17, Security Requirements and Incident Response
    - For more information, see Information Security Policy v3.1, http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf

6. Comply with MVA Record Disposition / Destruction Security Controls.

    - For more information, see Information Security Policy v3.1, http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf

7. Comply with MVA Third Party Data Security Controls.

    - For more information, see Information Security Policy v3.1, http://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf

8. Implement security controls in accordance with all relevant federal and State security policies and regulations.

9. Adhere to the principle of "Fail Safe" to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks.

10. Be built to prevent corruption or loss of data already accepted into DIWS 2 in the event of a system failure.

11. Display a configurable pre-login banner or warning (e.g. "System shall only be accessed by authorized users") prior to accessing any PII. In the event that DIWS 2 does not support pre-login capabilities, System shall display the banner immediately following authorization.

12. Not record sensitive data in debug logs or other application logs created by custom code or COTS components unless the PII data is encrypted.
13. Provide sufficient storage to record all necessary auditable items.
14. Be configured to audit, at a minimum, the following:
    a. type of event
    b. date and time of the event
    c. source of the event
    d. success or failure of the event
    e. identity/logon ID of the user associated with the event
15. Support logging based on selectable event criteria and produce audit reports.
16. Retain (for a configurable retention period) the aforementioned logs necessary to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation.
17. Monitor the aforementioned logs necessary to identify suspicious or questionable activity and report any suspicious or questionable activity to the State.
    - See also Section 5 Regulatory and Security, Requirement 21.
18. Support the protection of audit information and audit tools from unauthorized access, modification, and deletion.
19. Be configured to monitor and control communications at key internal boundaries (for example web servers, application servers, database servers) within DIWS 2.
20. Capture and store audit records for all security-relevant events, including all security, DBA and system administrator accesses.
21. Include procedures that routinely review and track audit records and transaction logs for indications of unusual activities, suspicious activities or suspected violations, authorization of system level changes, and documenting and controlling system level changes. Reports detailing the findings from these procedures shall be produced by DIWS 2 for authorized users.
22. Be subject to MDOT security/vulnerability scanning.
    a. The Contractor shall remediate any non-compliant results in a timely fashion.
    b. The Contractor shall not deploy any application to production that contains known vulnerabilities for which a generally accepted remediation is available.

23. Prevent further viewing and access to DIWS 2 upon detecting inactivity of an interactive session by either:
    a. Terminating the session, or
    b. Initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.
    c. The inactivity timeout shall be configurable and support MDOT policy.
24. Enforce a limit of (configurable) consecutive invalid access attempts by a user. 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 MDOT policy.
25. Include an up-to-date directory of all personnel who currently use or access DIWS 2 and/or databases and includes the user's role(s). This directory shall support defined MDOT policy.
26. Support the creation and utilization of data sensitivity classification.
27. Support the creation and utilization of data security classification.

**The DIWS 2 Contractor shall**:

28. Provide security reports to the State in a mutually agreeable format beginning when the system is placed into production.
    a. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to DIWS 2.
    b. The security reports shall occur at a frequency determined by the MVA Project Manager.
29. Ensure that test and training environments that allow access from outside of the State's LAN shall be subject to the same security requirements as those for production environments.
30. Subject the workstations used by Contractor Personnel to periodic, State and Contractor performed audits (MVA Project Manager to define the frequency) to ensure compliance with State security policies.
    a. A report detailing findings and remediation actions (as required) shall be delivered to MVA for review.
    b. The Contractor shall execute all security-related remediation actions within one business day of providing the report unless a different time period is granted by the MVA Project Manager.

31. The Contractor shall implement administrative, physical and technical safeguards to protect State data that are no less rigorous than accepted industry practices for information security, such as those listed below (see Section 5 Regulatory and Security Requirement 32), 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 and TO.

32. To ensure appropriate data protection safeguards are in place, at minimum, the Contractor shall implement and maintain the following controls at all times throughout the term of the Task Order (the Contractor may augment this list with additional controls):

    a. Establish separate production, test, and training environments for systems supporting the services provided under this Task Order and ensure that production data is not replicated in test and/or training environment(s) unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements. The Contractor shall ensure the appropriate separation of production and non-production environments by applying the data protection and control requirements listed in Section 5 Regulatory and Security Requirement 32.
    b. Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides, Security Technical Implementation Guides (STIG), or similar industry best practices to reduce the surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible and/or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the system configuration files.
    c. Ensure that State data is not comingled with non-State data through the proper application of compartmentalization security measures.
    d. Apply data encryption to protect Sensitive Data at all times, including but not limited to when at rest and also when archived for backup purposes. For all State data the Contractor manages or controls, data encryption shall be applied to such data in transit over untrusted networks. Encryption algorithms which are utilized for this purpose must comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-2:
    http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

e. Enable appropriate logging parameters to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards, including Maryland Department of Information Technology's Information Security Policy.

f. Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation, if required. The Department or Agency shall have the right to inspect these policies and procedures and the Contractor's performance to confirm the effectiveness of these measures for the services being provided under this Task Order.

g. The Contractor shall:

A. Ensure system and network environments are separated by properly configured and updated firewalls.

B. Restrict network connections between trusted and untrusted networks by physically and/or logically isolating systems from unsolicited and unauthenticated network traffic.

C. By default "deny all" and only allow access by exception.

D. Review at regular intervals (no less than yearly) the aforementioned 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.

h. Perform regular vulnerability testing of operating system, application, and network devices. Such testing is expected to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with or deviations from the security policy applicable to this Task Order, as identified in 1.1.8.2 item 2. Contractor shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and remediate the vulnerability no later than 30 days following the earlier of vulnerability's identification or public disclosure, or document why remediation action is unnecessary or unsuitable. The Department or Agency shall have the right to inspect the Contractor's policies and procedures and the results of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this Task Order.

i. Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current State of Maryland Department of Information Technology's Information Security Policy (http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx),

including specific requirements for password length, complexity, history, and account lockout.

j. Ensure Sensitive Data is not processed, transferred, or stored outside of the United States.

k. Ensure Contractor's Personnel shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State, which may be revoked at any time for any reason. The Contractor shall complete any necessary paperwork as directed and coordinated with the Task Order Manager to obtain approval by the State to connect Contractor-owned equipment to a State LAN/WAN.

l. Ensure that anti-virus and anti-malware software is installed and maintained on all systems supporting the services provided under this Task Order; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation. The Contractor shall perform routine vulnerability scans and take corrective actions for any findings.

m. Where website hosting or Internet access is the service provided or part of the service provided, the Contractor and/or Subcontractor shall conduct regular external vulnerability testing. External vulnerability testing is an assessment designed to examine the Contractor and/or Subcontractor's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. The Contractor and/or Subcontractor shall evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the system's security and/or integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The Department or Agency shall have the right to inspect these policies and procedures and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under this Task Order.

33. Provide security reports to the State in a mutually agreeable format beginning when the system is placed into production.

a. The security reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State files related to DIWS 2.

b. The security reports shall occur at a frequency determined by the MVA Project Manager.

# 6. User Interface

To support the user interface, **DIWS 2 shall**:

1. Provide a UI that accommodates diverse populations of users including those with disabilities and limited English proficiency as defined in section 504 of the Rehabilitation Act of 1973.
2. Provide a UI where all of the components look like they are part of the same system and be consistent in appearance to all users.
3. Provide a UI that visually identifies the mandatory fields (i.e. requiring user input) on each screen.
4. Validate that all mandatory data fields have been completed when a user attempts to save information.
5. Allow the user to review and update all entered/captured information before final submission.
6. Allow users to go back to prior screens during the processing of a transaction to adjust data and information and continue processing without cancelling the transaction.
7. Automatically save information as users enter data, thus reducing/eliminating the need to click a Save button.
8. Interactively inform the user of errors based on real-time validations performed as the user enters data.
9. Provide a context sensitive help function that utilize state-of-art User Interface/User Experience (UI/UX) features and functions.
10. Ensure that all codes and abbreviations used in DIWS 2 have corresponding and easy-to-view narrative descriptions.
11. Provide a free-form text note capturing capability that:
    a. Provides basic word processing functionality such as sentence case, spell check, auto text, bold, underline, italics, color font, bulleted lists, tabs, indents, wrap-text, tables, and printable output,
    b. Allows input to be limited by character count and character set.
12. Support the ability to copy/paste data from one application Graphical User Interface (GUI) to another.
13. Provide a GUI that presents text and graphics in standard formats that are supported by the top-5 desktop browsers in the USA as reported by StatCounter Global Stats.

14. Provide a GUI that presents text and graphics in standard formats that are supported by the top-5 mobile browsers in the USA as reported by StatCounter Global Stats.

15. The GUI shall maintain compatibility with the top five (in the USA as reported by StatCounter Global Stats) desktop browsers and currently supported versions of each, during development and ongoing operations and maintenance activities.

16. The GUI shall maintain compatibility with the top five (in the USA as reported by StatCounter Global Stats) mobile browsers and currently supported versions of each, during development and ongoing operations and maintenance activities.

17. Provide a single responsive GUI that runs on mobile devices as well as desktop devices:

    a. As long as the device's browser is compatible with DIWS 2,
    b. Optionally, DIWS 2 may reformat or reconfigure the GUI to the size of the screen.

18. When appropriate, limit the amount of information displayed, while also enabling the user to immediately expand the scope of the information visible.

19. Provide for a basic level of intuitive processing by directing users to alternative actions when a requested action cannot be completed due to business rule constraints.

20. Provide a UI and navigation that is simple, consistent, and to the extent permitted by business requirements, provides for undoing user input.

    - For the purpose of this requirement, "undoing user input" applies to actions and transactions that span multiple screens. A user should be able to have the system forget the information entered on a prior screen if that screen is part of a multiple screen activity.

21. Allow changes to the user interface layout (e.g., text positioning, font size, field size, field positioning, field tab order, adding/removing logos and images, revealing hidden fields, hiding fields, adding, and removing text) to be made without requiring the application to be rebuilt.

22. Allow changes to server components to be made without requiring the user interface to be rebuilt.

23. Allow changes to be made to any component of the user interface that is already available or can be made available as static content (i.e., not provided by the underlying business application), without requiring the need to rebuild the application.

24. Allow any component of the UI that is already available or can be made available as static content (i.e., not provided by the underlying business application), without requiring the need to rebuild the application."

25. Have a primary UI (including warnings, notifications and user prompts) that is free of grammatical and typographical errors.

# 7. Application Domain

To support the application domain, **DIWS 2 shall**:

1. Support SQL.
2. Manage all configuration parameters that are subject to user modification using table-driven designs and be maintainable via UI.
3. Support standard MIME file types.

The following application development and support tools are preferred by MVA:

4. The MVA currently develops and maintains multiple .Net applications using C# and this is the preferred application development language/framework.
5. The MVA uses Microsoft Outlook and Microsoft Exchange hosted and managed by MDOT
6. The MVA uses the Microsoft Office Suite (currently version 2010)
7. The MVA uses MS Visio.
8. The MVA's preferred DBMS is Microsoft SQL Server
9. The MVA uses StarSQL
10. The MVA uses Maximo for Change and Service Request Tracking
11. The MVA uses PCVS for defect tracking and software change requests
12. The MVA uses CA ERwin Data Modeler (currently version 9.6 and CA ERwin Mart for DB modeling
13. The MVA uses Microsoft TFS (currently version 2013) for support system development activities
14. The MVA uses Git for code version control
15. SyncSort
16. The MVA uses SharePoint (currently version 2013) for team collaboration, knowledge management, project repository, and workflow to support system development and operations
17. The MVA uses Microsoft Project (currently version 2010; going to 365 for the subscription version and 2013 for the client version)
18. The MVA uses Microsoft Project Server (currently version 2013)

19. The MVA uses the following tools from Information Builders:
    - 19.1. WebFOCUS Client
    - 19.2. WebFOCUS Reporting Server
    - 19.3. iWay Data Migrator
    - 19.4. iWay Data Quality Server

# 8. Database Domain

To support the database domain, **DIWS 2 shall**:

1. Employ a relational data model with referential integrity constraints.
2. Provide support for connectivity as required by the MVA. Current connectivity options are ODBC, JDBC and StarSQL.
3. Support the ability to share queries.
4. Use a database that supports MVA's existing Information Builders Business Intelligence tools.

# 9. Networking Domain

To support the network domain, **DIWS 2 shall**:

1. Support SNMP V3 use.
2. Support ISDN as required.
3. Support VLANs.

# 10. Platform Domain

To support the platform domain, **DIWS 2 shall**:

1. Be built and packaged to allow deployment to multiple State provided data center facilities or facilities hosted by a 3rd party.
2. Provide ability to send output to any of the following end-points: printers, file storage, e-mail, fax machines and SFTP.
3. Integrate with the current agency e-mail solution.
4. Be able to deploy its server platform in a virtual environment.

# 11. Enterprise Systems Management (ESM) Domain

To support the ESM domain, **DIWS 2 contractor shall**:

1. Ensure DIWS 2 is able to track and report usage by various business units to support financial management activities related to IT services chargeback/showback.
2. Ensure DIWS 2 can track the usage and time spent on screens and provide raw data needed to analyze system and transaction performance.
3. Engineer the DIWS 2 components so as not to prevent the use of compatible, MVA approved utilities, diagnostics, and systems management tools, including the installation of server agents, to monitor events on the information system, detect attacks, and provide identification of unauthorized attempted access.
4. Contractor shall be responsible for task and job scheduling, using MVA's provided tools or Contractor proposed alternatives, during development and ongoing operations and maintenance activities.

## 11.1 ESM Tools

To support the ESM domain, **The Contractor's tools shall**:

1. Provide monitoring capability at the transaction level providing detailed logging into an MVA-provided ESM toolset or the Contractor's proposed alternative and be capable of exporting data to other standards-based ESM tools.
2. Support an Enterprise Information Integration (EII) Tool using MVA's provided tools or Contractor proposed alternatives.
3. Include tools and/or features required to provide SLA monitoring and reporting capabilities.
4. Be provided by the Contractor unless specifically specified in this TO as being provided by the State.

# 12. System Administration and Disaster Recovery

To support system administration, **DIWS 2 shall**:

## 12.1 System Administration

1. Have the ability to generate administrative alerts and warnings when statistics indicate an impact or potential limits on system SLA for performance, and availability, including projection of storage capacity.
2. Communicate administrative alerts and warnings through various mechanisms including SMS, phone and e-mail using MDOT/MVA approved tools.
3. Provide system monitoring functionality according to industry best practices.
4. Provide logging and reporting for assessing errors and exceptions.
5. Provide system administration functions that simplify repetitive tasks (e.g. reference table maintenance and adding/removing/changing role and/or authorization for a user)
6. Support monitoring of back-up and recovery processes, including projection of storage capacity.
7. Provide an automated real-time capability to track and monitor performance of all system components (end-to-end).
8. Identify control points and classify those controls as preventive or detective or corrective.
9. Provide automated reports on control inventory to indicate strengthening or weakening control environment.
10. Quantify control measure in term of number of built-in controls.

## 12.2 Disaster Recovery

To support disaster recovery, **The Contractor shall**:

1. Develop and document a system continuity and recovery strategy consistent with identified requirements. The strategy shall address and identify all aspects of DIWS 2 relevant to creating continuity and recovery capabilities and procedures including, but not limited to, system design, architecture, construction, implementation; operational considerations (e.g. backup scheme); and any considerations internal or external to DIWS 2 necessary to support or execute the recovery strategy.

2. Provide a DIWS 2 continuity and recovery strategy and plan that includes considerations for recovery from both disaster and non-disaster (e.g. hardware failure) events.
3. Design, develop, and implement disaster recovery capabilities and procedures for DIWS 2.
4. Provide a DIWS 2 continuity and recovery strategy that specifically address data integrity by taking into account data dependencies across subsystems, and shall ensure data integrity when recovering from disaster or non-disaster events. For example, a transaction written to a database that is dependent on content in the ECMS shall ensure both transactions are restored to the same point in time meeting the Recovery Point Objectives (RPO) requirements of both components and subsystems.
    a. The DIWS 2 continuity and recovery strategy shall also include a definition of the steps for remediation of discrepancies.
5. Perform activities and provide deliverables that are consistent with the following MDOT and DoIT Disaster Recovery Plan (DRP) standards including:
    a. State of Maryland Information Technology (IT) Disaster Recovery Guidelines,
    b. Sample Disaster Recovery Report, Maryland Department of Budget and Management (DBM).
6. Perform disaster recovery activities and provide disaster recovery while the system is being maintained and at all times after the system is first placed into production.

7. Provide a DIWS 2 continuity and recovery strategy documentation that is developed and kept up to date by the Contractor and includes:
    a. Documentation sufficient to create a business impact analysis consistent with Continuity of Operations Planning (MDOT and DoIT) Standards
    b. Documentation necessary to establish RTO and RPO for services implemented or supported by DIWS 2.
    c. Documented time sensitivity requirements, elicited during the development of use cases and system designs.
    d. DIWS 2 recovery procedures, identifying tasks and order of operations necessary to execute the recovery strategy and plan. The recovery timeline shall include initial reaction to the disruptive event, establishment of degraded or partial services (e.g. failover), continued operations in degraded mode, and return to normal operations (e.g. failback).
    e. The findings of a system risk assessment. The assessment shall include system-level business continuity- and disaster recovery-related risks including, but not limited to, hosting location or infrastructure considerations, physical threats, electronic attacks, and system or infrastructure failures. The risk assessment shall include enumeration of possible disruption events.
8. Contractor shall provide a backup and restore solution sufficient to meet the RPO and Recovery Time Objectives RTO. Contractor shall implement a backup and restore solution sufficient to restore a consistent state across all DIWS 2 subsystems.
9. Develop database specific system recovery strategies which address MVA business requirements.
10. Ensure that DIWS 2 supports point-in-time and point-of-failure recovery.
11. Ensure that DIWS 2 supports backup of all system data, configuration files, metadata, server images and other artifacts as required to recover DIWS 2 to an alternate location.
12. DIWS 2 shall support disk-to-disk backup for all platforms using MVA's provided tools or Contractor proposed alternatives.
13. Perform backups of all systems and servers. Minimally, this shall include daily incremental backups and full weekly backups of all volumes of all systems and servers, as necessary to meet recovery point and recovery time objectives.
14. Encrypt all backups using a shared key.
15. Retain daily backups for one month, and weekly backups for two years.
16. Store daily backups off-site at an MVA designated location.

17. Perform a full system recovery from the most recent backups at least semi-annually beginning six months after the system is in production.
    - The recovery is not expected to be into the production environment. The MVA Project Manager will designate the environment to be used for the recovery.
18. Support the State's recovery of a backup set on demand.
19. Deliver high-availability between data centers with no loss of system functionality or data in the event of a data center outage.

    New and in-flight transactions shall automatically fail-over to the alternate location.

# 13. Contractor Architecture and Engineering Tasks

In performing the architecture and engineering asks, **the Contractor shall**:

1. Create system architecture documentation artifacts modeled per International Standards Organization/IEC/IEEE 42010 Architecture Description Template in support of The Open Group's Architecture Framework (TOGAF).
2. Document stakeholder/owners identified following the TOGAF Architectural Development Method (ADM) Architecture Model Role Matrix.
3. Participate in the maintenance of the MVA Enterprise Architecture Repository, beginning within 60 days of NTP, by:
    a. Participating in the weekly Enterprise Architecture Governance Board (EAGB) meeting
    b. Ensuring that all new technology is presented to the EAGB for review, discussion and final approval/disapproval
    c. Preparing presentation materials for EAGB topics
    d. Updating the EA registries in SharePoint, as required to reflect changes introduced by the Contractor and approved by the EAGB
4. Review, classify and catalog system services in a services catalog within the MVA Architecture Repository
5. Develop and document user account management procedures to include
    a. Obtaining authorization from appropriate officials to issue user accounts to intended individuals,
    b. Disabling user accounts in a timely manner,
    c. Archiving inactive or disabled user accounts,
    d. Developing and implementing standard operating procedures for validating DIWS 2 users who request reinstatement of user account privileges suspended or revoked by information systems
6. Maintain application development related documentation using MS TFS.
7. Utilize the MS TFS Application Life-cycle Management Tool.
8. Use MS TFS/Git for source code versioning and repository.
9. Follow and support the International Standards Organization (ISO) Open Systems Interconnect (OSI) reference model including TCP/IP when making any network decisions.
    a. All network related decisions shall also follow existing MDOT data communications enterprise network standards and infrastructure.

10. Install and maintain software and licenses for software proposed and/or required for use on DIWS 2 and be able to determine where and for whom the software is or was installed.
    - See related requirement in RFP section 3.10 that discusses the transfer of the license to the State's name.
11. If developing a solution from scratch, use the .Net framework and C# programming language.
12. If using .Net, follow existing or provided modern .Net Guidelines and follow similar guidelines when using other technologies.
13. Support policy-based storage management as required by MVA and MDOT procedures.
14. Map "rules/regulations documentation" to relevant context of the applicable screen/process and prepare documentation for the MVA-provided Knowledge Management sub-system.
15. The obtain approval from the State for all DIWS 2 hardware and software prior to installation and use.
16. Facilitate deployment of DIWS 2 to internal data centers and, as required, data centers hosted by a 3rd party.
17. Provide a means of periodically testing DIWS 2 recovery procedures. Provide tools, instrumentation, procedures, and documentation sufficient to enable future periodic testing of the production system recovery capabilities by MVA staff.
18. Perform a full system recovery from the most recent backups at least semi-annually after the system is in production.
    - The recovery is not expected to be into the production environment. The MVA Project Manager will designate the environment to be used for the recovery.
19. Periodically test the ability to recover DIWS 2 to an alternate location using their documented tools, instrumentation, and procedures. Recovery shall be tested from normal, regularly scheduled backups of the production system data and demonstrate that DIWS 2 functionality, data integrity and data currency is maintained and that performance remains within SLA boundaries.
20. Establish a comprehensive data dictionary and master data model and represent in ERwin.
21. Install and configure an ESM tools including the installation and configuration of agents on DIWS 2 components.

# 14. Response to Technical Requirements

The table below identifies the topics which the Offeror shall address in its Technical Proposal. Each topic in the response shall be identified with a heading corresponding to the table below. Responses should not be placed in the table.

Offeror shall refer to the referenced section of the Task Order to fully understand the State's requirements and expectations when preparing the response. The Offeror shall address the topics/questions identified in the table but is expected to elaborate or add additional information as appropriate to fully understand the Offeror's solution and approach.

The Offeror should provide a detailed description of the proposed solution but does not need to address every item or sentence in a particular section. The Offeror's response shall be construed to be inclusive of all requirements referenced by the table and shall bind the Offeror to all such requirements unless the Offeror specifically addresses partial or non-compliance in its response. Offerors shall describe requirements that cannot be met or that can only partially be met as part of the final question of the response table.

The Offeror shall adhere to any page limit for the topic.

In some topics below, the State has requested a sample of work from a previous project or a draft version of an artifact for this project (e.g. include a draft Project Plan for this project). These items are identified below and shall be included in [TAB O] and not inserted into the narrative. Such items are not included in page limits. If requested items are not available, briefly describe.

| **Response Requirements**<br>**Appendix 11 Technical Requirements** | | | |
|---|---|---|---|
| **Appdx Ref** | **Topic Title** | **Response Requirements** | **Page Limit** |
| 2 | General Requirements | Describe your approach to meeting the requirements in section 2. | |
| 3 | Authentication, Access and Permissions | a. Describe your technical solution for creating an access control system that supports role based, rule based and user-based authorizations. Elaborate on the features of the proposed DIWS 2 that will regulate access to transactions and system resources based on role, location and other limiting factors,<br>b. Explain how your proposed system will integrate with MVA's existing Active Directory infrastructure and provide easy to use tools to manage roles and permissions.<br>c. Explain how you propose to protect sensitive information from being accessed by database | |

| **Response Requirements**<br>**Appendix 11 Technical Requirements** | | | |
|---|---|---|---|
| **Appdx Ref** | **Topic Title** | **Response Requirements** | **Page Limit** |
| | | administrators and others with super user access/authorization. | |
| 4 | Interoperability and Integration | a. Describe your technical solution for creating a reusable, configurable interface engine. Specifically describe your solution for implementing the following types of interfaces:<br>1. Real-time<br>2. Batch<br>3. Point to point<br>b. Describe your general approach for implementing interfaces, including initial discovery, requirements definition, and testing.<br>c. Describe any requirements in section 4 that you cannot meet.<br>d. An overview discussion about your approach to the Interface Engine is requested in the response to Appendix 5. Your response here should be fully elaborated from a technical perspective. | |
| 5 | Regulatory and Security | a. Describe how the Contractor maintains physical and logical security relative to the solution and services it provides. This should include an overview of the policies, standards and practices to prevent, detect, and resolve security breaches.<br>b. In addition, the Offeror shall demonstrate experience and the ability to meet all federal and state regulatory requirements (e.g., fraud detection, data privacy, data protection [including sensitive data] and data loss prevention, Security Information and Event Management [SIEM] capabilities).<br>c. Describe the Offeror's approach to meeting IT accessibility standards, capabilities, and features as part of the proposed DIWS 2. This includes the provisions for MVA Regulatory and Security standards and compliance with all referenced Maryland IT Nonvisual Access (NVA) regulatory standards. | |

| **Response Requirements**<br>**Appendix 11 Technical Requirements** | | | |
|---|---|---|---|
| **Appdx Ref** | **Topic Title** | **Response Requirements** | **Page Limit** |
| 6 | User Interface | a. Describe the design approach and the characteristics of the UI for the proposed DIWS 2.<br>b. Describe your use of implementation tools including a rich Internet application framework.<br>c. Describe your approach to maintaining design standardization across internal and web/customer facing screens.<br>d. Describe how your tools and approach can support the implementation of functionality specifically designed to run on a smartphone platform, which is not an in-scope requirement, but is desired in the future. | |
| 7 | Application Domain | Describe the Offeror's approach to providing application domain capabilities and features as part of the proposed DIWS 2. This includes provisions for MVA regulatory and security standards, languages used in developing large new and complex applications anticipated to have high usage volumes and/or long life spans, vendor support, automation, standards, documentation, and repository usage. | |
| 8 | Database Domain | a. Describe the Offeror's approach to providing database domain capabilities and features as part of the proposed DIWS 2. This includes the provision for MVA regulatory and security standards, database support, DBA availability, production databases, controls, recovery, security, data modeling tools, Enterprise Information Integration, planning, etc.<br>b. Describe the Offeror's approach to providing information domain capabilities and features as part of the proposed DIWS 2. This includes the provision for MVA regulatory and security standards, information classification, analysis tools, policies, governance, SQL standards, software tools, data sensitivity/security and OLAP support. | |

| **Response Requirements**<br>**Appendix 11 Technical Requirements** | | | |
|---|---|---|---|
| **Appdx Ref** | **Topic Title** | **Response Requirements** | **Page Limit** |
| 9 | Networking Domain | Describe the Offeror's approach to providing networking and telecommunications domain capabilities and features as part of the proposed DIWS 2. This includes provisions for MVA regulatory and security standards, communications, networks, software products, SNMP, standards, protocols, ISO OSI standards, LAN, WAN, communications processors, telecommunications, etc. | |
| 10 | Platform Domain | a. Describe the Offeror's approach to providing platform domain capabilities and features as part of the proposed DIWS 2. This includes the provisions for MVA regulatory and security standards, storage, production deployment, private/hybrid cloud, platform management, servers, virtual environments, backup planning, capacity planning, standards, etc.<br>b. Offerors that include a private/hybrid cloud solution or component shall document their approach to deployment, specifically identifying:<br>1. Procedures required for production deployment of DIWS 2<br>2. Challenges and risks associated with production deployment of DIWS 2.<br>3. Management, visibility and control over production deployment of DIWS 2.<br>4. Governance and best practices for production deployment of DIWS 2. | |
| 11 | Enterprise Systems Management (ESM) Domain | Describe the Offeror's approach to providing Enterprise Systems Management Domain capabilities and features as part of the proposed DIWS 2. This includes the provisions for MVA regulatory and security standards, management, support, toolsets, ESM, future integration, monitoring, reporting, logging capabilities, change management, administrative policy adherence, controls and practices. | |

| **Response Requirements**<br>**Appendix 11 Technical Requirements** | | | |
|---|---|---|---|
| **Appdx Ref** | **Topic Title** | **Response Requirements** | **Page Limit** |
| 12 | System Administration and Disaster Recovery | a. The Offeror must provide a narrative overview of how the proposed solution shall meet DIWS 2 Administration and Disaster Recovery requirements including MVA Regulatory and Security standards, recovery documentation, recovery strategy, disaster recovery plans, and MVA requirements elicitation.<br>b. Describe your approach to operational management and explain how it aligns with the State's strategy, as outlined in section 1 – Overview, in this document. Additionally, describe automated and manual tools proposed as well as details on recommended processes to ensure effective system control, reliability, documentation, and recovery.<br>c. Describe the Offeror's approach for the proposed solution to meet Performance Standards related to MVA Regulatory and Security standards, response time, reporting, interactions, system availability, Dashboards, system maximum lookup performance, screen refresh, SLRs and interactive system transactions. | |
| 13 | Contractor Architecture and Engineering Tasks | Describe the Offeror's approach to meeting the requirements in this section. | |
| | Requirements not Met | The State assumes that the Offeror will meet all requirements described in Appendix 11 of the TO. For each section of this appendix, identify any requirements that cannot be met, why these requirements cannot be met, and any alternative proposed. | |