Appendix 10 – DIWS External Systems Integration

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

All requirements contain the word "shall" which may be part of the sentence containing the requirement or precede a list of requirements.

For requirements that include a lettered list, the lettered list is considered to be part of the requirement.

For requirements that contain a bulleted list, the bulleted list is provided for clarification, interpretation, reference, definition or example.

1. Overview

DIWS 2 provides a general purpose interface for other applications and external systems to interact with DIWS 2. One of these external systems will be the Project Core System that will use DIWS 2 to capture, receive, store, retrieve, manage, transmit and process operational unstructured content in the DIWS 2 repository. The Project Core System is MVA's primary computer system which supports, vehicle services, driver licensing services, driver enforcement services, business licensing services, financial operations and document imaging and workflow.

The Project Core System is expected to use DIWS 2 for storing and managing all operational unstructured content and documents other than check images. DIWS 2 shall support the Project Core System and other external systems with similar needs by providing, supporting and maintaining an interface.

2. General Information – DIWS 2 External System Integration

Legacy DIWS currently manages approximately **300** million images, approximately **30** TB of storage, and approximately **5 TB** of structured data. Legacy DIWS has over **450** named users using a browser interface, including **100** concurrent users using a client-server interface. This content from legacy DIWS will be migrated into DIWS 2.

Also, approximately **100** million images driver's photos, signatures, and supporting documents exist in an external system and will be migrated into DIWS 2. The migration of this content is discussed in Appendix 9 Legacy Migration.

One of the mechanisms external systems use for accessing the migrated content, and content that is added over time, is the external system integration capabilities discussed in Appendix 10. **All content stored in DIWS 2 shall be accessible using both the DIWS 2 user interface and the DIWS 2 External System interface.**

DIWS 2 provides the following services for external systems that need to access DIWS 2:

- Accepts content and indexing information from the external system, saves the content in the DIWS 2 repository, and returns a DIWS 2 identifier that can be used to retrieve the content in the future.
- Accepts non-resident content description and indexing information from the external system, saves the content in the DIWS 2 repository, and returns a DIWS 2 identifier that can be used to retrieve the non-resident content description in the future.
- Accepts a DIWS 2 user identifier(s) from the external system and returns the associated content, subject to security restrictions.
- Accepts a DIWS 2 identifier(s) for a template and a structure of data from the external system, assembles the content saves the content, and returns a DIWS 2 identifier that can be used to retrieve the content in the future.
- Accepts a DIWS 2 identifier(s), a device (e.g., CD, DVD, thumb drive) and publishing instructions; publishes the content to the device, and returns an indicator of the success of publishing the content.
- Accepts a DIWS 2 identifier(s) and an e-mail address, fax number, or text message destination for the content to be delivered to. After sending the content, DIWS 2 will capture and index e-mail confirmations, e-mail errors, and fax transmittal sheets.
- Monitors incoming fax lines for content, indexes and stores the content based on information contained on the fax, and calls an external procedure to trigger a DIWS 2 or external system workflow for processing the incoming fax.
- Monitors incoming e-mail mailboxes for content, indexes and stores the content based on information contained in the e-mail and attachments, and calls an external procedure to trigger a DIWS 2 or external system workflow for processing the incoming e-mail and attachments.

- Monitors incoming text message mailboxes for content, indexes and stores the content based on information contained in the text message and attachments, and calls an external procedure to trigger a DIWS 2 or external system workflow for processing the incoming text message and attachments.
- Scans content that arrives for bulk scanning; indexes this content based on the document type(s), stores this content in the DIWS 2 repository, and calls an external procedure to trigger a DIWS 2 or external system workflow associated with the document type and index values.
- Provides security for all content that limits access to the content to those with a legitimate business authorization.
- Provides the ability to store content that was captured using desktop/convenience scanning, operational/counter scanning and other capture devices external to DIWS 2.
- Accepts a DIWS 2 user identifier, security information and redaction instructions from an external system. DIWS 2 applies the redaction instructions to the content and returns a DIWS 2 identifier that can be used to retrieve the redacted rendition in the future
- Provides the ability to recognize a transaction identifier and business unit identifier from a barcoded sheet, transmits this information to an external system, and receives from the external system a list of attributes and attribute values associated with the transaction identifier and business unit identifier. DIWS 2 uses these attributes and attribute values to index one or more documents/content arriving with the barcoded sheet.
- Provides the ability to recognize a transaction identifier and business unit identifier from a barcoded sheet. DIWS 2 uses this transaction identifier and business unit identifier to create a temporary document/content type and index one or more documents/content arriving with the barcoded sheet.
- Provides the ability to allow an external system to change a document/content type and associated index values.
- Provide the ability to perform OCR/ICR on images, identify the content type of the image, and extract data from predefined areas of the content type.
- Provides the ability to allow for rapid bulk import of content from other repositories.
- Provides the ability to perform general audits and QA audits on content stored in DIWS 2.

2.1   Use Cases for DIWS 2 Integration with External Systems

Although there are an unlimited number of potential use cases for integration, several use cases are typical and highly probable. Use cases are collections of requirements that bundle discrete integration requirements together. The relationship between use cases and the discrete integration requirements are illustrated in **Table 1 Relationship between**

Integration Use Cases and Discrete Integration Requirements and **Table 2 Relationship between Integration Use Cases and Discrete Integration Requirements**.

Use cases are considered requirements in that they specify how multiple requirements are required to be seamlessly integrated to perform the activity described in the use case. There may be multiple ways in which a use case could be implemented and the notes associated with each use case provide clarification on the expectations. These use cases will likely be included among the many scenarios used for UAT testing of the integration.

The integration use cases can be split into three groups: capture and creation, retrieval and assembly, and management. The capture and creation use cases include:

- (#**C1**) Capture General Content
- (#**C3**) Capture of Solicited Correspondence
- (#**C4**) Capture of Unsolicited Correspondence
- (#**C9**) Create Redacted Documents
- (#**C14**) Create Content via Interchange with an External System
- (#**C15**) Create Temporary Content Type from Barcode Sheet
- (#**C16**) Mobile Capture

The retrieval and assembly use cases include:

- (#**C2**) Retrieve General Content
- (#**C6**) Assemble Documents
- (#**C12**) Transmit Content
- (#**C13**) Search for Content
- (#**C17**) Mobile Search and Retrieval

The management use cases include:

- (#**C5**) Manual Verification of Content
- (#**C7**) Delete Documents
- (#**C8**) Change Retention Period
- (#**C9**) Change Document/Content Type
- (#**C10**) Change Content Type
- (#**C11**) Modify Metadata
- (#**C18**) Data Extraction from Images
- (#**C19**) Rapid Bulk Import
- (#**C20**) General and QA Auditing Status Retrieval
- (#**C21**) General and QA Auditing Status Update

Table 1 Relationship between Integration Use Cases and Discrete Integration Requirements

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C1) Capture General Content	(#C2) Retrieval General Content	(#C3) Capture Solicited Correspondence	(#C4) Capture Unsolicited Correspondence	(#C5) Manual Verification of Content	(#C6) Assemble Documents	(#C7) Delete Documents	(#C8) Change Retention Period	(#C9) Create Redacted Documents
1. Accept content and indexing information…	X								
2. Accept non-resident content description and indexing information…	X								
3. Accept a DIWS 2 identifier …, and return the content and all associated meta data.		X		X		X	X	X	
4. Accept a DIWS 2 identifier … and mark the content for deletion.							X		
5. Allow an external system to establish a persistent session with DIWS…	X	X	X	X	X	X	X	X	X
6. Accept a DIWS 2 user identifier and return the associated content…		X							
7. Accept a DIWS 2 identifier for a template and a data structure, assemble template and data structure, save the assembled content, and return a DIWS identifier…		X				X			
8. Accept a DIWS 2 identifier and an e-mail address, fax number, or text message destination, and deliver the content to the specified destination.									
9. Monitor incoming fax lines for content, index and store the content, and trigger an external workflow…			X	X	X				
10. Monitor incoming e-mail mailboxes for content, index and store the content, and trigger an external workflow …			X	X	X				
11. Monitor incoming text message mailboxes for content, index and store the content, trigger an external workflow …			X	X	X				
12. Monitor incoming FTP and SFTP accounts for content, index and store the content, and trigger an external workflow.			X	X	X				
13. Capture and index e-mail confirmations, e-mail errors, and fax transmittal sheets…			X	X					
14. Designate certain content types and content arriving from specified interfaces as requiring manual verification….			X	X	X				
15. Provide the ability to clear the manual verification status associated with content.					X				
16. Provide the ability to manually add redact renditions for content in DIWS 2 repository.									X
17. Automatically create redacted renditions for content in DIWS repository.									X

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C1) Capture General Content	(#C2) Retrieval General Content	(#C3) Capture Solicited Correspondence	(#C4) Capture Unsolicited Correspondence	(#C5) Manual Verification of Content	(#C6) Assemble Documents	(#C7) Delete Documents	(#C8) Change Retention Period	(#C9) Create Redacted Documents
18. Query the presence of content in DIWS 2 repository.									
19. Retrieve the audit trial for content in DIWS.									
20. Provide the ability to alter the metadata associated with content in DIWS 2.									
21. Provide the ability to alter the retention period for content in DIWS.								X	
22. Provide the ability to assign or alter the security information associated with content in DIWS 2.									
23. Search for one or more pieces of content…		X							
24. Scan content that arrives for bulk scanning; index, store, and trigger an external workflow …	X		X		X				
25. Provide the ability to scan content using a specified scanner.	X		X		X				

Table 2 Relationship between Integration Use Cases and Discrete Integration Requirements

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C10) Modify Content Type	(#C11) Modify Metadata	(#C12) Transmit Content	(#C13) Search for Content	(#C14) Create Content via Interchange with an External System	(#C15) Create Temporary Content Type from Barcode Sheet	(#C16) Mobile Capture	(#C17) Mobile Search and Retrieval	(#C18) Data Extraction from Images	(#C19) Rapid Bulk Import	(#C20) General and QA Auditing Status Retrieval	(#C21) General and QA Auditing Status Update
1. Accept content and indexing information…										X		
2. Accept non-resident content description and indexing information…								X		X		
3. Accept a DIWS 2 identifier …, and return the content and all associated meta data.							X					
4. Accept a DIWS 2 identifier … and mark the content for deletion.												
5. Allow an external system to establish a persistent session with DIWS…	X	X	X	X	X	X	X	X	X	X	X	X
6. Accept a DIWS 2 user identifier and return the associated content…												
7. Accept a DIWS 2 identifier for a template and a data structure, assemble template and data structure, save the assembled content, and return a DIWS identifier…												
8. Accept a DIWS 2 identifier and an e-mail address, fax number, or text message destination, and deliver the content to the specified destination.			X									
9. Monitor incoming fax lines for content, index and store the content, and trigger an external workflow…												
10. Monitor incoming e-mail mailboxes for content, index and store the content, and trigger an external workflow …												
11. Monitor incoming text message mailboxes for content, index and store the content, trigger an external workflow …												

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C10) Modify Content Type	(#C11) Modify Metadata	(#C12) Transmit Content	(#C13) Search for Content	(#C14) Create Content via Interchange with an External System	(#C15) Create Temporary Content Type from Barcode Sheet	(#C16) Mobile Capture	(#C17) Mobile Search and Retrieval	(#C18) Data Extraction from Images	(#C19) Rapid Bulk Import	(#C20) General and QA Auditing Status Retrieval	(#C21) General and QA Auditing Status Update
12. Monitor incoming FTP and SFTP accounts for content, index and store the content, and trigger an external workflow.												
13. Capture and index e-mail confirmations, e-mail errors, and fax transmittal sheets…								X				
14. Designate certain content types and content arriving from specified interfaces as requiring manual verification….												
15. Provide the ability to clear the manual verification status associated with content.												
16. Provide the ability to manually add redact renditions for content in DIWS 2 repository.												
17. Automatically create redacted renditions for content in DIWS repository.												
18. Query the presence of content in DIWS 2 repository.				X								
19. Retrieve the audit trial for content in DIWS.				X								
20. Provide the ability to alter the metadata associated with content in DIWS 2.		X										
21. Provide the ability to alter the retention period for content in DIWS.												
22. Provide the ability to assign or alter the security information associated with content in DIWS 2.		X										
23. Search for one or more pieces of content…		X										

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C10) Modify Content Type	(#C11) Modify Metadata	(#C12) Transmit Content	(#C13) Search for Content	(#C14) Create Content via Interchange with an External System	(#C15) Create Temporary Content Type from Barcode Sheet	(#C16) Mobile Capture	(#C17) Mobile Search and Retrieval	(#C18) Data Extraction from Images	(#C19) Rapid Bulk Import	(#C20) General and QA Auditing Status Retrieval	(#C21) General and QA Auditing Status Update
24. Scan content that arrives for bulk scanning; index, store, and trigger an external workflow …					X	X	X					
25. Provide the ability to scan content using a specified scanner.					X	X	X					
26. Accept DIWS 2 identifiers, a device (e.g., CD, DVD, thumb drive) and publishing instructions; publish the content to the device, …			X									
27. Recognize the presence of barcoded pages and capture transaction identifiers, business unit identifiers and other attribute values from barcoded pages.					X	X						
28. Utilize transaction identifiers, business unit identifiers and other attribute pairs from barcoded sheets to obtain additional index information from an external system.					X							
29. Utilize transaction identifiers, business unit identifiers, other attribute pairs from barcoded sheets, and … to index the content that accompanies a barcoded sheet.					X							
30. Utilize transaction identifiers, business unit identifiers, and other attribute pairs from barcoded sheets … to index the content that accompanies a barcoded sheet using a temporary document/content type.												

Requirements (See section **2.2 DIWS 2 Functionality for External System Integration** for full text)	(#C10) Modify Content Type	(#C11) Modify Metadata	(#C12) Transmit Content	(#C13) Search for Content	(#C14) Create Content via Interchange with an External System	(#C15) Create Temporary Content Type from Barcode Sheet	(#C16) Mobile Capture	(#C17) Mobile Search and Retrieval	(#C18) Data Extraction from Images	(#C19) Rapid Bulk Import	(#C20) General and QA Auditing Status Retrieval	(#C21) General and QA Auditing Status Update
31. Provide the ability to use a mobile device to capture images and other content, index content and asynchronously transmit the content to DIWS 2.							X					
32. Provide the ability to use a mobile device to search DIWS 2 for content, navigate DIWS 2 folders, and asynchronously retrieve DIWS 2 content.								X				
33. Provide the ability to alter the document/content type of a document.	X											
34. Provide the ability to automatically determine the content type for a supplied image or document.									X	X		
35. Provide the ability to extract data from fields in specified areas of an image or document.									X	X		
36. Provide the ability to define a general audit or QA audit, including the expiration date for the audit.												X
37. Provide the ability to change the expiration date for an audit.												X
38. Provide the ability to add or remove documents from a defined general audit or QA audit.												X
39. Provide the ability to retrieve the audit status values for all documents, one document, or multiple documents, associated with a defined audit.											X	
40. Provide the ability to alter the audit status for one or more documents associated with a defined audit.												X

To address the most probable use cases, **DIWS 2 shall demonstrate the following use cases at load levels and performance levels specified in DIWS 2 Appendix 5, Sections 6.2 Capacity and 6.3 Performance**:

C1. Capture General Content – The external system performs the capture of content and sends the content, along with document type(s) and indexing information, to DIWS 2. DIWS 2 stores the content in the repository and returns an indication to the external system that the content was successfully stored in the repository. For documents received electronically for which manual verification is required (see Appendix 5 Toolbox, Section 3.4 Quality Assurance, for an explanation), DIWS 2 shall send an indicator indicating this for each document this applies to.

As described in the note on page 1, the following requirements qualify C1:

a. "Content" shall refer to one or more items of content. For each content item, the content type and the indexing information is provided to DIWS 2.
b. DIWS 2 shall return an indicator for each content item that is sent to DIWS 2 that indicates whether the content was successfully stored.
c. DIWS 2 shall receive an optional flag that indicates whether an error on storing any of the content items in the repository shall result in abandoning the storage of all of the content items from the repository.
d. Audit trail information shall be captured and managed according to the requirements in Appendix 5, Section Audit Trail.
e. DIWS 2 shall indicate whether the manual verification flag was set for each content item and pass this indication to the external system.
f. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
g. This requirement shall be interpreted the requirements in Section 2.2, requirements **1, 2**, and other requirements in section 2.2.

C2. Retrieve General Content – The external system provides DIWS 2 with one or more unique identifiers. Optionally, one or more content formats is/are specified. DIWS 2 performs the retrieval of content and sends the content in the requested formats, along with the associated content type and metadata to the external system. For documents received electronically for which manual verification is required (see Appendix 5 Toolbox, Section 3.4 Quality Assurance, for an explanation), DIWS 2 shall send an indicator indicating this for each document this applies to.

As described in the note on page 1, the following requirements qualify C2:

a. "Content" shall refer to one or more items of content. For each content item being requested, a unique identifier will be provided to DIWS 2.

b. "One or more content formats" shall allow multiple formats to be requested. Examples of formats include, but are not limited to, TIFF, JPEG, PDF, and thumbnail. The absence of a value results in the configurable default format being returned for the content type. The formats may be listed in order of preference and/or a request for multiple formats being returned on one request.

c. DIWS 2 shall return the metadata associated with each content item.

d. DIWS 2 shall return an indicator for each content item that is requested from DIWS that indicates whether the content was successfully retrieved.

e. DIWS 2 shall receive an optional flag that indicates whether an error on retrieving any of the content items in the repository shall result in abandoning the retrieval of all of the content items from the repository.

f. DIWS 2 shall indicate whether the manual verification flag is set for each content item and pass this indication to the external system. The external system is expected to reply to DIWS 2 once the content has been manually verified.

g. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

h. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3**, **23**, and other requirements in section **2.2**.

C3. Capture of Solicited Correspondence – DIWS 2 performs the capture of content that arrives with information that ties the correspondence to a trigger event in DIWS 2 or an external system. After capturing the content, DIWS 2 triggers a workflow in DIWS 2 or an external system and passes the content's unique identifier and other indexing information to the workflow. DIWS 2 also supports returning a configurable message or e-mail based on incoming document type and communications medium to be returned acknowledging receipt of the e-mail.

As described in the note on page 1, the following requirements qualify C3:

a. "Performs the capture" shall include, but is not limited to:
   1 scanning paper documents
   2 retrieving the electronic attachments from e-mail
   3 retrieving the fax stream from an incoming fax
   4 retrieving the incoming data stream from FTP/SFTP
b. "Content that arrives" shall indicate content that has arrived via mail, courier, hand delivery, e-mail, fax, FTP/SFTP, messaging, or other means.
c. "Content" shall refer to one or more items of content. For each content item, the content type is automatically determined by the capture software. Additionally, for certain content types, indexing information shall also be automatically extracted from the content.
d. "Information that ties the correspondence to a trigger event in an external system" shall include cover sheets, bar codes, subject lines in e-mail, subject lines in faxes, the text of a text message, the file name of an FTP/SFTP transmission, and other sources.
e. "Communications medium" shall refer to the mechanism used for sending the information.
   - Examples of communications mediums include: mail, courier, hand delivery, e-mail, fax, FTP/SFTP, messaging, or other means. For e-mail, a configurable e-mail could be returned and for messaging, a configurable message could be returned.
f. DIWS 2 shall use the e-mail system to provide an acknowledgement and/or an acknowledgement e-mail if one was requested by the sender.
   1 DIWS 2 shall send an automated response e-mail message to the sender indicting that the e-mail was received.
   2 "An acknowledgement" shall refer to an MS Outlook delivery receipt or an MS Outlook read receipt.
   3 "An acknowledgement e-mail" shall refer to an e-mail with configurable content.

g. "Trigger event" shall refer to a combination of one or more content types and metadata values.
  - Examples of a trigger event could be a case number or some other recognizable identifier.

h. "Triggers a workflow" shall refer to launching a specific workflow from a set of workflows or continuing a workflow that is waiting for content.
  1 The specific workflow is determined by the content type, content source, and other identifiable information.
  2 A default workflow shall always available for instances where a specific workflow is not found.
  3 An option shall be provided to not trigger a workflow.

i. A configurable number of attempts shall be to initiate the workflow in the external system.
  1 After the configurable number of attempts fails, an error handling workflow in DIWS 2 shall be triggered.

j. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

k. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **9**, **10**, **11**, **12**, **13**, **24**, and other requirements in section **2.2**.

C4. Capture of Unsolicited Correspondence – DIWS 2 performs the capture of content that arrives without information that ties the correspondence to a trigger event in DIWS 2 or an external system. After capturing the content, DIWS 2 triggers a workflow in DIWS 2 or an external system. For a workflow in an external system, DIWS 2 passes the content's document identifier and other indexing information to the external system. Unsolicited correspondence may become solicited correspondence once the content is reviewed and a connection between the content and a trigger event in DIWS 2 or an external system is discovered.

As described in the note on page 1, the following requirements qualify C4:

a. "Unsolicited Correspondence" is correspondence that has not been requested by the MVA (as indicated by the presence of a unique identifier such as a case number or barcode), or is correspondence that returns to the MVA without the unique identifier included.

b. "Performs the capture" shall include, but is not limited to:
1 scanning paper documents
2 retrieving the electronic attachments from e-mail
3 retrieving the fax stream from an incoming fax
4 retrieving the incoming data stream from FTP/SFTP

c. "Content that arrives" shall indicate content that arrived via mail, courier, hand delivery, e-mail, fax, FTP/SFTP, messaging, or other means.

d. "Content" shall refer to one or more items of content. For each content item, the content type shall be automatically determined by the capture software. Additionally, for certain content types, indexing information shall also be automatically extracted from the content.

e. "Trigger event" shall be refer to a combination of one or more content types and metadata values.
▪ Examples of a trigger event could be a case number or some other recognizable identifier.

f. "Triggers a workflow" shall refer to launching a specific workflow from a set of workflows or continuing a workflow that is waiting for content.
1 The specific workflow shall be determined by the content type, content source, and other identifiable information.
2 A default workflow shall always available for instances where a specific workflow is not found.
3 An option shall be provided to not trigger a workflow.

g. A configurable number of attempts shall be made to initiate the workflow in the external system.
1 After the configurable number of attempts fails, an error handling workflow in DIWS 2 shall be triggered.

h. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

i. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **9, 10, 11, 12, 24**, and other requirements in section **2.2**.

C5. Manual Verification of Content – The external system provides DIWS 2 with one or more unique identifiers that indicate that the content associated with these identifiers has been manually verified. DIWS 2 clears the manual verification status associated with the content. The external system may also direct DIWS 2 to remove content from the repository that was determined to be unsatisfactory as a result of manual verification.

As described in the note on page 1, the following requirements qualify C5:

a. "One or more unique identifiers" shall allow the external system to indicate that multiple items have been manually verified as a batch or as individual items.

b. "Content" shall refer to one or more items of content. For each content item that has been manually verified, a unique identifier will be provided to DIWS 2.

c. "Manually verified" is determined by the external application or business unit rules and shall be accepted by DIWS 2.

   ▪ Examples of manual verification could include inspection for readability, correct content type, appropriateness or inappropriateness. Manual verification may be required when certain content types are received electronically from a potential list of external interfaces.

d. "Clears the manual verification status" shall result in a flag or other value being reset or unset.

e. "To remove content from the repository" shall cause DIWS 2 to delete, or mark for deletion, identified content that has been found unsatisfactory during manual verification.

f. DIWS 2 shall return an indicator for each content item that indicates whether the manual verification status associated with content was successfully cleared.

g. DIWS 2 shall receive an optional flag that indicates whether an error on clearing the manual verification indicator for any content shall result in abandoning the retrieval of the remaining manual verification identifiers.

h. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

i. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3, 14, 15**, and other requirements in section **2.2**.

C6. Assemble Documents – The external system provides DIWS 2 with one or more unique identifiers, values, a content type, and indexing information for the document assembly. DIWS 2 shall perform the retrieval of content and shall assemble the content into a composite document that shall be stored in DIWS 2 using the content type and indexing information. DIWS 2 shall return an indicator for each content item confirming the success or reason for failing to include each content item in the assembly.

As described in the note on page 1, the following requirements qualify C6:

a. "Content" shall refer to one or more items of content. For each content item being assembled, a unique identifier will be provided to DIWS 2. Although there may be a practical upper limit on the number of content items that may be included in an assembly, this practical limit shall be on an order of magnitude of tens of thousands of content items.

b. "Values" shall refer to one or more values that are to be assembled into the content (e.g., in hash tags occurring within document headers). The values shall include combinations of constants (e.g., "Contains Personally Identifiable Information") or references to document metadata (e.g., *document name* and *document creation date*).

c. "Content type" shall refer to a content assembly type. Content assembly types shall have instruction files that explain what should be done with the content being assembled.

d. "Indexing information" shall include the set of index values used for storing the content assembly.

e. DIWS 2 shall receive an optional flag that indicates whether an error on any of the content going into the assembly should result in termination of the assembly creation activity.

f. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

g. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3**, and **7**, and other requirements in section **2.2**. Other requirements apply and these are mentioned to emphasize their importance.

C7. Delete Documents – The external system provides DIWS 2 with one or more unique identifiers of content that shall be deleted. DIWS 2 shall check for legitimate reasons why the content shouldn't be deleted, such as those identified in Appendix 5 Section 4.15 Records Management and Legal Hold. If no reasons are found, DIWS 2 shall perform the deletion of content and return an indicator confirming the success or reason for failing to delete each content item.

As described in the note on page 1, the following requirements qualify C7:

a. "Content" shall refer to one or more items of content. For each content item being deleted, a unique identifier shall be provided to DIWS 2.
b. "Legitimate reasons" shall refer to the many reasons why content may not be successfully deleted, including user authorization and legal hold, as further described in requirements throughout the RFP.
c. DIWS 2 shall receive an optional flag that indicates whether an error on deleting any of the content shall cease attempts to delete remaining content.
d. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
e. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3, 4**, and other requirements in section **2.2**.

C8. Change Retention Period – The external system provides DIWS 2 with one or more unique identifiers of content that should have their record retention times changed by a specified number of days. The number of days the retention value is changed is determined by a parameter passed for each unique identifier. DIWS 2 performs the retention extension and returns an indicator confirming the success of extending the extension for each content item.

As described in the note on page 1, the following requirements qualify C8:

a. "Content" shall refer to one or more items of content. For each content item whose retention period is being changed, a unique identifier will be provided to DIWS 2.

b. "Reason for failing" shall perform the checks mandated by Appendix 5 for reasons why the retention period may not be altered, including user authorization and legal hold.

c. "Number of days of the retention is changed is determined by a parameter" shall allow the change to be a negative or positive value.

   1   The negative value shall not result in a date is before the current date.

d. DIWS 2 shall receive an optional flag that indicates whether an error on changing the retention period for any of the content shall cease attempts to change the retention period for the remaining content.

e. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

f. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3, 21**, and other requirements in section **2.2**.

C9. Create Redacted Documents – The external system provides DIWS 2 with one or more unique identifiers of content for which redacted versions of the content shall be created. The external system either passes redacted versions of content or instructs DIWS 2 to create redacted versions of content. The external system also passes to DIWS 2 the type of redacted content that is being created.

As described in the note on page 1, the following requirements qualify C9:

a. "Content" shall refer to one or more items of content.
   1. For each content item being redacted, a unique identifier shall be provided to DIWS 2.
b. "Passes redacted versions of content" shall indicate the external system is passing content that is the same content type as the content type of the unique identifier and all index values that are not related to redaction shall be maintained.
c. "Instructs DIWS 2 to create redacted versions of content" shall mean that DIWS 2 will use a redaction profile to redact key information such as SSNs and date of birth.
   1. The created content shall has the same content type as the content type of the unique identifier and all index values that are not related to redaction shall be maintained.
d. "Type of redacted content" shall allow multiple types of redaction to take place.
   - For example, a strong redaction profile may redact names, dates, SSNs, phone numbers and other potentially sensitive information. A weaker redaction profile may limit redaction to SSNs and values associated with DOB fields.
e. DIWS 2 shall receive an optional flag that indicates whether an error on creating any redactions for any of the content shall cease attempts to create redactions for the remaining content.
f. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
g. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **16, 17**, and other requirements in section **2.2**.

C10. Change Document/Content Type – Provides the ability to allow an external system to change a document/content type and associated index values. The external system provides DIWS 2 with one or more sets of: content identifiers, pairs of content types and associated metadata pairs. DIWS 2 returns the content identifiers, the content type, and associated metadata for all content types that were converted.

As described in the note on page 1, the following requirements qualify C10:

a. "One or more sets" shall refer to the set of information required for changing the content type for a particular item of content.
b. "Content identifier" shall refer to the unique identifier for the content item that shall be changed from one content type to another content type.
c. "Pair of content types" shall be the current content type associated with the content identifier and the target content type that the content shall be changed to.
d. "Metadata pair" shall be the name of an attribute and the associated attribute value.
   1 Attribute values shall include any combination of single and multiple value wildcard characters.
      ▪ Multiple "Metadata pairs are typically used.
e. "Content types that were converted" shall refer to the target content types for which the content type change was successful.
   1 If it is necessary to change the unique content identifier, the old and new unique content identifiers shall be returned.
f. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
g. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **33**, and other requirements in section **2.2**.

C11. Modify Metadata – The external system provides DIWS 2 with one or more unique content identifiers and the metadata pairs for the metadata that should be updated.

As described in the note on page 1, the following requirements qualify C11:

a. "Content" shall refer to multiple items of content.
   1 For each content item whose metadata is being updated, a unique identifier shall be accepted by DIWS 2.
b. "Metadata pairs" indicates the metadata field and metadata value that shall be updated.
   1 The metadata field will shall updated with the metadata value for all content. One or more metadata fields and its associated updated value shall be accepted by DIWS 2.
c. DIWS 2 shall receive an optional flag that indicates whether an error on updating the metadata for any of the content shall cease attempts to update metadata for the remaining content.
d. DIWS 2 shall receive an optional flag that indicates whether an error on updating the metadata for any of the content shall allow all content to remain without updates.
   ▪ In other words, rollback the changes to any metadata that was successfully updated as part of this request.
e. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
f. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **20, 22**, and other requirements in section 2.2.

C12. Transmit Content – The external system provides DIWS 2 with one or more unique identifiers of content and one or more electronic destinations that the content should be sent to. DIWS 2 performs the transmission of the content to the specified destinations and returns an indicator confirming the success or reason for failing to delete each content item.

As described in the note on page 1, the following requirements qualify C12:

a. "Content" shall refer to one or more items of content.
   1 For each content item being requested, a unique identifier shall be accepted by DIWS 2.
b. "Electronic destinations" shall refer to any combination of one or more e-mail addresses, fax numbers, FTP/SFTP, message addresses, CDs, DVDs, and thumb drives, including the appropriate parameters (e.g., number of retries for a fax) for the electronic destinations.
c. DIWS 2 shall return an indicator for each content item that is requested to be sent from DIWS 2 that indicates whether the content was successfully transmitted.
d. DIWS 2 shall determine when content shall be sent in multiple transmissions due to limitations of the electronic destination (e.g., page limits for faxes, size limits for e-mail, attachment limits for messages).
e. DIWS 2 shall receive an optional flag that indicates whether an error on retrieving any of the content items in the repository shall result in abandoning the retrieval of all of the content items from the repository.
f. DIWS 2 shall receive an optional flag that indicates whether an error on transmitting any of the content items to an electronic destination shall result in abandoning the transmission of all of the content items to the remaining electronic destinations.
g. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
h. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **5**, **8**, **43**, and other requirements in section **2.2**.

C13. Search for Content – The external system provides DIWS 2 with one or more content types, associated metadata pairs, and an audit trail indicator for content that should be searched for. Additionally, the manner in which the results should be returned is provided. DIWS 2 returns the content identifiers, associated metadata for all content matching the criteria, the number of results satisfying the search criteria and the number of results being returned.

As described in the note on page 1, the following requirements qualify C13:

a. "Content type" shall refer to one or more content types.
b. "Metadata pairs" shall be the name of an attribute and the associated attribute value.
   1. Attribute values shall be able to include any combination of single and multiple value wildcard characters.
c. "Audit trail indicator" specifies whether the search shall exclude audit trail records, be limited to audit trail records or include audit trail records.
d. "Manner in which the results should be returned" shall provide the ability to:
   1. Limit the number of fields returned.
   2. Limit the number of search results.
   3. Indicate the subset of the search results that should be returned.
   4. Specify how the information is delivered to the external system.
e. "Returns" shall be limited to returning the number of search results associated with a supplied value, the user, or the role.
f. "Number of results being returned" shall be less than or equal to the number of results satisfying the search criteria.
   - For example, 400,000 items may satisfy the search results, but only 20 are being returned.
g. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
h. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **20, 22**, and other requirements in section **2.2**.

C14. Create Content via Interchange with an External System – DIWS 2 performs the capture of content, recognizes a transaction identifier, business unit identifier, and other attributes from a barcoded sheet, transmits this information to an external system, and receives from the external system a list of attributes and attribute values associated with the transaction identifier and business unit identifier. DIWS 2 uses these attributes and attribute values to index one or more documents/content arriving with the barcoded sheet. After indexing and storing the content, DIWS 2 triggers a workflow in DIWS 2 or an external system and passes the content's unique identifier(s) and other indexing information to the workflow. DIWS 2 also supports returning a configurable message or e-mail based on incoming document type and communications medium to be returned acknowledging receipt of the content.

As described in the note on page 1, the following requirements qualify C14:

a. "Barcoded sheet" shall refer to a sheet containing information recognized by an external system and, when available, shall be used to link incoming content with existing cases, transactions, and workflows.

b. "Transaction identifier, business unit identifier, and other attributes" refer to information that shall be used in linking arriving information with existing cases, transactions, and workflows.

c. There shall be a real-time exchange of information with the external system.

1 The information on the barcoded sheet shall be sent to the external system.

2 The external system in turn sends additional attribute information to DIWS 2.

d. DIWS 2 shall utilize the attributes from the barcoded sheet and the additional attribute information to index the content that accompanied the barcoded sheet.

e. Audit trail information shall be captured and managed for content arriving via e-mail and messages just as it is captured and managed for images scanned by DIWS 2.

f. "Triggers a workflow" shall launch a specific workflow from a set of workflows or continuing a workflow that is waiting for content.
    1 The specific workflow shall be determined by the content type, content source, and other identifiable information.
    2 A default workflow shall always available for instances where a specific workflow is not found.
    3 An option shall be provided to not trigger a workflow.

g. A configurable number of attempts shall be made to initiate the workflow in the external system.
    1 After the configurable number of attempts fails, an error handling workflow in DIWS 2 shall be triggered.

h. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

i. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **5, 24, 25, 27, 28, 29**, and other requirements in section **2.2**.

C15. Create Temporary Content Type from Barcode Sheet – Provides the ability to recognize a transaction identifier and business unit identifier from a barcoded sheet. DIWS 2 uses this transaction identifier and business unit identifier to create a temporary document/content type and index one or more documents/content arriving with the barcoded sheet. After indexing and storing the content, DIWS 2 triggers a workflow in DIWS 2 or an external system and passes the content's unique identifier(s) and other indexing information to the workflow.

As described in the note on page 1, the following requirements qualify C15:

a. "Barcoded sheet" shall refer to a sheet containing information recognized by an external system and, when available, shall be used to associate incoming content with existing cases, transactions, and workflows.

b. "Transaction identifier, business unit identifier, and other attributes" shall refer to information that is useful in associating arriving information with existing cases, transactions, and workflows.

c. "A temporary document/content type" is a document type or content type that shall exist until it is changed (see Section 2.1 Use Cases for DIWS 2 Integration with External Systems, item C10.) The barcoded information is used to look up one or more potential content/document types permitted for the transaction identifier. The content/document type is temporary to the extent that the automatic content/document type selection may have been incorrect and may need to be changed. It is anticipated that most times there is sufficient information available to correctly assign the document/content type, especially in the case of solicited correspondence with only one document.

d. There shall be a real-time exchange of information with the external system.

    1 The information on the barcoded sheet shall be sent to the external system.

    2 The external system in turn sends additional attribute information to DIWS 2.

e. DIWS 2 shall utilize the attributes from the barcoded sheet and the additional attribute information to index the content that accompanied the barcoded sheet.

f. Audit trail information shall be captured and managed for content arriving via e-mail and messages just as it is captured and managed for images scanned by DIWS 2.

g. "Triggers a workflow" shall launch a specific workflow from a set of workflows or continuing a workflow that is waiting for content.

    1 The specific workflow shall be determined by the content type, content source, and other identifiable information.

    2 A default workflow shall always available for instances where a specific workflow is not found.

    3 An option shall be provided to not trigger a workflow.

h. A configurable number of attempts shall be made to initiate the workflow in the external system.

    1 After the configurable number of attempts fails, an error handling workflow in DIWS 2 shall be triggered.

i. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

j. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **5, 24, 25, 27, 30**, and other requirements in section **2.2**.

C16. Mobile Capture – DIWS 2 performs the capture of images and documents using a smartphone, tablet, or other mobile device. The device user is able to index the documents and images. Once indexed, the images are automatically an asynchronously transmitted to DIWS 2 with retries automatic performed. Once the content arrives is DIWS 2, DIWS 2 triggers a workflow in DIWS 2 or an external system and passes the content's unique identifier and other indexing information to the workflow. DIWS 2 also supports returning a configurable message or e-mail based on incoming document type and communications medium.

As described in the note on page 1, the following requirements qualify C16:

a. DIWS 2 shall support mobile workers that may be working remotely for days or weeks. DIWS 2 shall be able to immediately, subject to connectivity, transmit content back to the DIWS 2 repository so that the content is available for normal business activity. In this context, connectivity is typically provided through a cellphone (e.g., Verizon), but could be provided by a local network connection.

b. "Asynchronously transmitted" shall allow additional content to be captured without waiting for prior transmissions to be completed. The transmissions shall take a lower priority than the capture activity.

c. DIWS 2 shall be configurable to send an automated message to the users indicating the arrival of content.

d. "Triggers a workflow" shall launch a specific workflow from a set of workflows or continuing a workflow that is waiting for content.

  1 The specific workflow shall be determined by the content type, content source, and other identifiable information.

  2 A default workflow shall always available for instances where a specific workflow is not found.

  3 An option shall be provided to not trigger a workflow.

e. A configurable number of attempts shall be made to initiate the workflow in the external system. After the configurable number of attempts fails, an error handling workflow in DIWS 2 shall be triggered.

f. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

g. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **3, 24, 25, 31**, and other requirements in section **2.2**.

▪ There are MVA staff that travel outside of the MVA office for days or weeks at a time. These trips (e.g., from a visit to a driver training school) result in collection of images, documents, forms and other materials. The collected material is expected to be transferred back to DIWS 2 for access and processing by MVA staff. The MVA staff that is traveling often have smart devices with cellphone connectivity for data. When the staff has connectivity via the smart device, the collected information should be automatically uploaded to DIWS 2. There is an expectation that the connectivity will be automatic because it might occur when the staff is travelling between sites at a time the staff does not have the ability to check for connectivity. When the staff is in an area without cellphone data connectivity, the smartphone should continue attempting to connect until the connectivity is re-established.

C17. Mobile Search and Retrieval – DIWS 2 provides the ability to search for content in DIWS 2 using a smartphone, tablet, or other mobile device. DIWS 2 also provides the mobile device user with the ability to retrieve content based on search results or by navigation. The retrieval requests are processed asynchronously. The search results are cached locally on the mobile device for a configurable number of days. Based on configuration parameters, the user is notified by a text message when the content has been retrieved. Attempts are made to retrieve content after communication errors are encountered.

As described in the note on page 1, the following requirements qualify C17:

  a. DIWS 2 shall also return the metadata associated with each content item.
  b. DIWS 2 shall return an indicator for each content item that is requested from DIWS that indicates whether the content was successfully retrieved.
  c. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
  d. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **2**, **13**, **32**, and other requirements in section **2.2**.

- Here is a scenario. The MVA mobile worker is traveling to an area of the State where connectivity is intermittent. At some point the search request is submitted, but due to limited connectivity, the results do not appear on the worker's smart device for several hours. Once the results are available, the worker then requests several documents from the search results which may not be processed immediately because the worker continues to be travelling in a region of intermittent connectivity. Eventually the documents appear on the workers smart device and are available for use by the worker. The worker may also request other documents from the previous search results which were cached locally.

C18. Data Extraction from Images – The external system sends the content, along with optional content type information, to DIWS 2. If the content type is not supplied, DIWS 2 attempts to determine the content type. For recognized document types and content that is supplied with a content type, DIWS 2 performs OCR/ICR on the image and extracts data from the areas defined for the content type. The extracted fields and field values are returned to the external system. For content types that are unknown or unrecognized, DIWS 2 performs OCR/ICR on the content and returns the resulting text data. DIWS 2 does not index or store the supplied content.

As described in the note on page 1, the following requirements qualify C18:

- a. "Content" shall refer to one or more items of content.
- b. "Content type" shall optionally be provided for some or all of the content. Content types shall be verified to be predefined values recognized by DIWS 2.
- c. The approach to "determine the content type" is not prescribed, but shall be based on using heuristics derived from being presented with some number of samples representative of the content type.
- d. "Areas defined for the content type" shall refer to fields containing values within the content.
  - Examples include, name, address, identifiers, and other values that typically occur on the image of a specified content type.
- e. "Returned to the external system" shall refer to returning the extracted field names and field values for all fields defined for the content type.
  - Some fields may contain null values.
- f. "Text data" shall refer the OCR/IC text data for a content type that is undefined, was not recognized, or did not fit the profile associated with the content type.
  - 1 This data shall be returned in a data structure appropriate to the task.
- g. DIWS 2 shall receive an optional indicator from the external system instructing DIWS 2 as to whether an error on extracting data from any of the content items shall result in abandoning the further extraction of data from the remaining content items.

h. DIWS 2 shall return a content type for each content item that is supplied. For unrecognized or undefined content types, an appropriate value shall be returned.

i. DIWS 2 shall return an indicator for each content item that is supplied that indicates whether the content was successfully processed.

j. Audit trail information shall be captured and managed just as it is captured and managed for images scanned by DIWS 2.

k. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

l. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **1, 2**, **34, 35**, and other requirements in section **2.2**.

C19. Rapid Bulk Import – The external system sends the content, along with optional content type information, to DIWS 2. If the content type is not supplied, DIWS 2 attempts to determine the content type. For recognized document types and content that is supplied with a content type, DIWS 2 performs OCR/ICR on the image and extracts data from the areas defined for the content type. The extracted fields and field values are returned to the external system. For content types that are unknown or unrecognized, DIWS 2 performs OCR/ICR on the content and returns the resulting text data.

As described in the note on page 1, the following requirements qualify C19:

a. "Content" shall refer to one or more items of content.
b. "Content type" shall optionally be provided for some or all of the content. Content types shall be verified to be predefined values recognized by DIWS 2.
c. The approach to "determine the content type" is not prescribed, but shall be based on using heuristics derived from being presented with some number of samples representative of the content type.
d. "Areas defined for the content type" shall refer to fields containing values within the content.
   ▪ Examples include, name, address, identifiers, and other values that typically occur on the image of a specified content type.
e. "Returned to the external system" shall refer to returning the extracted field names and field values for all fields defined for the content type.
   ▪ Some fields may contain null values.
f. "Text data" shall refer the OCR/IC text data for a content type that is undefined, was not recognized, or did not fit the profile associated with the content type.
   1 This data shall be returned in a data structure appropriate to the task.
g. DIWS 2 shall optionally receive an indicator from the external system instructing DIWS 2 as to whether an error on extracting data from any of the content items shall result in abandoning the further extraction of data from the remaining content items.
h. DIWS 2 shall return a content type for each content item that is supplied. For unrecognized or undefined content types, an appropriate value shall be returned.
i. DIWS 2 shall return an indicator for each content item that is supplied that indicates whether the content was successfully processed.
j. Audit trail information shall be captured and managed just as it is captured and managed for images scanned by DIWS 2.
k. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.

l. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **34, 35**, and other requirements in section **2.2**.

C20. General and QA Auditing Status Retrieval – The external system provides DIWS 2 with one or more defined audits, and optionally one or more unique content identifiers, for retrieving the general auditing status values or QA auditing status values.

As described in the note on page 1, the following requirements qualify C20:

a. "Content" shall refer to one or more items of content.
   1 If a content identifier is not passed for a defined audit, all status values for that defined audit shall be returned.
   2 If one or more a content identifiers are is passed for a defined audit, the status values for the documents associated with that defined audit shall be returned.
b. "Defined audits" indicates the general audit or QA audit defined in DIWS 2 as specified in Appendix 5 Toolbox, Section 4.14 General Auditing and QA Auditing.
   1 One or more audits shall be accepted and the audit status values for these audits shall be returned.
c. DIWS 2 shall receive an optional flag that indicates whether an error on retrieving auditing status values for any of the content shall cease attempts to retrieve auditing status values for the remaining content or defined audits.
d. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
e. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **36**, **37**, **38**, **39**, **40**, and other requirements in section **2.2**.

C21. General and QA Auditing Status Update – The external system provides DIWS 2 with one or more pairs of defined audits and operations, one or more pairs of unique content identifiers and an auditing status values, optional users and optional expiration dates, that are to be updated.

As described in the note on page 1, the following requirements qualify C21:

a. "Defined audits" shall indicate, as specified in Appendix 5 Toolbox, Section 4.14 General Auditing and QA Auditing, either:
  1 a unique name for a general audit or QA audit that is to be defined
  2 the general audit or QA audit previously defined in DIWS 2
b. "Operations" shall include the following values:
  1 Creating an audit
  2 Updating users in an audit
  3 Updating expiration date for an audit
  4 Updating audit status values for defined audit.
c. "Content" shall refer to one or more items of content.
d. "Auditing status value" shall be the status value associated with the Content identifier.
e. "Optional users" shall be the user identifiers to be added or removed when the Operation is "creating an audit" or " updating users in an audit"
f. "Optional expiration dates" shall be the expiration date(s) to be added or updated when the Operation is "creating an audit" or " updating expiration date" for an audit"
g. DIWS 2 shall receive an optional flag that indicates whether an error an operation shall cease attempts to execute further operations as part of this use case.
h. The operations described in this case shall be performed on behalf of an authenticated external system with the appropriate permissions and subject to the security limitations associated with the user or user group this action is being performed for.
i. This requirement shall be interpreted according to the requirements in Section 2.2, requirements **36**, **37**, **38**, **39**, **40**, and other requirements in section **2.2**.

NOTE: The cases for the interfaces and information exchanged across the interfaces may change during the requirements verification activities and design activities. Additional cases, interfaces and information exchange may be added as a result of the requirements verification activities and design activities.

The Contractor's scope of responsibility under the fixed price Offer shall include all necessary requirements decomposition and refinement of the cases named in Section 2.1 Use Cases for DIWS 2 Integration with External Systems. Additional requirements and details that are not related to the cases interfaces named in Section 2.1 Use Cases for DIWS 2 Integration with External Systems may be incorporated via change order or work order in the future.

2.2   DIWS 2 Functionality for External System Integration

These requirements are expected to be built on similar requirements described in the DIWS 2 toolbox described in Appendix 5. These requirements typically take one or more of the toolbox requirements, and extends and packages their functionality.

To support integration with the external systems, **DIWS 2 shall**:

1. Accept content and indexing information arriving via the external system interface, save the content in the DIWS 2 repository, and return a DIWS 2 identifier that can be used to retrieve the content in the future.

   ▪ For the purpose of this requirement, the indexing information received via the external system interface may include a unique key that could be used to retrieve the content in the future. In cases where the unique key is provided by the system using the external system interface, DIWS 2 will accept a parameter that allows suppression of the DIWS 2 identifier being returned.

2. Accept non-resident content description and indexing information arriving via the external system interface, save the location of content in the DIWS 2 repository, and return a DIWS 2 identifier that can be used to retrieve the non-resident content description in the future.

   a. In cases where the unique key is provided by the external system using the DIWS 2 external system interface, DIWS 2 shall accept a parameter that allows suppression of the DIWS 2 identifier being returned.
   - The indexing information received via the external system interface may include a unique key that could be used to retrieve the content in the future.
   - Non-resident content is content that is managed by DIWS 2, but is not physically stored in the DIWS 2 repository. Examples of this content include sensitive content, fragile content, valuable content, and other content that is stored (often in a non-electronic format) external to DIWS 2. For non-resident content, DIWS 2 typically stores the location of the content and information on where to go and who to contact to request access. Non-resident content could have renditions stored in DIWS 2, but these renditions are often not considered to be the copy of record.

3. Accept a DIWS 2 identifier that was previously provided by DIWS 2 when content was saved, and return the content and all associated meta data.

   - For the purpose of this requirement, if a unique identifier was provided by the external system that passed the information to DIWS 2, this will be indicated by a parameter that will be used by DIWS 2 to retrieve the content.

4. Accept a DIWS 2 identifier that was previously provided by DIWS 2 when content was saved, and mark the content for deletion.

   a. For the purpose of this requirement, if a unique identifier was provided by the external system that passed the information to DIWS 2, this will be indicated by a parameter that shall be used by DIWS 2 to delete the content.
   b. Deletion shall be subject to all constraints being satisfied such as: the user belongs to a role that has authority to delete the specified content, that the content is not subject to legal hold, and the applicable retention policies permit the deletion.

5. Allow an external system to establish one or more persistent sessions with DIWS 2 for the purpose of executing all of the capabilities provided by the DIWS 2 external system interface.

   a. The Contractor shall provide guidance to allow External Systems to manage a pool of persistent connections between DIWS 2 and the External System(s).

   b. The number of persistent sessions that are allowed to be opened concurrently by each External System shall be configurable for each External System. (e.g., ES1 is allowed 1 persistent session, ES2 is allowed 10 persistent sessions, ES3 is allowed 4 persistent sessions.)

   c. DIWS 2 shall be designed such that no passwords are compiled into the source materials, hardcoded, or stored in an unencrypted format.

   d. DIWS 2 shall incorporate security policies that shall require external system interface passwords to be changed on a configurable period.

   e. DIWS 2 shall provide an automated mechanism for updating the external systems interface passwords throughout the system whenever they are changed.

   f. A persistent session shall be a session that persists over a configurable period of time, measured in hours, days, weeks or months, which does not require credentials to be supplied at any time other than when the session is first established.

   g. A persistent session shall terminate after a configurable period of inactivity, measured in minutes or hours.

   h. The initial configuration value for the persistence of the session shall be one day.

   i. The persistence of the session shall end when the external system requests that it be ended, connectivity is broken, a period of inactivity has occurred, or an administrator issues a command to disable the interface.

   j. The establishment and termination of persistent sessions shall be logged.

   k. All transactions performed using persistent sessions shall be logged.

6. Accept a DIWS 2 user identifier and other information arriving via the DIWS 2 external system interface and return the associated content, subject to security restrictions for that user identifier.

   For the purpose of this requirement:

   a. A DIWS 2 user identifier, when passed along with a command or operation, shall be used to limit access to content based on the credentials of the user associated with the user identifier.

   b. This limiting behavior shall exist until the command or operation has completed, the command or operation has resulted in an error, or the session has terminated.

7.   Accept a DIWS 2 identifier for a template and a data structure arriving via the DIWS 2 external system interface, assemble template and data structure, save the assembled content, and return a DIWS 2 identifier that can be used to retrieve the content in future.

   ▪   For the purpose of this requirement, assembling the content allows for data to be merged into a document or template. An example of this requirement would be including the name, address and date into the addressee section of the template.

8.   Accept a DIWS 2 identifier and an e-mail address, fax number, or text message destination, and deliver the content to the specified destination.

   As described in the note on page 1, the following requirements qualify Requirement 8:

   a.   DIWS 2 shall e-mail the content to the specified e-mail address and include a subject line that was passed along with the e-mail address or create a subject line using the content's metadata.
   b.   DISW 2 shall fax the content to the specified fax number and include a cover page using information that was passed along with the fax number or create a cover page using the content's metadata.
   c.   DIWS 2 shall send a text message with the content to the smart device at the specified number and include a message that was passed along with the number or create a text message using the content's metadata.

9.   Monitor incoming fax lines for content, index and store the content based on information contained on the fax, and call an external procedure to trigger a DIWS 2 external system workflow for processing the incoming fax.

10.   Monitor incoming e-mail mailboxes for content, index and store the content based on information contained in the e-mail and attachments, and call an external procedure to trigger a DIWS 2 External System workflow for processing the incoming e-mail and attachments.

11.   Monitor incoming text message mailboxes for content, index and store the content based on information contained in the text message and attachments, and call an external procedure to trigger a DIWS 2 External System workflow for processing the incoming text message and attachments.

   ▪   For the purpose of this requirement, there may be technical limitations that may limit certain capabilities. For example, attachments are not supported by basic text messaging (SMS), but they are supported by MMS.

12. Monitor incoming FTP and SFTP accounts for content, index and store the content based on information contained in the file names or control file, and call an external procedure to trigger a DIWS 2 External System workflow for processing the incoming text message and attachments.

    ▪ For the purpose of this requirement, a "control file" is a file with a specific name that contains information about other files that were transmitted. For example, a control file might contain the names of three files and information that could be used to index each of those files.

13. Capture and index e-mail confirmations, e-mail errors, and fax transmittal sheets associated with all attempts to send e-mails, faxes, and text messages.

14. Provide the ability to designate certain content types and content arriving from specified interfaces as requiring manual verification and have the manual verification status set for those content types.

    For the purpose of this requirement:
    a. "Certain content types and content arriving from specified interfaces" shall mean that this requirement applies to content types and also applies to content arriving from specified interfaces.
    b. "Certain content types" shall mean a list of content types (or content subtypes, or content sub-subtypes) that are specified in a configurable list.
    c. "Content arriving from specified interfaces" shall mean that this requirement applies to named interfaces that are specified in a configurable list. For example, a named interface might be a specific fax machine, all fax machines, a specific e-mail account, a specific FTP account, or other interface.

15. Provide the ability to clear the manual verification status associated with content.

16. Provide the ability to manually add redact renditions for content in DIWS 2 repository.

17. Provide the ability to automatically create redacted renditions for content in DIWS 2 repository.

18. Provide the ability to query the presence of content in DIWS 2 repository.

19. Provide the ability to retrieve the audit trial for content in DIWS 2.

20. Provide the ability to alter the metadata associated with content in DIWS 2.

21. Provide the ability to alter the retention period for content in DIWS 2.

22. Provide the ability to assign or alter the security information associated with content in DIWS 2.

23. Provide the ability to search for one or more pieces of content in DIWS 2 using metadata values containing full, partial or wild card values.

24. Scan content that arrives for bulk scanning; indexes this content based on the document type, stores this content in the DIWS 2 repository, and calls an external procedure to trigger an external workflow associated with the document type and index values.

    For the purpose of this requirement:

    - "Content that arrives for bulk scanning" is typically content that arrives in paper form by mail or courier.
    - "An external workflow" would include a DIWS 2 External System workflow and would be triggered using the DIWS 2 External System interface that exists for the purpose of triggering such a workflow.

25. Provide the ability to scan content using a specified scanner.

    These too are requirements:

    a. The identifier of the specified scanner shall be accepted at the time this capability is invoked.
    b. The invoking system shall have the option of utilizing any features (e.g., color, double-sided), through DIWS 2, of the scanner.
    c. The scanning subsystem shall accept instructions from the invoking system to return a file containing the scanned image.
    d. The scanning subsystem shall accept instructions from the invoking system to store the scanned image in the repository. The scanning subsystem shall also accept instructions from the invoking system to automatically determine the document type.
    e. The scanning subsystem shall accept instruction by the invoking system that field values be automatically detected and extracted from the scanned image.

26. Accept one or more DIWS 2 identifiers, a device (e.g., CD, DVD, thumb drive) and publishing instructions; publish the content to the device, and returns an indicator of the success of publishing the content.

    As described in the note on page 1, the following requirements qualify Requirement 26:

    a. "Publishing instructions" shall include, but are not limited to:
        1 restrictions such as a limit on the number of files permitted on a device,
        2 a limit on the size of files permitted on a device,
        3 splitting content so that it spans multiple devices,
        4 volume labels, and
        5 other instructions and information relevant to publishing.
    - An example is writing 1GB of content onto CDs. The system needs to detect that 1GB exceeds the capacity of a CD and would split the content on two CDs.

27. Recognize the presence of barcoded page/sheet and capture transaction identifiers, business unit identifiers and other attribute values from barcoded pages.

    ▪ Barcoded sheets are defined in Appendix 5, section 3.1 Scanning. They arrive with a batch of related content and contain barcoded information (e.g., transaction identifiers, business unit identifiers, and attribute values) relevant to that content.

    ▪ The barcoded sheets may arrive as paper, by e-mail, by fax, or as attachments to messages.

28. Utilize transaction identifiers, business unit identifiers and other attribute pairs from barcoded sheets to obtain additional index information from an external system.

    ▪ Barcoded sheets are defined in Appendix 5 Toolbox Sections **3.2 Capture and** 3.5 **Indexing**. They arrive with a batch of related content and contain barcoded information (e.g., transaction identifiers, business unit identifiers, and attribute values) relevant to that content.

    ▪ The additional index information may contain document/content types and attribute pairings. It may also contain no additional index information if the barcoded information was sufficient for indexing the content.

29. Utilize transaction identifiers, business unit identifiers and other attribute pairs from barcoded sheets, along with additional index information from an external system to index content that arrived with the barcoded sheets.

30. Utilize transaction identifiers, business unit identifiers and other attribute pairs from barcoded sheets to index content that arrived with the barcoded sheets as a temporary content type.

    ▪ The intent is to use the minimal information that is present on the barcoded sheets as the index values.

    ▪ A temporary document/content type is used that aligns with the available index information. There will be multiple temporary document/content types available and the correct one will need to be determined based on the available attributes.

31. Provide the ability to use a mobile device to capture images and other content, index content and asynchronously transmit the content to DIWS 2.

   a. Search and navigation shall take priority over content retrieval.
   b. Transmission shall be performed asynchronously relative to capture allowing additional content to be captured before pending content transmissions have been completed.
   c. Content transmission shall take place automatically and continuously in the background. For example, the actual transmission of content may take place while driving between locations.
   d. Due to the unpredictable nature of communications in some parts of the State, transmission shall be continuously retried until successfully completed.

32. Provide the ability to use a mobile device to search DIWS 2 for content, navigate DIWS 2 folders, and asynchronously retrieve DIWS 2 content.

   a. Search and navigation shall take priority over content retrieval.
   b. Retrievals shall be performed asynchronously relative to navigation and searches allowing additional retrieval requests to be made before pending requests have been completed.
   c. Content retrieval shall take place automatically and continuously in the background. For example, the actual retrieval of content may take place while driving between locations.
   d. Due to the unpredictable nature of communications in some parts of the State, communications shall be continuously retried until successfully completed.
   e. The user shall be able to request a notification at the time the retrieval request is made that informs the user when the content has been received.

33. Provide the ability to alter the document/content type of a document.

   ▪ For example, change a temporary document type to a different document type.

34. Provide the ability to automatically determine the content type for a supplied image or document.

   ▪ See Appendix 5, section 3.2 Capture, for additional requirements related to automatically recognizing content types.

35. Provide the ability to extract data from fields in specified areas of an image or document.

   ▪ See Appendix 5, section 3.5 Indexing, for additional requirements related to extracting information.

36. Provide the ability to define a general audit or QA audit, including the expiration date for the audit.

    ▪ See Appendix 5, section 4.14 General Auditing and QA Auditing, for additional requirements related to auditing.

37. Provide the ability to change the expiration date for an audit.

    ▪ See Appendix 5, section 4.14 General Auditing and QA Auditing, for additional requirements related to auditing.

38. Provide the ability to add or remove documents from a defined general audit or QA audit.

    ▪ See Appendix 5, section 4.14 General Auditing and QA Auditing, for additional requirements related to auditing.

39. Provide the ability to retrieve the audit status values for all documents, one document, or multiple documents, associated with a defined audit.

    ▪ See Appendix 5, section 4.14 General Auditing and QA Auditing, for additional requirements related to auditing.

40. Provide the ability to alter the audit status for one or more documents associated with a defined audit.

    ▪ See Appendix 5, section 4.14 General Auditing and QA Auditing, for additional requirements related to auditing.

NOTE: The requirements for the interfaces and information exchanged across the interfaces may change during the requirements verification activities and design activities. Additional interfaces and information exchange may be added as a result of the requirements verification activities and design activities.

The Contractor's scope of responsibility under the fixed price Offer shall include all necessary requirements decomposition and refinement of the requirements named in Section 2.2 DIWS 2 Functionality for External System Integration. Additional requirements and details that are not related to the interfaces named in Section 2.2 DIWS 2 Functionality for External System Integration may be incorporated via change order or work order in the future.

2.3 Additional Integration Requirements

Due to the nature of the integration, it is anticipated the Contractor will have a collaborative role in further developing and defining the use cases and identifying requirements that are typical of a system such as DIWS.

The following requirements discuss activities that will be performed by the Contractor in designing, developing and delivering the DIWS 2 external systems interface. **The Contractor shall:**

1. Publish an external system ICD that defines and describes, but is not limited to, the APIs, Web services and Enterprise Service Bus to provide the use cases specified in section **2.1**, **Use Cases** for DIWS 2 Integration with External Systems and the functionality specified in section **2.2, DIWS 2 Functionality for External System** Integration.

    ▪ For the purpose of this requirement, the specific nature of the interface as an API, Web service and/or Enterprise Service Bus, shall be determined during the DIWS 2 requirements gathering and design activities.

2. Maintain version history for the external system interface such that:

    a. Each external system communicating with DIWS 2 using the external system integration interfaces shall have the option of communicating the version of the interface that it is using to communicate.
    b. DIWS 2 shall be backward compatible with all versions of the external system integration interfaces.
    c. DIWS 2 shall communicate with external systems using the current version of the external systems integration interfaces, unless the external systems provided an external system integration interface version that is earlier than the current version.
    d. DIWS 2 shall communicate with external systems using the version of the external systems integration interfaces supplied by the external system, if and only if the external system communicated an external system integration interface version.
    e. Maintain an external system ICD for each version of the external system integration interface.

3. Where appropriate, propose XML standards that apply to information being exchanged.

    ▪ For the purpose of this requirement, XML standards are preferred, but the MVA reserves the right to accept, reject, or modify any proposed standards.

4. Work with MVA to definitize and finalize the requirements for the DIWS 2 ICD for the DIWS 2 external system interface.

   a. The Contractor shall work with the Project Core Vendor to identify, understand and incorporate any external system integration capabilities that the Project Core System may require.

   b. When working with the Project Core Vendor, the requirements stated in Appendix 10 shall be provided regardless of whether the requirements are needed by the Project Core System.

      ▪ Recall that this is a general purpose interface to be used by the Project Core System _and_ all systems that the MVA will deploy in the future. The Project Core System is the first, but not the only user for this interface.

5. Review the DIWS 2 ICD with MVA.

6. Receive approval from MVA Project Manager for each version of the DIWS 2 ICD.

7. Include a library of APIs, Web services, or Enterprise Service Bus components for the interface described in the DIWS 2 ICD.

8. Include support and maintenance of the external system integration interface for all environments defined in the DIWS 2 ICD.

   ▪ For the purpose of this requirement: environments are development, test, training, production, and those identified in Appendix 3 - System Supported, section 2.2 O&M Timeline.

9. Ensure the DIWS 2 External System interface shall be fully operational in all environments.

   a. The interface in one DIWS 2 environment (e.g., test) shall be able to be integrated with the DIWS 2 External System (e.g., Project Core System) in one or more other environments (e.g., test and training).

10.   During system development (i.e., prior to full system delivery), Include a minimum of six (6) periodic updates to the ICD and library of APIs, Web services, and Enterprise Service Bus components at a frequency to be determined by the MVA Project Manager and with the first periodic delivery occurring of not more than 90 after days the interface was initially delivered.

   a.   For the purpose of this requirement, updates shall be delivered to address requirement defects, missing functionality and capability, address documentation enhancements, and remediate performance problems.
   b.   The first periodic update shall be delivered in approximately 90 days.
   c.   The second, and subsequent updates, shall be delivered at dates determined by the MVA Project Manager.
   d.   Changes to the ICD and library of APIs, Web services, and Enterprise Service Bus components shall be provided a version in accordance with Section 2.3 Additional Integration Requirements, Requirement 2.

2.4   Process

To deliver the process capabilities required for the DIWS 2 External System integration, **the DIWS 2 Contractor shall**:

1.   Identify a process for working with the team responsible for utilizing the DIWS 2 External System interfaces.

2.   Identify measurements for ensuring the process is repeatable, achieves goals, and produces meaningful results.

3.   Execute the process for the first project that utilizes the DIWS 2 External System Interface.

   ▪   At this time, the first project is anticipated to be Project Core.

4.   Support Project Core during their testing of the DIWS 2 External System Interface.

5.   Demonstrate successful use of the DIWS 2 External System interface to meet functional and performance goals.

2.5   Document Types

To support the logging of traffic across the DIWS 2 External System interfaces, a document type shall be defined that is used for all DIWS 2 External System interface logs. Document subtypes shall also be defined as necessary to support this capability.

To deliver the document type capabilities required for the DIWS 2 External System integration, **DIWS 2 shall**:

1. Support the logging of traffic across all DIWS 2 External System interfaces using a document type defined for all DIWS 2 External System interface logs.

   ▪ For diagnostic and other purposes, it may be necessary to have the ability to log some or all of the traffic across an external interface.

2. Define document subtypes as necessary to support capturing DIWS 2 External System interface logging information.

3. Define the attributes associated with the document type and subtypes used for logging DIWS 2 External System interface traffic during the requirements gathering and design activities.

4. Automatically capture the following attribute values for all DIWS 2 External System interface logs to include all of:

   a. the logical name of the interface
   b. the user identifier of the person that issued the command to capture the transactions
   c. the date and time for all communication
   d. the source and destination for all communication
   e. the nature of captured information (e.g., commands, parameters, results, content)
   f. the credentials associated with the interface

5. Provide the ability to cease logging all transactions taking place on one or more DIWS 2 External System interfaces.

2.6   User Interfaces

To support the DIWS 2 External System integration, DIWS 2 shall provide a user interface that will support authorized administrative and development personnel in the use, administration, management and diagnosis of the DIWS 2 External System integration interface(s). To deliver the user interface capabilities of the DIWS 2 External System integration, **DIWS 2 shall**:

1. Provide the ability to determine the status of all DIWS 2 External System interface(s).

2. Provide the ability to enable or disable all DIWS 2 External System interfaces.

3. Provide the ability to determine the status of one or more specific DIWS 2 External System interfaces.

4. Provide the ability to enable one or more specific DIWS 2 External System interfaces.

   a. A specific DIWS 2 External System interface shall include the following:
      1. An interface that is accessed by a specific set of credentials.
      2. An interface that is accessed by a specific mode (e.g., API, Web service, Enterprise Service Bus).
      3. An interface that is accessed by a specific logical name.

5. Provide the ability to specify the dates and times that one or more DIWS 2 External System interfaces will automatically be enabled.

   a. For purposes of this requirement
      1. Dates shall be specified as days of the week.
      2. Multiple dates and times shall be specified as dates and times may be recurring
         - An example is to enable interface MAB10 every Monday morning at 7:00 AM. Another example is to enable interface MAB10 and MCRT10 every weekday from September 1 through May 31 at 7:45 AM.

6. Provide the ability to specify a date and time that one or more DIWS 2 External System interfaces will automatically be disabled.

   a. This requirement shall allow multiple dates and times to be specified and any of these dates and times to be recurring (e.g., disable interface MAB10 every Monday morning at 6:00 PM).

7. Provide the ability to disable one or more specific DIWS 2 External System interfaces.

   a. A specific DIWS 2 External e System interface shall include the following:
      1. An interface that is accessed by a specific set of credentials.
      2. An interface that is accessed by a specific mode (e.g., API, Web service, Enterprise Service Bus).
      3. An interface that is accessed by a specific logical name.

8. Provide the ability to assign logical names to each DIWS 2 External System interface.

9. Provide the ability to log all transactions taking place on one or more DIWS 2 External System interfaces.

10. Provide the ability to specify a date and time that logging of one or more DIWS 2 External System interfaces will automatically be enabled.

    a. This requirement shall allow multiple dates and times to be specified and any of these dates and times to be recurring (e.g., enable logging or transactions for interface MAB10 every Monday morning at 6:00 PM).

11. Provide the ability to specify a date and time that logging of one or more DIWS 2 External System interfaces will automatically be disabled.

   a. This requirement shall allow multiple dates and times to be specified and any of these dates and times to be recurring (e.g., disable logging or transactions for interface MAB10 every Monday morning at 6:00 PM).

12. Provide the ability to specify whether logging includes any or all of:

   b. Inbound transactions – commands
   c. Inbound transactions – commands and parameters
   d. Inbound transactions – command, parameters and results (excluding images, documents or content)
   e. Inbound transactions – command, parameters and results (including images, documents or content)

13. Include in the log for all captured transactions:

   a. the date and time for all communication
   b. the source and destination for all communication
   c. the logical name of the interface
   d. the credentials associated with the interface
   e. the nature of captured information (e.g., commands, parameters, results, content)
   f. the user identifier of the person that issued the command to capture the transactions

14. Provide the ability to halt logging all transactions taking place on one or more DIWS 2 External System interfaces.

15. Provide the ability to spool the transaction information taking place on one or more DIWS 2 External System interfaces.

16. Provide the ability to store the results of any logged information in a designated area of the ECM repository.

17. Provide the ability to monitor the transactions taking place on one or more DIWS 2 External System interfaces.

   a. For the purpose of this requirement, monitor shall mean displaying the specific DIWS 2 External System interface transactions in real-time or displaying the contents of the log with a delay that does not exceed five seconds of when a transaction took place.

18. Provide the ability to launch a dialog box or similar user interface to perform scanning, indexing and image quality operations on behalf of an external system.

   a. The dialog box used to perform scanning, indexing and image quality operations shall be a dialog box provided by DIWS 2.

19. Provide the ability to launch a dialog box or similar user interface to perform content searching, with the ability to view content on behalf of an external system.

   a. The dialog box used to perform content searching shall be a dialog box provided by DIWS 2.

20. Provide the ability to launch a dialog box or similar user interface to perform content assembly on behalf of an external system.

   a. The dialog box used to perform content assembly shall be a dialog box provided by DIWS 2.

21. Provide the ability to launch a dialog box or similar user interface to perform content redaction on behalf of an external system.

   a. The dialog box used to perform content redaction shall be a dialog box provided by DIWS 2.

2.7   Reports and Queries

To support the logging traffic across the DIWS 2 External System interfaces, reports and queries shall be provided to locate captured DIWS 2 External System interface logs

To deliver the reporting and query capabilities necessary for the DIWS 2 External System integration, **DIWS 2 shall**:

1. Provide the ability to search for logs that have been captured and stored in the DIWS 2 repository using reports and queries.

   ▪ For the purpose of this requirement, a report is the result of a query that is formatted for printing or storage. A query is search that provides a list of documents that satisfy specified criteria.

2. Provide the ability to define a query that contains one or more of the specified search criteria:

   a. One or more logical interface names.
   b. One or more user identifiers of the person(s) that issued the command to capture the transactions.
   c. A range of dates and times for all communication.
   d. One or more sources and destinations for all communication.
   e. The nature of captured information (e.g., commands, parameters, results, content).
   f. The credentials associated with the interface.
   g. For the purpose of this requirement, "one or more of the specified search criteria", means logical names, user identifiers and multiple dates and times could be specified.

3. Provide the ability to store the results of the query or report in the DIWS 2 repository.

2.8 External Interfaces

DIWS will make available a set of interfaces packaged as an API, Web service and Enterprise Service Bus, that satisfies the capabilities listed in section **2 General Information – DIWS 2 External** System Integration.

To deliver the DIWS 2 External System interface, necessary for the DIWS 2 External System integration, **DIWS 2 shall**:

1. Provide an operational interface for all DIWS 2 environments.

   - For the purpose of this requirement, *all environments* is defined as documented elsewhere in this TO and includes environments such as development, test, training, and production. For example, it would be unacceptable to create an operational interface that could only be used in test and production.

2. Provide an operational interface that can be used concurrently with the operational interfaces for all other DIWS 2 environments.

   - For the purpose of this requirement, *all environments* is defined as documented elsewhere in this TO and includes environments such as development, test, training, and production. For example, it would be unacceptable to create an operational interface that could not be used in the development environment and the test environment at the same time because the interface was being used in the production environment.

3. Ensure that all aspects of the interfaces are capable of operating synchronously, with options for asynchronous operation for specific components.

4. Provide an operational interface that is capable of working simultaneously with multiple external environments.

   - For the purpose of this requirement, multiple external environments should be considered as one or more external environments interacting simultaneously and or concurrently with one DIWS 2 environment.
   - An example of this would be the test and training environment of the DIWS 2 External System interacting concurrently with the DIWS 2 test environment.

5. Provide an operational interface that is capable of working simultaneously with multiple external systems at loads specified in Appendix 5 6.2 Capacity and at performance specified in Appendix 5 6.3 Performance.

   a. "Multiple external systems" shall be considered as one or more external systems interacting simultaneously the Project Core System and/or concurrently with one DIWS 2 environment.
   - An example of an external system is the Project Core System.

6. Provide an operational interface that is multi-threaded from a system perspective.

   For the purpose of this requirement:

   - *Multithreaded from a system perspective* means that one external system would likely be sending multiple simultaneous requests to DIWS 2. This also means that multiple external systems would likely be sending multiple simultaneous requests to DIWS 2.

7. Provide an operational interface that is multi-threaded from a user perspective.

   These too are requirements:

   - *Multithreaded from a user perspective* means that one user could potentially be sending multiple simultaneous requests to DIWS 2.

8. Be available 24x7, with the exception of published maintenance windows approved by the business and State program manager.

   - An example of why the external interface may be required seven days each week, 24 hours each day, is that documents may need to be captured and stored for a web-transaction.
   - The expectation is that DIWS 2 must be available whenever MVA business is being transacted, including business that takes place in person, by mail, electronically, using the Internet, and all other modes used by MVA.

2.9   Current Data Model

There is no data model explicitly defined for the DIWS 2 External System interface or other external interfaces that is relevant to DIWS 2 at this time.

3. Response to DIWS 2 External Systems Integration

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.

In addition to completing the DIWS 2 External Systems Integration response table below, Offerors shall complete the worksheet in the Excel spreadsheet (see Appendix 17 Offeror Response) that corresponds to this Appendix.

Response Requirements Appendix 10 DIWS 2 External Systems Integration			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
2.1	Use Cases for DIWS 2 Integration with External Systems	a. Based on your prior experience, are there additional use cases that should be considered? b. How do you suggest security be handled to protect against malicious or counterfeit e-mail and messages, given the known vulnerabilities associated with authentication, weak encryption, ID spoofing, denial of service attacks and other threats? c. Explain how you would approach testing the use cases. Include how testing would be automated. d. Explain how you would return audit trail information that shows us as part of search results (i.e., use case C12).	
2.2	DIWS 2 Functionality for External System Integration	Explain how you would approach testing each of the requirements? Include how testing would be automated, including tools, the loading of test data, and automated regression testing.	
2.3	Additional Integration Requirements	Describe any requirements in this section that are not met using the out of the box application software that you are proposing (including configuration, but excluding customization) and how and when you would meet these requirements.	
2.4	Process	Explain the process you envision for working with another team to utilize the DIWS 2 External System interface, including how you would: a. ensure the interface requirements are complete b. provide guidance and training on the use of the interface c. operate the interface in a multiple environments (e.g., development, testing, training, production) d. address functional deficiencies (i.e., missing requirements) discovered in the interface e. test the performance of the interface f. test the functionality of interface components that are not used by the first team to use the interface g. measure success of the initial integration	

Response Requirements Appendix 10 DIWS 2 External Systems Integration			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
2.5	Document Types	Describe any requirements in this section that are not met using the out of the box application software that you are proposing (including configuration, but excluding customization) and how and when you would meet these requirements.	
2.6	User Interfaces	Describe any requirements in this section that are not met using the out of the box application software that you are proposing (including configuration, but excluding customization) and how and when you would meet these requirements.	
2.7	Reports and Queries	Describe any requirements in this section that are not met using the out of the box application software that you are proposing (including configuration, but excluding customization) and how and when you would meet these requirements.	
2.8	External Interfaces	Describe any requirements in this section that are not met using the out of the box application software that you are proposing (including configuration, but excluding customization) and how and when you would meet these requirements.	
2.9	Current Data Model	There are currently no requirements defined for this section.	
	Requirements not Met	The State assumes that the Contractor will meet all requirements described in Appendix 10 of the TO. Identify any areas that cannot be met and why these areas cannot be met.	