Appendix 5 – Toolbox Requirements

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

As used in this document, "support," when referring to DIWS 2, should be interpreted as "work with." When referring to the Contractor, should be interpreted as "provide assistance to."

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

The DIWS 2 enterprise content management (ECM) toolbox is a collection of capabilities that is intended to provide a foundation for all DIWS 2 applications. These capabilities have been selected to ensure a solid base-that can be extended in the future. Not all of the technology (e.g., Microsoft Windows 10) is expected to be leveraged immediately, but there is a likelihood that this technology will be utilized prior to the end of DIWS 2's useful life.

This set of toolbox capabilities is not intended to be comprehensive. Most of the leading ECM platforms are sufficiently mature and provide a superabundance of features that allow business goals to be met, albeit in different ways.

The deployment of toolbox capabilities is divided into:

a. Toolbox Basic capabilities shall include all capabilities in Section 3 Capture Functionality Requirements that are not related to FTP/SFTP and messaging; and Section 4 Common ECM Requirements that are not related to redaction and Records management and legal hold.
b. Toolbox Advanced capabilities shall include all capabilities identified herein, including the subset of requirements identified as Toolbox Basic.

2. Introduction

The MVA expects to use DIWS 2 for applications and functions that are not currently included in the DIWS 2 requirements. To allow DIWS 2 to be used for future applications, DIWS 2 contains the DIWS 2 ECM toolbox. It is desirable that the DIWS 2 ECM toolbox capabilities allow the MVA to build additional components in a common and consistent fashion. DIWS 2 accepts content from, and provides content to, multiple sources using a variety of interfaces. The interfaces are illustrated in **Figure 1 DIWS 2 Content Sources and Destination Interfaces**.

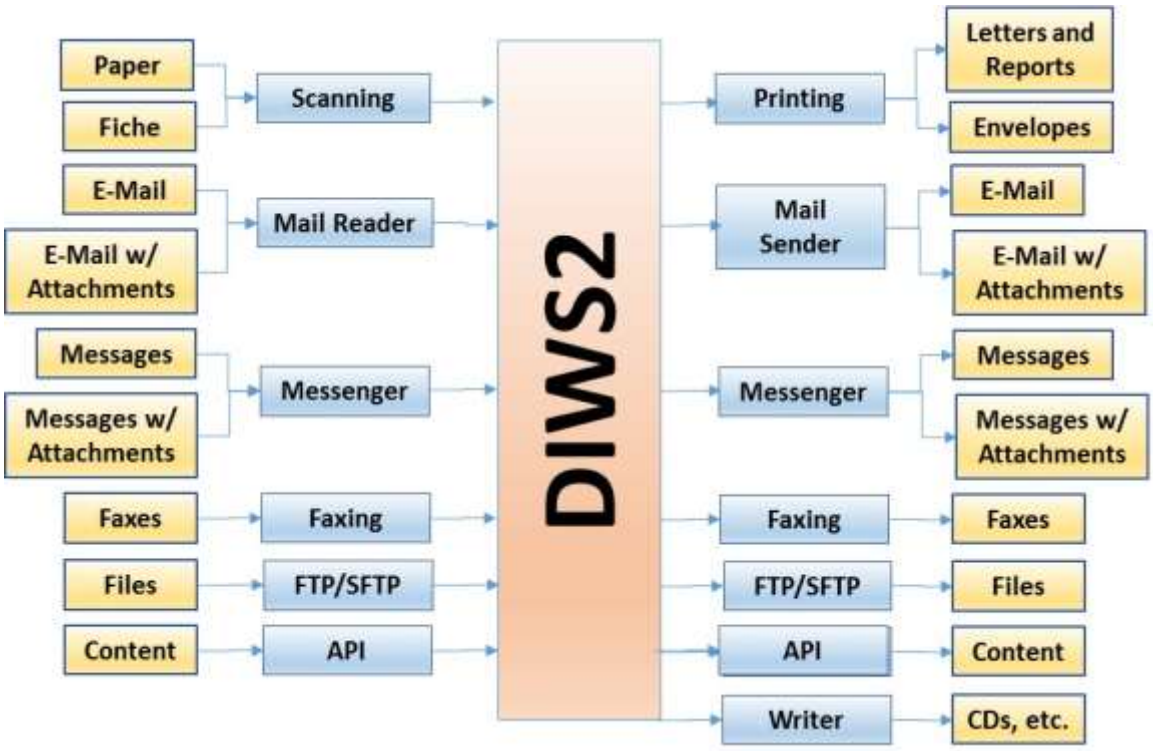

Figure 1 DIWS 2 Content Sources and Destination Interfaces

The Offeror should balance these requirements and its experience to propose a secure, reliable, flexible, enterprise level solution that is cost effective and realistic.

The ECM toolbox functionality is organized by capability and is categorized into four areas:

- Capture Functionality Requirements
- Common ECM Requirements
- ECM Advanced Requirements
- Nonfunctional Requirements

3. Capture Functionality Requirements

The Legacy DIWS ECM system is expected to provide integrated document capture capabilities that:

- Captures MVA-related content
- Assigns index field values to this content
- Allows operators to perform quality control of the content
- Releases the content for storage in the ECM repository.

The requirements for these capabilities have been categorized into the following subsections within the **Capture Functionality Requirements** section:

- Scanning
- Capture
- Incoming FTP/SFTP
- Quality Assurance
- Indexing
- Release

3.1 Scanning

The DIWS 2 scanning capabilities shall:

1. Provide the ability to scan paper documents and produce images in 1-bit bi-scale (also known as black and white).
2. Provide the ability to scan paper documents and produce images in 8-bit grayscale.
3. Provide the ability to scan paper documents and produce images in 24-bit color.
4. Provide the ability to scan single-sided paper documents.
5. Provide the ability to scan double-sided documents images.
6. Provide the ability to enable and disable the automatic detection and scanning of double-sided paper documents.
7. Provide the ability to automatically detect and orient the image file for scanned portrait images.
8. Provide the ability to automatically detect and orient the image file for scanned landscape images.

9. Provide the ability to scan form factors as small as a credit card and Maryland driver's license.
10. Provide the ability to scan form factors as large "A" size, legal size, and "B" size paper.
11. Provide the ability to automatically crop the image to the size of the scanned document.
    - For example, a credit card image should be automatically cropped to 3.370 × 2.125 inches (85.60 × 53.98 mm).
12. Provide the ability to define scanning profiles for content types or families of content types.
13. Provide the ability to scan at resolutions of:
    a. 75 DPI
    b. 150 DPI
    c. 300 DPI
    d. 600 DPI
14. Provide the ability to scan batches of multiple documents.
    - A batch is a collection of documents. Each document in a batch may be one or more pages.
15. Provide the ability to assign a unique identifier to each batch.
16. Provide the ability to assign a unique sequential number to each batch.
17. Provide the ability to assign a unique sequential number and a batch description to each batch.
18. Provide the ability to detect and adjust for different document sizes within a batch.
19. Provide the ability to detect multiple content types within a batch.
20. The system shall permit the batch operator who creates the batch to enter or select information describing the batch (e.g., content type, date)
21. Provide the ability to print a batch cover sheet indicating the batch identification information, scanner identification, scan operator, date, time, number of scanned pages, and other relevant information.
22. Provide the ability to scan documents containing up to as many pages the scanner can scan.
23. Provide the ability to combine multiple scanned documents into one document.
24. Provide the ability to split a document into one or more documents.
25. Provide selected users with the ability to rotate an image permanently.

26. Provide the Document Coordinator, and only that role, the ability to request an image to be deleted (prior to export to document repository).
27. Provide the ability to create a new document upon recognition of a separator page.
    - For the purpose of this requirement, separator pages take many formats and are referred to by many names (e.g., barcode pages, "T pages").
    - Note that this requirement should not be interpreted to mean separator pages are mandatory. There is an expectation that the software would recognize and differentiate new documents without a separate page being present.
28. The scanning functionality shall be able to recognize and decipher:
    a. Alpha-numeric barcodes (Code 128, Code 39, Code 93, LOGMARS)
    b. 2-Dimensional barcodes (PDF417 and DataMatrix)
    c. QR codes™
29. Provide the ability to capture transaction identifiers, business unit identifiers and other index field values from barcoded pages.
    - For the purpose of this requirement, "barcoded pages" are pages that contain information that applies to one or more pages within the batch. Barcoded pages often arrive with a packet of related content. These should not be confused with separator pages which are used to separate documents.
    - Barcoded pages are tightly tied to indexing functionality and are referenced in Section **3.5 Indexing**.
    - Note that this requirement should not be interpreted to mean barcoded pages are mandatory.
30. Provide the ability to capture multiple values from each barcode on each barcoded page.
    - For the purpose of this requirement, "barcoded page" is a page that contains information that applies to one or more pages within the batch. Barcoded pages often arrive with a packet of related content. These should not be confused with separator pages which are used to separate documents.
    - Barcoded pages are tightly tied to indexing functionality and are referenced in Section **3.5 Indexing**.
    - Note that this requirement should not be interpreted to mean barcoded pages are mandatory.

31. Provide the ability to capture information from multiple barcodes on each barcoded page.
    - For the purpose of this requirement, "barcoded page" is a page that contains information that applies to one or more pages within the batch. Barcoded pages often arrive with a packet of related content. These should not be confused with separator pages which are used to separate documents.
    - Barcoded pages are tightly tied to indexing functionality and are referenced in Section **3.5 Indexing**.
    - Note that this requirement should not be interpreted to mean barcoded pages are mandatory.
32. Provide the ability to create scanner profiles for color scanning for each scanner model at each supported resolution and each supported form factor.
    a. "Scanner model", as used in this requirement, shall apply to all scanners in use during development, testing, and production for as long as the system is under development or being supported in production.
33. Provide the ability to create scanner profiles for each scanner model.
34. Provide the ability to create scanner profiles for color scanning for each scanner model at each supported resolution.
35. Provide the ability to create scanner profiles for grayscale scanning for each scanner model at each supported resolution.
36. Provide the ability to create scanner profiles for bi-scale (i.e., black and white) scanning for each scanner model at each supported resolution.
37. Provide the ability to name each scanner profile with a unique name.
38. Provide the ability to centrally manage all scanner profiles.
39. Provide the ability to specify the scanner contrast as part of the scanner profile.
40. Provide the ability to specify the scanner brightness as part of the scanner profile.
41. Provide the ability to specify the scanner color settings as part of the scanner profile.
42. Provide the ability to specify the scanner resolution as part of the scanner profile.
43. Provide the ability to specify the scanner image format as part of the scanner profile.

44. Provide the ability to specify the scanner duplex or simplex as part of the scanner profile.
45. Provide the ability to specify the scanner scan area as part of the scanner profile.
46. Provide the configurable ability based on document type to detect blank documents and:
    a. Ignore/exclude the blank document
    b. Include the blank document
    c. Prompt the user on whether to include or exclude the blank document.
47. Provide an application that is configured for scanning the content associated with all DIWS 2 document types and content types using any and all of the scanning functions and parameters.

3.2 Capture

Capture is a general term that is used to refer to acquiring and storing content and the associated metadata with the content. Those capture requirements specifically related to scanning are located in Section **3.1 Scanning**. Requirements in this section apply to all forms of capture, including scanning.

The DIWS 2 Capture capabilities shall:

1. Provide document recognition capability for a minimum of **4,000** content types.
   - 4,000 content types is the future growth number.
2. Train the system to automatically recognize **400** content types and associate the document with its appropriate content type.
   - 400 content types is the target for the end of the Contract.
3. Be configurable to capture all images in a lossless format when feasible or legislated.
   - For purposes of this requirement, images may originate from a scanner, fax machine or other source.
4. Be configurable to capture all images in TIFF format.
   - For purposes of this requirement, images may originate from a scanner, fax machine or other source.
5. Be configurable to capture all multipage images as a multipage image file.
   - For purposes of this requirement, images may originate from a scanner, fax machine or other source.

6. Be configurable to capture all multipage images as a set of single image files.
   - For purposes of this requirement, images may originate from a scanner, fax machine or other source.
7. Be configurable to capture all fax images in TIFF format with CCITT G4, subject to any extensions provided by automated fax capturing equipment.
8. Capture all e-mail, including all parts of the e-mail header and body.
   - The standard format for an e-mail is described in RFC 5322, commonly referred to as the Internet Message Format (IMF).
9. For external e-mail that was forwarded internally, capture all available information about the external sender.
   - External e-mails may arrive at the enterprise from external sources via e-mail addresses other than those set up for capturing e-mail. In these cases the recipient will forward the e-mail to the e-mail address set up for capturing e-mail. It is important to capture the information about the external sender that will appear earlier in the e-mail thread.
   - In the event an e-mail was forwarded multiple times externally to the MVA, capture the external e-mail information that forwarded the e-mail to the MVA.
   - "All available information" acknowledges the fact that the full header may not be available for e-mails that are forwarded. However, the sender, subject, date and time should be available.
10. Be configurable to capture all e-mail attachments in their native format.
    - For the purpose of this requirement, "native format" is the format of the attachment.
    - This requirement is intended to preserve the evidentiary value and other value of preserving a file in the form it was received. This requirement should not be interpreted as a replacement for other requirements that allow captured content to be converted to a standard format or stored in a decrypted format.
11. Be configurable to convert all e-mail attachments to the default format for the content type.
    - This is intended to allow all attachments (that may arrive in a diverse number of formats) to be saved in the default format associated with a content type.
    - This requirement is not intended to preclude storing e-mail attachments in their native format.
12. Detect whether an e-mail attachment is encrypted and provide the ability to set metadata to indicate attachment is encrypted.

13. Provide the ability to configure the system to store encrypted e-mail attachments as-is.
    - For the purpose of this requirement, "store encrypted e-mail attachments as-is", shall be interpreted as storing the attachment without modifying the content of the file. This means the encrypted file would be stored in its encrypted state.
    - This requirement is intended to preserve the evidentiary value and other value of preserving a file in the form it was received. This requirement should not be interpreted as a replacement for other encryption performed by the DIWS 2 system.
14. Provide the ability to store a password for all encrypted e-mail attachments.
15. Provide the ability to configure the system to store encrypted e-mail attachments as decrypted files.
    - For the purpose of this requirement, "store encrypted e-mail attachments as decrypted files", shall be interpreted as storing the attachment after decrypting the file.
    - This requirement should not be considered mutually exclusive with requirements for storing encrypted e-mail attachments without decryption.
16. Capture all text messages in their native format.
17. Provide document recognition capability that automatically detects a new document without the presence of a separator page.
18. Provide the ability to automatically extract the text from fields on up to 400 content types.
    - Most content types that automatic extraction will be applied to are single page image formats (e.g., TIFF).
    - If a content type contains two or more pages, then each page of the content type will count as one content type for the purposes of satisfying 400 content types.
19. Provide the ability to specify up to **40** fields on each page, with an average of 10 fields per page, of each content type and extract the text in those fields.

    For the purpose of this requirement:
    - "Extract" will typically be taken in the context of converting image information into text information.
    - "Fields" are predefined locations in a content type such as an image.
    - Typically, across all content types that are subject to automatic field extraction, there are ten fields per page of each content type. However, the upper limit is 40 fields per page, of each content type.
20. Provide the ability to capture:

a. scanned documents
b. incoming e-mails
c. incoming e-mail attachments
d. outgoing e-mails
e. outgoing e-mail attachments
f. incoming faxes
g. outgoing faxes
h. incoming FTP transmissions
i. incoming Secure FTP (SFTP) transmissions
j. incoming messages (SMS, MMS, iMessage/APNs)
k. outgoing messages (SMS, MMS, iMessage/APNs)
l. files from the desktop
m. files from a file store or file share
n. content from a drop box
o. files from an MVA-authorized encrypted/unencrypted flash drive

21. Provide the ability to automatically recognize the following data on all documents:

    a. Date of birth (in multiple date formats)
    b. Phone/fax numbers (in multiple formats)
    c. SSN/TPI number
    d. Zip code
    e. e-mail address
    f. other patterns defined by the business

22. Provide the ability to automatically place a captured image/document into a document workflow where the workflow is determined by the content type and metadata.

23. Provide the ability to automatically associate captured e-mail with captured e-mail attachments.

24. Provide the ability to automatically capture, for all incoming and outgoing faxes, the following information for each attempt/retry:

    a. the originating fax number
    b. the destination fax number
    c. the subject of the fax
    d. the number of pages faxed (including cover page)
    e. the fax format
    f. the date and time the fax transmission began
    g. any errors encountered on the transmission

    - For the purpose of this requirement, “capture” is considered to mean identify and store.

25. Provide the ability to automatically capture, for all incoming and outgoing text messages, the following information:
    a. the originating text number
    b. the destination text number
    c. the subject of the text
    d. the number of bytes texted
    e. the number of attachments (e.g., images for MMS or APNs messages)
    f. the text format (e.g., SMS, MMS, iMessage/APNs)
    g. the date and time the text transmission began
    h. any errors encountered
    - For the purpose of this requirement, "capture" is considered to mean identify and store.
26. Provide the ability to automatically capture, for all incoming and outgoing e-mails, the following information:
    a. the originating e-mail address
    b. the destination e-mail address(es)
    c. the subject of the e-mail
    d. the number of bytes
    e. the number of attachments (e.g., images for MMS or APNs messages)
    f. the time the e-mail transmission began
    g. the error message if an error message was received
27. The capture functionality shall be able to recognize and decipher:
    a. Alpha-numeric barcodes (Code 128, Code 39, Code 93, LOGMARS)
    b. 2-Dimensional barcodes (PDF417 and DataMatrix)
    c. QR codes™
    - For the purpose of this requirement, "recognize and decipher" is considered to mean identify, translate to text, and store.

28. Maintain a configurable profile for each device that is capable of providing content to DIWS 2 that includes relevant operational parameters for that device.

    For the purpose of this requirement, the minimal operational parameters include:

    a. scanners – brightness, contrast, dpi, scanner credentials, action to take on device offline or repeated failure
    b. incoming e-mails – e-mail address, frequency to check for e-mails, e-mail credentials, action to take on device offline or repeated failure
    c. incoming faxes – incoming fax number, frequency to check for faxes, fax machine credentials, action to take on device offline or repeated failure
    d. incoming SFTP/FTP transmissions – frequency to check for FTP/SFTP transmissions, SFTP/FTP credentials, action to take on device offline or repeated failure
    e. incoming messages – frequency to check for messages, supported protocols (e.g., SMS, MMS, iMessage/APNs), messaging credentials, action to take on device offline or repeated failure
    f. drop box – frequency to check drop box for content, drop box credentials, action to take on device offline or repeated failure

29. Maintain a configurable profile for each device that is capable of requesting or accepting content from DIWS 2 that includes relevant operational parameters for that device.

    For the purpose of this requirement, the minimal operational parameters include:

    a. outgoing e-mails – e-mail address, number of times to retry, maximum byte count, e-mail credentials, action to take on device offline or repeated failure
    b. outgoing faxes – outgoing fax number, number of times to retry, maximum page count, time between retries, hours of operation, fax machine credentials, action to take on device offline or repeated failure
    c. outgoing SFTP/FTP transmissions –number of times to retry, time between retries, hours of operation, SFTP/FTP credentials, action to take on device offline or repeated failure
    d. outgoing messages –supported protocols (e.g., SMS, MMS, iMessage/APNs), maximum byte count, maximum attachment count, messaging credentials, action to take on device offline or repeated failure
    e. drop box – number of times to retry, time between retries, hours of operation, drop box credentials, action to take on device offline or repeated failure

30. Provide one or more applications that are configured for capturing the content associated with all DIWS 2 document types and content types using any and all of the capture functions and parameters.

31. Provide one or more applications that are configured for capturing content using smartphones and tablets when working remotely and at client/customer locations and transmitting that content to DIWS without returning to the office.

    For the purpose of this requirement:

    a. It is often necessary to travel to an external site and use a smartphone or tablet to capture images of people, equipment and facilities. These images shall be indexed and transmitted to DIWS using communications capabilities built into the device.
    b. In another scenario the staff are working offsite for days or weeks at a time. There is an expectation that the images that the staff captures shall be sent to DIWS immediately, possibly triggering a workflow, without requiring the worker to visit an MVA facility.
    c. An example is visiting a driver instructional school where images of the classroom, the instructors and the vehicles used for driver training are captured on a cellphone or a tablet. The captured images are then indexed on the device and transmitted back to the DIWS 2 for immediate use. The application shall be smart enough to know when a communications signal is available to begin transmitting the images and to continually retry transmission until successful.

3.3 Incoming FTP/SFTP

Within the capture capabilities, there are a set of requirements necessary to enable capturing incoming FTP and SFTP communications.

The DIWS 2 FTP and SFTP capabilities shall:

1. Provide external users with one or more secure areas ("Secure Area") where they can save electronic documents using FTP and SFTP.
   - For the purpose of this requirement, *external users* refers to MVA customers, suppliers, and other non-MVA staff, located outside of the firewall.
2. Protect the Secure Area with a password that is known only to each external user.
3. Allow external users who have more than one Secure Area to be assigned a password for accessing each Secure Area.

4. Isolate each external user's secure area from all other Secure Areas.
   - For the purpose of this requirement, *isolate* could be as simple as using separate folders with adequate security protection for each external user.
5. Ensure external users are prevented from having any form of access to another external user's Secure Area.
   - For the purpose of this requirement, *any form of access* refers to reading, writing, updating, deleting, renaming, searching, listing, copying, or altering the security of the content in the secure area or metadata about the content in the Secure Area.
6. Scan all content saved in the secure area by an external user for virus and other malware threats immediately after the content is saved in the Secure Area.
7. Provide a configurable option to allow external users to overwrite their documents in the Secure Area.
   - For example, external users may be granted permission to update or replace previously saved content, such as in the case of an error during content transfer.
8. Provide a Secure Area of up to a configurable number of bytes per external user, used to store content.
   - For the purpose of this requirement, configurable value shall be defined as a range between 10MB and 10TB. The initial value is expected to be approximately 2GB.
   - The Offeror shall, for the purpose of initial sizing, use a 2GB capacity. This does not relieve the 10TB upper limit that can be achieved by adding additional storage in the future.
9. Provide a Secure Area capable of storing individual documents that are up to up to a configurable number of bytes in size.
   - For the purpose of this requirement, configurable value shall be defined as a range between 10MB and 16GB. The initial value is expected to be approximately 100MB.
   - For the purpose of this requirement, "storing individual documents that are up to a configurable number of bytes" refers to the total amount of storage occupied by one document stored by an external user.
10. Provide a configurable capability to send an e-mail, text, or other acknowledgement to external users, referred to as the FTP acknowledgement, each time a document has been saved in their Secure Area.
11. Provide a configurable capability to send an e-mail to external users each night, referred to as the nightly inventory e-mail, following any documents saved in their Secure Area.

12. Include the following information in the nightly inventory e-mail sent to the external user:
    a. Time and date the e-mail was generated.
    b. Name of the external user.
    c. File names and extensions of each document saved in their Secure Area.
    d. Date and time stamp of each document saved in their Secure Area.
    e. File size in bytes of each document saved in their Secure Area.
    f. Name of the Secure Area where the documents were saved.
13. Allow the nightly inventory e-mail feature to be configurable to allow a mailing list containing one or more names of DIWS defined roles to be copied on the e-mail.
14. Provide an automated process configurable for each external user and Secure Area that shall run to transfer documents from the Secure Area into DIWS:
    a. Immediately (e.g., on demand).
    b. Daily at a specified time.
    c. On a specific date and time in the future.
    d. Daily at a specified time beginning after a specific future date and time.
15. Provide an audit trail, consistent with audit trail requirements enumerated in Section 4.12 Audit Trail for:
    a. All access to the Secure Area
    b. All transfers from the Secure Area to the DIWS repository
    c. All transfers from the DIWS repository to the Secure Area
16. Provide an automated process configurable for each external user and Secure Area that deletes all content from the Secure Area after it has been transferred into DIWS.
17. Automatically index all documents transferred from the Secure Area to the DIWS repository using information from the file name and external user's Secure Area.
18. Provide an application that is configured for capturing the content associated with all DIWS 2 document types and content types using any and all of the FTP/SFTP functions and parameters.
    - For the purpose of this requirement, "capturing the content" refers to content that will be sent to a receiving FTP/SFTP partner.
19. Provide an application that is configured for receiving the content associated with all DIWS 2 document types and content types using any and all of the FTP/SFTP functions and parameters.
    - For the purpose of this requirement, "receiving the content" refers to content that arrived from a sending FTP/SFTP partner.

20. Provide external users with a user interface for:
    a. accessing the Secure Area
    b. a mechanism for saving documents in the Secure Area
    c. performing other operations the external user is allowed to perform in Section 3.3 Incoming FTP/SFTP

3.4 Quality Assurance

The DIWS 2 Quality capabilities shall:

1. Provide the ability to adjust image contrast.
2. Provide the ability to adjust image brightness.
3. Provide the ability to adjust image skew (and deskew).
4. Provide the ability to perform image cropping.
5. Provide the ability to perform image despeckling.
6. Provide the ability to adjust image rotation.
7. Provide the ability to verify color, grayscale and bi-scale fidelity.
    a. Bi-scale is represented as one bit per pixel.
    b. Grayscale is represented as one byte (8 bits) per pixel.
    c. Color is represented as three bytes (24 bits) per pixel.
8. Provide the ability to verify legibility.
9. Provide the ability to verify sharpness of image.
10. Provide the ability to verify dimensional accuracy compared with the original.
11. Provide the ability to verify there is no distortion in the image.
12. Provide the ability to verify completeness of the overall image area.
13. Provide the ability to verify index data accuracy.
14. Provide the ability to verify index format compliance.
15. Provide the ability to verify image format compliance.
16. Provide the ability during quality control to designate any page in a document for rescanning.
17. Provide the ability during quality control to designate one or more pages in a document for rescanning.
18. Provide the ability during quality control to mark one or more documents in a batch for rescanning.
19. Provide the ability during quality control to mark an entire batch for rescanning.

20. Provide the ability to set a "manual verification required" flag at the point that content is captured for a configurable set of content types.
    - "Manual verification required" allows content to be inspected before becoming subject to record retention and other rules.
    - For example, content types that are used exclusively for content that is uploaded by external users could contain content that is considered malicious, offensive, inappropriate, and unrelated to business. In these cases, the content is permitted to be deleted before reaching the ECM repository (see requirements 26 and 27 below). This requirement does not perform the deletion; it only allows the content to be deleted before becoming subject to the controls (e.g., security) of the ECM repository.
21. Provide the ability to set a "manual verification required" flag for content that arrives from a configurable set of interfaces.
    - For example, content that arrives via an e-mail interface or fax interface could contain content that is considered malicious, offensive, inappropriate, and unrelated to business. Interfaces include, but are not limited to, specific e-mail addresses, FTP accounts, and fax numbers.
    - Similar to requirement 21, this requirement does not perform the deletion; it only allows the content to be deleted before becoming subject to the controls (e.g., security) of the ECM repository.
22. Provide an aging report for all content that has the "manual verification required" flag set.
23. Provide a report for all content that has the "manual verification required" flag set, organized by content type and sub-sorted by date.
24. Provide the ability to clear "manual verification required" flag using an API.
25. Provide the ability to clear "manual verification required" flag using a graphical user interface.
26. Provide the ability to delete content at the time the "manual verification required" flag is being cleared.
27. Allow content to be immediately deleted independent of the record retention rules if deletion is performed while clearing the "manual verification required" flag.
    a. Content with the "manual verification required" flag set shall not be subject to record retention rules.
    b. Content with the "manual verification required" flag set shall not be subject to legal hold rules.
    c. Content that is being "immediately deleted" shall not marked for deletion [at a later time].

28. Allow content in DIWS 2 to be accessed from external systems when the "manual verification required" flag is set or is not set.
    - External systems may also access content when the "manual verification required" flag is not set. This comment is to ensure this flag does not limit access to this content. It is already understood that content can be accessed when the flag is not set.
29. Provide external systems with the ability to execute functionality that clears the "manual verification flag".
30. Allow content to be automatically deleted if the "manual verification required" flag has not been cleared within a configurable period of time that is based on the document type and/or metadata values.
31. Provide an application that is configured for performing quality assurance on the content associated with all DIWS 2 document types and content types using any and all of the quality assurance functions and parameters.

3.5 Indexing

The DIWS 2 indexing capabilities shall:

1. Allow metadata to be associated with all documents, including non-resident documents.
    - Non-resident documents are documents that are stored externally to the content management system (CMS), but are indexed by the CMS.
2. Allow a unique set of metadata to be used for each content type.
3. Provide the ability to manually index all captured documents.
4. Provide the ability to automatically detect the presence of data types in fields within scanned images.
    - Examples of data types include numbers, text, dates and times.
5. Provide the ability to automatically extract indexing information and other data from the subject line and other fields on incoming faxes.
6. Provide the ability to automatically extract indexing information and other data from the subject line and other fields on incoming e-mails.
7. Provide the ability to automatically extract indexing information and other data from the text accompanying images in text messages.
8. Provide the ability to automatically extract indexing information and other data from fields within scanned images based on the content type of the image.
    - Many images have highly structured layouts (e.g., driver's license, vehicle title) from which information can be reliably extracted.

9. Provide the ability to return all extracted data, including values that were not used for indexing, to external applications that use DIWS 2 for content type recognition.
10. Prior to completing indexing-related activities, automatically perform all necessary activities to enable full-text search on the content within the document.
11. Provide the ability to index a subset of the documents in a batch of scanned documents.
12. Provide the ability to index all documents in a batch of scanned documents.
13. Enable sticky fields when indexing.
    - For purposes of this requirement, sticky fields are fields that are prefilled with the value used to index the prior document.
14. Preconfigure sticky field behavior based on content type.
    - For purposes of this requirement, sticky fields are fields that are prefilled with the value used to index the prior document.
15. Allow the index operator to override sticky field behavior.
    - For purposes of this requirement, sticky fields are fields that are prefilled with the value used to index the prior document.
16. Allow the index operator to turn on sticky field behavior for any field.
    - For purposes of this requirement, sticky fields are fields that are prefilled with the value used to index the prior document.
17. Provide the ability to preconfigure fields to be prefilled with values based on the content type being indexed.
18. Provide the ability to designate index fields as mandatory, optional or not applicable.
19. Provide the ability to use all database data types as index field data types.
    - For the purpose of this requirement, the database refers to the database used by the ECM system, subject to the database constraints identified in Appendix 11 and Appendix 5, Section 6.4 Integration.
20. Provide the ability to allow an index field to be assigned multiple values.
21. Provide the ability for the user to select index values from a list of values where the list is a predefined list of values.
    - Examples of a list of values would be the days of the week, months of the year, colors, states, countries, counties, and other values from configurable enumerated lists.
22. Provide the ability for the user to select index values from a list of index values where the list is the result of a database query.

23. Provide the ability for the user to select index values from a list of index values where the list is obtained from external reference data or external master data.
    - The expectation is that DIWS 2 will access external systems to obtain the reference data for a significant number of index values. This will need to be designed to ensure performance objectives are met.
24. Provide the ability to quickly navigate through a list of index values by typing consecutive letters of values in the index or by using scrolling operators.
25. Provide the ability to apply constraints to all index field types.
    - For the purpose of this requirement, index field types include, but are not limited to: current date, past dates, times, future dates, number, currency, text, and enumerated list of values.
26. Provide the ability to automatically index all captured documents.
27. Provide the ability to associate two images and/or documents together.
    - For example, associate a driver's photo and a driver's signature together so that they are able to be connected with each other.
28. Provide the ability to link three images and/or documents together.
    - For example, link a driver's photo, signature, and a document together so that they are able to be associated with each other.
29. Provide the ability to use geospatial metadata embedded in images to automate the indexing of images that were geotagged.
30. Provide the ability to automatically associate geospatial coordinates with addresses and business names for use in indexing.
31. Provide the ability to use geospatial metadata embedded in messages to automate the indexing of messages that wee geotagged.
    - SMS images are typically tagged using the GeoSMS standard.
32. Utilize transaction identifiers, business unit identifiers and other index field pairs from barcoded sheets to obtain additional index information from an external system.
    - Barcoded sheets are defined in Section **3.2 Capture**. They arrive with a batch of related content and contain barcoded information (e.g., transaction identifiers, business unit identifiers, and index field values) relevant to that content.
    - The additional index information may contain document/content types and index field pairings. It may also contain no additional index information if the barcoded information was sufficient for indexing the content.

33. Utilize transaction identifiers, business unit identifiers, other index field pairs from barcoded sheets, and additional index information from an external system to index the content that accompanies a barcoded sheet.
34. Consistently apply the field validation requirements identified in Section **4.2 Field Validation** to all fields in the Capture Functionality Requirements and the enterprise CMS.
35. Provide an application that is configured for indexing the content associated with all DIWS 2 document types and content types using any and all of the indexing parameters and functionality.

3.6 Release

The DIWS 2 release capabilities shall:

1. Allow the quality or index operators to designate all or part of a batch for release to the CMS.
2. Transfer all or part of a batch designated for release from the functionality to the CMS.
3. Confirm that the transfer of content and index information from the capture functionality to the CMS took place without loss or corruption of data or content.
4. Automatically trigger the appropriate workflow within DIWS 2 for those documents or content types identified in a configurable list.
5. Automatically invoke the appropriate API, web service or other interface to trigger an appropriate workflow external to DIWS 2 for those documents or content types identified in a configurable list.
    a. The configurable list shall identify the external system, the mechanism triggering a workflow in the external system, and the information that will be passed to the external system when the workflow is triggered.
    b. The external system shall be identified based on the content/document type, and one or more index values (i.e., metadata values).
6. When triggering workflows, either in DIWS 2 or external systems, allow the trigger to be to be tied to an individual document or to collections of documents.
7. Provide a mechanism for external systems to manage the configuration values for releasing content to external systems for all content associated with all DIWS 2 document types and content types.

8. Automatically trigger the generation of a notification to the appropriate user or user group for those documents or content types identified in a configurable list.
9. Provide an application that is configured for releasing content to the DIWS 2 repository for all content associated with all DIWS 2 document types and content types.
10. Provide an application that allows managing the configuration values for releasing content to external systems for all content associated with all DIWS 2 document types and content types.

4. Common ECM Requirements

The Common ECM Requirements are called this because they conceptually apply to the functionality found both within the capture functionality and to functionality located outside the capture functionality.

Because Offerors may incorporate capture functionality with a profusion of features and capabilities, the organization of these requirements in this document is intended to provide a degree of flexibility that is not intended to favor one vendor's capture functionality.

When the requirements in Section **4 Common ECM Requirements**, are used in multiple areas within the DIWS 2 system, the user experience shall be the same across all areas. This means navigation should behave consistently, searches should be consistent, the information captured in audit trails should be consistent, and all functionality identified in this TO should be consistent.

The scope of the common ECM requirements includes:

- Content Creation
- Field Validation
- Electronic Forms
- Searching
- Navigation
- Redaction
- Workflow
- Reports and Queries
- Administration
- Security and Privacy
- Audit Trail
- Journaling
- General Auditing and QA Auditing
- Records Management and Legal Hold

4.1 Content Creation

DIWS 2 provides the ability to create content such as MS Word documents and MS Excel spreadsheets using the tightly integrated capabilities provided by the ECM.

DIWS 2 content creation capabilities shall:

1. Allow the creation of documents in the repository from within MS Office tools.
   - For example, provide a button or pull-down menu within MS Word to create a document in the repository.
2. Allow opening documents in the repository from within MS Office tools.
3. Allow editing documents in the repository from within MS Office tools.
4. Allow saving documents to the repository from within MS Office tools.
5. Provide standardized templates for each content type that is presented to the user when creating documents.
6. Enable composing/editing MS Office documents in a web browser.
7. Allow new documents to be created without a workflow.
8. Include providing the capability to create, manage, and retrieve language renditions for a document.
   - For the purpose of this requirement, a "language rendition" is a translation or transliteration of the content in a document. For example, the same document may exist in English and Spanish.
9. Include providing the capability to create, manage, and retrieve language renditions for document templates.
   - For example, the same document template may exist in English and Spanish.
10. Provide check-in and check-out to manage versions and changes.
11. Allow all versions of a document to be deleted.
12. Allow a single, specific version of a document to be deleted.
13. Enable the creation of PDF renditions of documents and images.
14. Enable the creation of HTML renditions of documents and images.
15. Enable the creation of XML renditions of documents and images.
16. Enable the creation of TIFF renditions of documents and images.
17. Enable rendering the following document and image formats to PDF:
    a. TIFF
    b. JPEG
    c. All MS Office formats
    d. Text
    e. Rich Text
    f. PDF (in the case of rendering multiple PDF documents into one PDF document)

18. Enable rendering any format to any other format through use of plug-ins or similar architecture.
    a. The formats that shall be supported are listed in Section 4.1 Content Creation, Requirements 13, 14, 15, 16, and 17.
    - For the purpose of requirements 18 and 18.a, the focus is on the ability to render using a plug-in.
    - For example, by installing a plug-in that converts PDF documents to MS Word, DIWS 2 would be able to render MS Word documents from PDF files.
19. Allow dynamic references (via hyperlink) to be created to documents stored in the DIWS 2 repository from within documents.
20. Allow dynamic references (via hyperlink) to be created to documents stored in the DIWS 2 repository from within e-mail.
21. Allow dynamic references (via hyperlink) to be created within documents to be configurable to specific versions of the document stored in the DIWS 2 repository.
22. Allow dynamic references (via hyperlink) to be created within the e-mail to be configurable to specific versions of the document stored in the DIWS 2 repository.
23. Allow dynamic references (via hyperlink) to be created within documents to be configurable to the most recent version of the document stored in the DIWS 2 repository.
24. Allow dynamic references (via hyperlink) to be created within the e-mail to be configurable to the most recent version of the document stored in the DIWS 2 repository.
25. Allow the attachment of documents stored in the DIWS 2 repository to an e-mail, without manually saving the document prior to attaching the document.
    - For example, occasionally the need arises to send documents as an e-mail to those that do not have access to the ECM system. In cases where a document must be sent as a file attached to an e-mail the ECM system should not require the user to save a document as a file on their C: drive and then import the file as an attachment to an e-mail.

26. Ensure all PII and PHI content sent using e-mail is encrypted.
    - For example, e-mail sent from one MVA e-mail user to another MVA e-mail user.
    - "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using a technology that: (1) is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards issued by the National Institute of Standards and Technology; and (2) renders such data indecipherable without an associated cryptographic key necessary to enable decryption of such data.
27. Maintain a configurable list of fax destinations and for each destination whether faxes sent to those destinations require encryption:
    a. always
    b. for PHI content
    c. for PII content
28. Ensure all PII and PHI content sent using electronic fax is encrypted unless the destination fax is configured in DIWS 2 as not requiring encryption.
    - Some faxes such as those within the building may not require encryption to share PII and PHI content.
29. Allow the transmission of documents stored in the DIWS 2 repository via FTP/SFTP, without manually saving the document prior to attaching the document.
30. Ensure all PII and PHI content sent using FTP/SFTP will be encrypted unless sent by SFTP or destination FTP is configured as not requiring encryption.

4.2 Field Validation

DIWS 2 shall consistently apply the same set of field validation criteria to all input fields, whether located in fields used by the capture functionality or the capabilities of the more general ECM.

For purposes of these requirements, input fields are those fields accessible to users and electronic interfaces where data is supplied for indexing, searching and other purposes.

DIWS 2 field validation capabilities shall:

1. Provide the ability to perform data validation on all index fields using a fixed list of values
2. Provide the ability to perform data validation on all index fields using a data look-up from an external system.
3. Provide the ability to perform data validation on all index fields using values in database table.

4. Provide the ability to perform data validation on all index fields to ensure compliance with a data format (e.g., date, time, SSN, zip code).
5. Provide the ability to perform data validation on all index date fields requiring future dates.
6. Provide the ability to perform data validation on all index date fields requiring past dates.
7. Provide a configurable manual validation override for all past date fields.
8. Provide a configurable manual validation override for all future date fields.
9. Provide the ability to perform data validation on all index fields where the type of validation is based on the value of another field.
10. Ensure all mandatory data fields have been completed when a user attempts to submit information.
11. Interactively inform the user of errors based on real-time validations performed as the user enters data.
12. Provide a data dictionary that defines each field for used for indexing.
13. Provide a master data source for all fields for used for indexing. Examples include but are not limited to:
    a. State names
    b. State abbreviations
    c. Country names
    d. Country abbreviations (three letter and two letter)
    e. County names
    f. City/Town/Village names
    g. Month names
    h. Month abbreviations
    i. VINs
    j. Titles
    k. Registrations
    l. Soundex
    m. Gender
    n. Race/Ethnicity

4.3 Electronic Forms and Signatures

Electronic forms are collections of Structured Data and possibly unstructured data that reside within the rows of one or more database tables. Forms may be presented to a user with information pre-populated from a database or other source. While this information normally originates from a database, it may also include images (e.g., image of person,

image of signature). The user is allowed to enter information into areas of a form associated with the user's role. A form may then be routed as part of a workflow.

The DIWS 2 electronic forms capabilities shall:

1. Provide the ability to create electronic forms.
2. Provide the ability to enter data into electronic forms.
3. Provide the ability to apply an electronic signature to an electronic form.
4. Provide the ability for a user to delegate the user's electronic signature for a specific purpose to another user for a specified period of time.
    a. Electronic signatures shall be able to be delegated for specific forms, all forms, specific workflows, all workflows, specific reviews, all reviews, specific approvals, all approvals, and correspondence tracking.
5. Provide the ability for a user to terminate delegation of the user's electronic signature to another user.
6. Provide the ability to apply one or more electronic signatures to an electronic form.
    - Electronic signatures are a recognition that the form has been signed and typically requires a user to enter a PIN or biometric information. The electronic signature does not inherently require an image of a person's wet-ink signature to be present.
    - Some forms may require electronic signatures by multiple approvers.
    - Electronic signatures do not preclude the possibility that wet-ink signatures may also be required on a form.
    - See related signature requirement in Section 4.7 Workflow, Requirement 11.
7. Provide the ability for a user to apply his/her electronic signature in multiple locations on an electronic form.
8. Provide authentication of the person providing the electronic signature at the time the electronic signature is applied.
9. Provide authentication of the person delegating his/her electronic signature at the time the electronic signature is delegated.
10. Provide authentication of the person providing the electronic signature using a password, pin, biometric or other technique(s) acceptable to the MVA Project Manager.
    - See related signature requirement in Section 4.7 Workflow, Requirement 11.

11. Provide the ability to apply a representation of a wet-ink signature to an electronic form.
    - A representation of a wet-ink signature is an image of a person's signature applied to the appropriate field or area of a form.
    - See related signature requirement in Section 4.7 Workflow, Requirement 11.
12. Provide the ability to ensure the representation of a wet-ink signature is the wet-ink signature associated with the person applying the representation to an electronic form using a technique that minimizes impersonation.
13. Provide the ability to limit data entry to certain fields of an electronic form.
    - For example, on a change control form the initiator may fill in fields within the proposal section, but be unable to enter data into fields in the analysis, review and approval sections of the form.
14. Provide the ability to restrict electronic signature fields to appropriate users.
    - If a user is not authorized to sign an electronic form in his/her current role, the signature field should not accept the signature.
15. Provide the ability to include images on an electronic form where the images come from either or both of:
    a. the DIWS 2 repository
    b. the user's desktop
    - For an example, a form may include an image of the person completing the electronic form.
16. Provide the ability to route forms and the form data through a workflow.
17. Maintain an audit trail on all revisions of a form, including changes to the form, sections, fields, and other structural components of the form.
18. Maintain an audit trail on all revisions to data on a form.
    - "Revisions to data on a form", includes entering, deleting, changing or refreshing values in fields on a form.
19. Provide search functionality on data within forms.
    - This provides the ability to search for a specific field on a collection of forms for a specific value. For example, search all change management forms for approval dates in July 2016.
20. Provide search functionality on forms.
    - This treats the completed form as any other document when performing searches.
21. Return the associated forms as the result of a search.

22. Allow data within fields on a form to be searched.
    - This provides the ability to search the data fields within a specific form. For example, a multi-page form that contained many fields may be searched for all occurrences of "compliance".
23. Provide version control for all forms.
    - In the context of this requirement, "forms" refers to the form template. Think of this as a blank form that will be filled in.
24. Associate data with the version of the form that was used to collect the data.
    - All data entered on a form should be associated with the version of the form that the data is entered on.
    - Think of this as a blank form that has been filled in with data values.
25. Provide the ability for a user to bring his/her data from an earlier or later version of a form to a later or earlier version of a form.
    - For example, Mrs. Smith begins entering her information onto the 2016 version of a form. Before she submits the form, she learns that there is a 2017 version of the form that she is required to use. Mrs. Smith should be provided with a mechanism that allows her to automatically have her data applied to the 2017 version of the form.
26. Recreate earlier versions of forms.
    - For example, the 2016 version of a form contained five data fields and the 2020 versions of a form contains 10 fields. If Mrs. Smith completed the 2015 version of the form, that version of the form should be retrievable with the data entered by Mrs. Smith populated into the form.
27. Store all form data within a database.
28. Allow all web browsers used by DIWS to be used to fill in electronic forms.
    - Web browsers are listed in Appendix 11, Section 6 User Interface, requirements 13-16.
29. Allow form sections to be assigned to specific groups/roles in the context of a workflow.
30. Assemble form content into one document as needed.
    - There is no prescription within these requirements that form data must be stored in the same physical structure (e.g., file) that the form template is stored. This requirement provides the ability to create such a structure that contains the form template and form data assembled into one document.
31. Provide the ability to route forms based on data entered into the form.
32. Provide the ability to add comments/notes to form fields.

33. Automatically extract data from scanned forms.
    - On a form with a predefined layout, it is possible to extract values from the fields on that form. See related requirements for extracting values in Section 3.2 Capture, Requirement 8, Section 3.5 Indexing Requirement 5, 6, 7, 8, and 9.
34. Automatically extract form data from PDF forms.

4.4 Searching

DIWS 2 shall provide a search capability for searching content in the repository.

The DIWS 2 search capabilities shall:

1. Provide the ability to search using a browser interface.
2. Provide the ability to select search values from a drop down list for all fields that are not free-form text fields.
3. Provide the ability to search using an API.
4. Provide the ability to search using a GUI interface (e.g., dialog box within Microsoft Office).
5. Provide a dialog box for MS Office that allows searches for content in the ECM repository.
6. Provide the ability to search for images/documents based on any index field associated with the image/document.
7. Provide the ability to search for images/documents based on one or more index values for any index fields associated with the image/document.
8. Allow users to perform searches on any combination of metadata tags and values.
9. Provide the ability to perform full text searches on content in the repository.
10. Provide the ability to perform combined index field and full text searches on content in the repository.
11. Provide the ability to perform subsequent searches on the results of the prior search.
    - For the purpose of this requirement, this may be referred to as refined search or refining search results.
12. Provide the ability to perform full text searches independently of metadata searches.

13. Provide the ability to perform full text searches united with metadata searches.
14. Provide the ability to hide images/documents that the user is not allowed to see from appearing in the search results
15. Provide the ability to indicate whether redacted and/or non-redacted versions of an image/document are available in the search results.
16. Provide the ability to limit access to redacted and non-redacted content, listed in the search results, based on the user role.
    a. Redacted versions of a document shall be subject to security roles and rules in a manner similar to the non-redacted content.
    - Redacted versions of documents are likely to be accessible to a broader audience. A user that is not permitted to see an unredacted health record containing PHI, may be allowed to see the same document with the PII information redacted.
17. Provide the ability to show users only those documents they are permitted to know exist in search results.
    a. This requirement, in conjunction with Section 4.4 Searching Requirement 16, shall provide authorized users with the ability to see documents as part of a list of search results where only the redacted versions of the documents appear in the results.
    b. This requirement, in conjunction with Section 4.4 Searching Requirement 16, shall prevent users from seeing unredacted versions of documents as part of a list of search results unless they are authorized to know the unredacted documents exist.
    - Some of these users may or may not be allowed to retrieve, update or delete these documents.
18. Hide (i.e., do not display) the existence of documents in the search results that a user role is not permitted to see.
19. Provide the ability to filter certain fields from the search results, based on a user's authorization to see Sensitive Data.
    a. For the purpose of this requirement, the search results shall exclude field values that are considered to be PII, PHI, or otherwise Sensitive Data for users not authorized to see Sensitive Data.
    - PHI stands for Protected Health Information. PHI is defined on the U.S. Department of Health & Human Services website in the section on HIPAA. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

20. Provide the ability to filter certain images, documents and other content from appearing in the set of results if that content contains Sensitive Data that the user is not permitted to have access.

    a. For the purpose of this requirement, the search results shall exclude those documents that designated as containing PII, PHI, or otherwise Sensitive Data.

21. Provide a configurable upper limit for each role and user that specifies the number of results that will be returned for a search.

    - For the purpose of this requirement, the upper limit associated with the user's role is used if a limit for the user has not been defined. If a limit has been defined for the user, that limit takes precedence over the limit defined for the role.

22. Provide the ability for an administrator to change the configurable upper limit, which specifies the number of results that will be returned for a search, for each role and each user.

23. Provide the ability for the user to specify an upper limit on the number of returned search results, where the limit is less than or equal to the limit associated with the role or user.

    - For the purpose of this requirement, the upper limit specified for the search will be used in place of the limit associated with the role or the user. In cases where a user limit is defined, the lesser of the supplied limit and the user limit is used. If no user limit is defined, the lesser of the supplied limit and the role limit is used.

24. Provide the ability to accept parameters that specify the subset of search results that should be returned.

    - For the purpose of this requirement, "parameters that specify the subset of search results" are two values. One value indicates the where to begin returning results. The second says how many results should be returned. An example of how this works is a query may result in 10,000 content items satisfying the query. The upper limit may have restricted the results to no more than 2,000 content items being identified. The subset of search parameters might result in 100 results being returned each time the query is executed. Further the first execution of the query would ask for results 1-100, the second would ask for results 101-200, and so on.
    - From a practical perspective, this capability is useful when external applications are using the API.

25. Provide the ability to indicate the number of results that satisfied the search parameters and the number of results being returned or presented.

26. Provide the ability to allow successive calls to a search API to return the next batch of results.

27. Provide an application that is configured for performing searching all DIWS 2 document types and content types subject to the security, rendition, redaction and other restrictions described within this TO.
28. Provide the ability to sort search results by any column or combination of columns in either ascending or descending order.
29. Provide the ability to filter search results using any column or combination of columns in a manner similar to the filter capability provided by Microsoft Excel.

4.5 Navigation

DIWS 2 shall provide a navigation capability for navigating through content in the repository.

The DIWS 2 Navigation capabilities shall:

1. Provide the ability for a user to navigate through content that is organized in a folder structure similar to the structure provided by the current version of the Microsoft Windows operating system.
2. Provide the ability to restrict users from seeing documents in a list or folder of documents by hiding the documents.
   - For purposes of this requirement, *restrict users from seeing documents* shall be interpreted as hiding documents and the existence of documents from a user.
3. Provide content transparency from any device where a user can have a continuous experience from multiple devices without losing the continuity in the actions being performed.
   - For the purpose of this requirement, this is similar to the Amazon Kindle eBook approach, where a user can read a book from multiple devices without losing the last page read.
4. Provide an application that is configured for performing navigation of all DIWS 2 document types and content types subject to the security, rendition, redaction and other restrictions described within this TO.

4.6 Redaction

DIWS 2 shall provide the ability to manually and automatically redact information within images, documents and other content and save the redacted versions of this content.

The DIWS 2 redaction capabilities shall:

1. Provide the ability to create saved instructions for performing redaction operations (Redaction Rules) and apply the Redaction Rules to one or more documents.
2. Provide the ability to apply multiple Redaction Rules at the same time to one or more documents.
3. Provide the ability to apply Redaction Rules serially on the same document.
4. Provide the ability to define Redaction Rules based on a form template.
5. Provide the ability to specify in Redaction Rules the color of the redaction (e.g., black, white)
6. Provide the ability to automatically apply redaction rules based on the document type and format of the content at the time the content is captured in DIWS 2.
7. Provide the ability to manually identify a collection of one or more documents and have a set of redaction rules applied to the collection of documents.
   - Redaction does not alter the original document. It always results in a redacted copy being created.
   - Occasionally, a freedom-of-information-act request needs to be processed that may require the same areas on hundreds of scanned documents to be redacted. (See redaction Requirement 17.)
8. Provide the ability to create a redacted version (or versions) of a document.
   - In the context of redaction, a redacted version of a document is the same version number as the underacted version of the content. The redacted version is a type of rendition.
9. Provide the ability to save a manually redacted version of a document in the repository.
10. Provide the ability to save an automatically redacted version of a document in the repository.
11. Provide the ability to create multiple redacted documents for content where each redacted document is associated with a different group of roles.
    - For the purpose of this requirement, a supervisor role may be associated with an unredacted document, a customer-facing role may be associated with a minimally redacted document, and a clerical role may be associated with a fully redacted document.
12. Provide each rendition with its own sets of permissions.
    - From a security perspective, each rendition is treated is treated as a separate document, but remains associated with the document from which it was rendered.

13. Based on user role and user profile, provide the ability to present a redacted version of a document to users not authorized to see the non-redacted version of the document.
14. Provide the ability for an authorized role to override the redacted view of a document and view the non-redacted version of a document by supplying appropriate credentials.
15. Provide the ability to manually redact information on an image based on user role.
16. Provide the ability for the system to identify additional instances of manually redacted content within a document and prompt the user for possible manual redaction.
    - For example, if 123-4506789 is being redacted, the tool should aid in identifying and redacting other instances of this value in the document.
17. Provide the ability to automatically redact information on an image that is located in one or more areas of the image. This shall include creating Redaction Rules for redacting one or more rectangular areas on an image based on the following information:
    a. Page (for multi-page images)
    b. Corner of the rectangle to be redacted
    c. Length and width of the rectangle to be redacted
18. Provide the ability to apply each Redaction Rule to one or more locations on a document or form, including multiple rectangles.

19. Provide the ability to automatically redact human-readable information on an image. This shall include creating redaction rules (Redaction Rules) for redacting one or more of the following types of information:

    a. date of birth
    b. SSNs, TINs, EINs, and TPI numbers
    c. phone numbers (in multiple formats)
    d. zip codes
    e. states
    f. e-mail addresses
    g. VIN numbers
    h. title numbers
    i. driver license numbers
    j. vehicle license plate numbers/letters
    k. names
    l. addresses
    m. photographic images
    n. signatures
    o. medical or disability information
    p. other patterns defined by the business

    For the purpose of redaction:

    - Five digit zip codes are not considered personal information under the Maryland Public Information Act Manual (PIA).
    - VINs are not considered personal information under the PIA.
    - Title numbers are not necessarily considered personal information under the PIA.
    - Vehicle license numbers are not necessarily considered personal information under the PIA.

20. Provide the ability to create redaction profiles for applying a predefined set of automatic redaction rules to content. This shall include one or more of the following content Redaction Rules for redacting the following types of human-readable and machine readable (e.g., barcode) information.

    a. date of birth
    b. SSNs, TINs, EINs and TPI numbers
    c. phone numbers (in multiple formats)
    d. zip codes
    e. states
    f. e-mail addresses
    g. VIN numbers
    h. title numbers
    i. driver license numbers
    j. vehicle license numbers
    k. other patterns defined by the business

21. Provide the ability to automatically redact information on an image that is encoded in non-human readable formats such as barcodes. This shall include one or more of the following content Redaction Rules for redacting the following types of information:

    a. date of birth
    b. SSNs, TINs, EINs, and TPI numbers
    c. phone numbers (in multiple formats)
    d. zip codes
    e. states
    f. e-mail addresses
    g. VIN numbers
    h. title numbers
    i. driver license numbers
    j. vehicle license numbers
    k. other patterns defined by the business

22. Provide the ability to create and save redacted instances of a set of documents redacting the same physical locations in all documents in the collection. (See also Requirement 17.)

    - This requirement demonstrates a lack of awareness of the nature of the information that needs to be redacted, but an awareness that the information must be redacted.
    - For example, redact the same physical locations on a set of similar documents specified by the user.
    - In the paper world, we have a stack of documents that require the same area to be redacted on all documents.

23. Provide the ability to create and save redacted instances of a set of documents redacting the same fields in all documents in the collection.
    - This requirement demonstrates an awareness of the nature of the content, knowing at least the name of the field that must be redacted.
    - For example, redact the fields (e.g., name, address, phone number) on a set of similar documents specified by the user.
24. Ensure there is no way to remove the redaction from a document to expose the underlying content.

4.7 Workflow

DIWS 2 shall provide a workflow engine for implementing business processes involving content and supporting application data.

The DIWS 2 workflow capabilities shall:

1. Provide the ability to automatically notify a user that an image/document has been placed in a document workflow and requires attention.
2. Provide the ability to create workflows using a GUI.
3. Provide the ability to save workflows.
4. Provide the ability to update workflows.
5. Provide the ability to delete workflows.
6. Provide the ability to treat workflow definition files or configuration profiles the same as documents with respect to version control and security.
7. Provide the ability to create workflows containing any combination and any nesting of serial and parallel paths.
8. Provide the ability to create workflows containing time triggers.
    - For example, if action is not taken within 30 days, proceed to a specified document workflow step.
9. Provide the ability to create workflows containing event-trigger paths.
    - For example, if a new version of a document is created, then launch a document workflow or proceed to a specified document workflow step.
10. Provide the ability to electronically sign any workflow step.
11. Provide the ability to utilize signatures in the form of passwords, fingerprint scans, signature pads, and finger signing on mobile devices.
    - See related requirements in Section 4.3 Electronic Forms, Requirements 6-12, and 14.

12. Provide the following types of workflow triggers:
    a. Date (with optional time)
    b. Duration
    c. Workflow inactivity
    d. Failure to complete a workflow step within a period of time
    e. Failure to complete a workflow step by a specified date and time
    f. Failure to complete a workflow within a period of time
    g. Failure to complete a workflow by a specified date and time
13. Provide the ability to use a workflow trigger to:
    a. Automatically send of an e-mail to an individual or group if a document workflow step is not completed by a specified time.
    b. Automatically send of an e-mail to an individual or group if a document workflow step is not completed within a specified duration.
    c. Automatically make certain document workflow steps active or inactive.
    d. Automatically terminate a document workflow step.
    e. Automatically terminate a document workflow.
    f. Automatically transition to another document workflow step.
    g. Automatically transition to another document workflow.
    h. Automatically transition to an external workflow.
14. Provide the ability to seamlessly use XPDL 2.1 or 2.2.
15. Provide the ability to use Wf-XML and OASIS Asynchronous Service Access Protocol (ASAP).
16. Provide the ability to assign a user or a member of a group with responsibility for the actions associated with a workflow step.
17. Provide the ability to delegate responsibility for the actions associated with a workflow step.
18. Provide the ability to automatically trigger a workflow in an external system.
19. Provide the ability to pass along pointers to workflows for content managed by DIWS.

4.8 Reports and Queries

DIWS 2 shall provide the ability to generate reports and queries. For purposes of this requirement, queries are reports that are displayed to the user using the local user interface.

The DIWS 2 report and query capabilities shall:

1. Consider the report and query capabilities specified in this section to be *in addition* to reports and queries specified in other sections of this document.
2. Configure each report to be automatically executed at a configurable period of time.
   - For example, every Tuesday at 8:00 AM, the last day of the month, the last day of the quarter at 5:00 PM, every other Friday at 8:00 PM.
     a. For some reports, the configurable period of time shall be to manually execute the report.
3. Allow all reports to be executed on demand.
4. Provide the ability to designate reports as being executable with one or more of these restrictions:
   a. On demand, real-time during peak hours
   b. On demand, low priority during peak hours
   c. Only off hours
   d. Only as low priority

   - Some reports are likely to place a significant load on the system resources (e.g., database). To minimize the impact of these reports on production operations, they may be limited to off hours or as a low priority during peak hours, or a combination of both.
5. Allow access to report execution to be limited based on user role and security classification.
6. Allow access to query execution to be limited based on user role and security classification.
7. Maintain separate security profiles for each report.
8. Allow each report to be configured in a manner that allows the output of the report to be:
   a. E-mailed to a distribution list
   b. Saved to a local storage area
   c. Sent to a printer or similar device
   d. Saved in the repository as a document
9. Provide 20 parameter-less reports, including other parameter-less-reports explicitly named in the DIWS 2 Appendices 6-8.
   - The underlying query is a based on a SQL query that is not dependent on values supplied by a user when the report is generated.
10. Provide 20 one-parameter reports, including other one-parameter reports explicitly named in the DIWS 2 Appendices 6-8.
    - The underlying query is a based on a SQL query that contains static query values and one value provided by the user when the report is generated.

11. Provide 20 two-parameter reports, including other two-parameter reports explicitly named in the DIWS 2 Appendices 6-8.
    - The underlying query is a based on a SQL query that contains static query values and two values provided by the user when the report is generated.
12. Provide 20 three-or-more-parameter reports, including other three-or-more-parameter reports explicitly named in the DIWS 2 Appendices 6-8.
    - The underlying query is a based on a SQL query that contains static query values and three or more values provided by the user when the report is generated.
13. Provide a comprehensive, parameter-driven, *deleted content and Records report* that provides information on deleted documents.
    - For more information on deleted Records, see Section **4.15 Records Management and Legal Hold**.
    - For more information on deleted scan content, see Sections **3.2 Capture** and **3.4 Quality Assurance**.
    - For more information on deleted content in the repository, see Section **5.1 Repository Management**.
    - There are other requirements to delete content and Records (e.g., Section 3.1 Scanning, Requirement 26). These were included to provide an indication of the scope and breadth of this requirement.
14. Provide the ability for the user to execute any report as a query with the report results displayed to the user.
    - The underlying query is a based on a SQL query that is not dependent on values supplied by a user when the report is generated.
15. Provide the ability to sort query results by any column or combination of columns in either ascending or descending order.
16. Provide the ability to filter query results using any column or combination of columns in a manner similar to the filter capability provided by Microsoft Excel.
17. Provide the ability for the user to create ad hoc queries that are queries written by a user against any data the user is allowed to access.
18. Provide the ability to save queries as easily as documents are saved.
19. Provide the ability to share queries, including ad hoc queries, with other users as easily as documents are shared with other users.
    - For the purpose of this requirement, “share “should be interpreted to mean one user can share an ad hoc query with another user, without having the other user rekeying the query, without requiring an administrator to become involved, and without requiring a developer to become involved.

20. Provide the ability to store the results of reports in the repository.
21. Provide the ability to store the results of queries in the repository.
22. Provide a deleted document report based on date, user and document parameters that identifies all documents that have been deleted, when they were deleted, and the user identifier of the person performing the deletion.
23. Provide an application that is configured for executing all reports and queries within DIWS 2 subject to the security, rendition, redaction and other restrictions described within this TO.

4.9 Administration

DIWS 2 shall provide DIWS 2 administrators with a set of tools and reports that are accessible from the user interface for administering DIWS 2. These tools, user interfaces, and reports shall be available both locally and remotely through all supported devices identified in Section 6.5 Devices.

The DIWS 2 administration capabilities shall:

1. Provide the ability to administer storage, including specifying the volumes that content types are stored in.
   - For the purpose of this requirement, it is considered desirable to store related content on one or more storage volumes assigned to the related content types.
   - For example, all HR content is stored on a set of volumes used exclusively by HR. Similarly all AP content is stored on volumes used exclusively by AP.
2. Provide the ability to store multiple content types on the same storage volumes.
3. Provide the ability to administer scanner profiles for all DIWS scanners that are profile-driven.
4. Provide administrators with the ability to execute a query that indicates the names of all users that have access to a specified document.
   - This requirement may be satisfied by providing the LDAP user identifier for the user.

5. Provide administrators with the ability to administer users and roles.
    a. This shall include adding, suspending, restoring, renaming and removing users.
    b. This shall include adding, suspending, restoring, renaming, removing, adding users to, and removing users from roles.
    c. This shall include designating other users as administrators, including removing administrative privileges.
    d. This shall include specifying the authorizations for other administrators.
6. Provide administrators with the ability to see workflows that are becoming stalled or otherwise inefficient.
    a. DIWS 2 shall provide a query and report on workflows that have not completed that indicates:
        1 for each workflow, the number of times the workflow was executed, the time spent on each workflow, the average time spent on each workflow, the minimum time spent on each workflow, the maximum time spent on each workflow, the standard deviation of the time spent on each workflow, organized by time period, by person, by document, with totals and subtotals.
        2 for each workflow step, the number of times the workflow step was executed, the time spent on each workflow step, the average time spent on each workflow step, the minimum time spent on each workflow step, the maximum time spent on each workflow step, the standard deviation of the time spent on each workflow step, organized by workflow, by time period, by person, by document, with totals and subtotals.
7. Provide administrators with the ability to reassign workflows to other users.
8. Provide authorized users with the ability to designate others as being back in the office.
9. Provide the ability to automatically synchronize DIWS 2 out of the office status with the out of the office status in Microsoft Outlook for configurable user roles.
    - The user's DIWS 2 inbox status should be set to “out of office” based on their Microsoft Outlook “out of office” status and reset when the Microsoft Outlook "out of office" status is reset.
10. Allow administrators to define and alter workflows.
11. Allow each administrative function to be assigned and protected separately from all other administrative functions.
    - 'Protected' mean the same as administered and entitled individually.

12. Provide administrators with the ability to see the productivity of workflows.
    a. DIWS 2 shall provide a historical query and report that indicates the number of times a workflow has been executed, by time period, by person, by document, with totals and subtotals.
13. Provide administrators with the ability to define queries and reports.
14. Provide administrators with the ability to administer access to
    a. Audit trail search functionality
    b. Saving audit trail search results
    c. Forwarding audit trail search results to other users

4.10 Self-Administration

DIWS 2 shall provide authorized users with the ability to perform self-administering actions using the DIWS 2. Actions shall be available both locally and remotely through all supported devices identified in Section 6.5 Devices.

The DIWS 2 administration capabilities shall:

1. Provide authorized users with the ability to designate themselves as out of the office to avoid workflow tasks being assigned to themselves.
2. Provide authorized users with the ability to designate themselves as being back in the office.
3. Provide the ability to automatically synchronize out of the office status with Microsoft Outlook out of the office status for configurable user roles.

4.11 Security and Privacy

DIWS 2 shall provide a secure environment that protects content and functions from unauthorized access, alteration, creation, analysis or destruction. Security shall be based on user roles and security groups. Documents are assigned to security groups which also determine the type of access permitted to the document. One group may be defined for proof of identity documents, and another group may be defined for redacted autonomous vehicle registrations. Operations that are document-independent (e.g., changing a user profile) are also assigned to security groups.

Combinations of users are assigned to user roles. User roles are given access to documents directly and through security groups. For example, a user role may allow members of that role to view unredacted vehicle registration documents. Another user role may allow users to create identity documents.

The **DIWS 2 security and privacy requirements shall:**

1. Encrypt content at rest.
   - For the purpose of this requirement, *content at rest* is considered to be content being stored in the DIWS 2 repository. It also includes information in any database of configuration files used by DIWS 2.
2. Encrypt content in transit.
   - For the purpose of this requirement, *content in transit* is considered to be content being transferred between the user/device/application and the ECM repository and ECM file stores.
3. Encrypt Structured Data at rest.
   - For the purpose of this requirement, *Structured Data at rest* is considered to be metadata or application data that is being stored in a database or in the repository.
4. Encrypt Structured Data in transit.
   - For the purpose of this requirement, *Structured Data in transit* is considered to be metadata or application data between the user/device/application and the repository.
5. Encrypt validation data in transit.
   - When validation data is being transferred between the user/device/application and the validation source.
6. Provide FIPS 140-2, Level 2, compliance.
7. Provide user-role-based security classification for content management operations.
   - Each user role may have a security classification associated with it. This allows restrictions to be placed on the operations that may be performed by users assigned to that role.
8. Provide security-group-based security classification for content.
9. Provide the ability to place none, one, or more, of the following restrictions on content:
   a. Celebrity
   b. PHI
   c. Confidential 1
   d. Confidential 2
   e. Confidential 3
   - The definitions and interpretations of the aforementioned list of restriction titles will be determined during the requirement and design phases. For planning purposes, understand that there are five restrictions that are required to be available for use by DIWS 2 users.

10. Limit access to restricted content to those users that have been explicitly authorized to access content with the designated restriction.
11. Limit access to restricted content to those users that have been explicitly authorized to access content with the designated restriction AND satisfy all other security, privacy and access rules for the content, including:
    a. Preventing users, including administrators and other super users, from overriding the restrictions on content.
    b. Allowing super users to remove restrictions on content
12. Allow for access to documents based on user identifier.
13. Allow for access to documents based on user role.
14. Allow for access to functions and operations based on user identifier.
15. Allow for access to functions and operations based on user role.
16. Provide an unlimited number of configurable user roles.
17. Provide an unlimited number of configurable security groups.
18. Allow new security groups and user roles to be defined based on an enumerated list of permissions and authorizations.
19. Allow new security groups to be defined based on adding or removing permissions to existing security groups.
20. Allow an administrator to determine which security groups have access to any given document.
21. Allow an administrator to determine which user roles have access to any given function or operation.
22. Allow the definition of user groups containing zero, one or more users.
23. Prevent the deletion of user groups containing one or more users.
24. Allow the definition of user group profiles with assigned security roles.
25. Allow for the management of user group profiles.
26. Allow for the management of security groups.
27. Allow security groups to be associated with including or excluding access to documents based on any combination of document metadata values.
28. Allow security groups to be associated with including or excluding access to documents based on one or more document metadata fields.
29. Allow security groups to be associated with including or excluding access to documents based on one or more document metadata field values.
30. Provide for any security group that allows updating, deleting or changing documents, a similar role that is limited to viewing those documents.

31. Provide the ability to prevent users from seeing a document in a list of documents (i.e., be unaware that a document exists).
32. Provide the ability to prevent users from viewing a document.
33. Provide the ability to prevent users from making annotations on a document.
34. Provide the ability to prevent users from updating a document.
    - In the context of this requirement:
      - *Updating* may involve changing a document or a creating or altering a rendition of a document.
      - The user is not creating a version but is updating the document properties or updating the actual document content.
35. Provide the ability to prevent users from creating a new version of a document.
    - In the context of this requirement, *new version* may be a major version, minor version, or other version.
36. Provide the ability to prevent users from deleting a specific version of a document.
37. Provide the ability to protect documents and content types at a level that satisfies MVA PHI requirements.
    a. DIWS 2 does not have Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements, but medical records shall be treated in accordance with PHI rules, guidelines, policies and standards.
    - See TO Section 3.3.1 Required Project Policies, Standards, Guidelines and Methodologies.
38. Provide the ability to protect metadata containing Sensitive Data.
    - For purposes of this requirement, an index field that indexes a document containing information such as HIV status is Sensitive Data.
39. Provide the ability to protect metadata containing PII and other Sensitive Data that MVA has chosen to protect at a higher level than information of a lesser sensitivity.
    - For purposes of this requirement, an index field that contains information such as a social security number is Sensitive Data.

40. Protect rows and columns of non-metadata, Structured Data using encryption and mechanisms that restrict access to those with a business need to access the Structured Data.

    - This Structured Data includes, but is not limited to, data such as the supporting data for Human Resource, Accounts Payable and Procurement applications that is specified in other DIWS 2 TO appendixes.

41. Provide the configurable ability for a user to temporarily adopt the user role and security profile associated with another user by having the other user enter their user identifier and security authorization credentials.

    - For the purpose of this requirement, *temporarily* shall be considered to begin at the time the credentials for the adopted role are entered/provided and terminate when any of the following take place:
        a. The user session is terminated (e.g., logoff or period of inactivity).
        b. The user indicates the adopted role should terminate.
        c. The user enters the credentials for another adopted role.
    - This feature is useful in many situations. For example when a user lacks credentials to perform a task that can be performed by a supervisor.

42. Provide the ability for all APIs, web services, and other interfaces that perform functionality for which security permissions are required, to allow that functionality or command to be executed by a service machine but with the security groups of a user with lesser or fewer permissions and authorizations.

        a. Based on a configuration parameter, transactions shall be logged, including the all information typically logged in an audit trail and the groups and permissions.

    - For the purpose of this requirement, this capability allows a service machine with super user authorization to execute all commands for all users. The service machine would accept the user identifier passed along with the command and assume the security limitations associated with that command for the duration of the command.
    - For the purpose of this requirement, the user password would not need to be supplied with the user identifier because communications with the service machine would be considered secure.

4.12 Audit Trail

DIWS 2 shall maintain an audit trail that captures access to the system, peripherals, interfaces, functionality and content. The information that is captured shall allow unambiguous details related to the user or system that initiated/requested an activity, the

time and date the activity took place, and sufficient information to determine the functionality, peripherals and content involved in the access. For purposes of the requirements in this section, "access" shall also include attempted access in the event access was either partially or fully denied.

The DIWS 2 audit trail requirements shall:

1. Capture all user access to the CMS in an audit trail, including Web interface, client interfaces, and API usage.
2. Capture all user access to content in the CMS in an audit trail.
3. Capture all user access to the capture functionality in an audit trail.
4. Capture all user access to content (e.g., scanning and indexing) in the capture functionality in an audit trail.
5. Maintain a seamless audit trail and provide the ability to present that seamless audit trail from the point at which the document was initially captured (e.g., scanned) and continuing through the life of the document.
6. Provide a means of periodically archiving all or part of the audit trail for the capture functionality.
7. Provide a means of periodically archiving all or part of the audit trail for the CMS.
8. Capture all machine access (e.g.., non-user interface access) to the CMS in an audit trail.
9. Capture the date, time, user identifier, type of access, and source of access, (the IP address and the MAC address of the device initiating the transaction) for all audit trail entries.
10. Capture the information that was changed for all audit trail entries, including the data values of the information before and after it was changed, and the data source if the change was system generated.
11. Capture a unique document identifier for all retrieval, update, deletion, transfer from a capture subsystem, versioning, renaming, and storage access for all documents.
12. Capture the details on all administrative operations performed.
    - See Section **4.9 Administration** for more information on audit-related operations.
13. Capture the details on all Records management operations performed.
    - See Section **4.15 Records Management and Legal Hold** for more information on audit-related operations.

14. Capture the details on all auditing operations performed.
    - See Section **4.14 General Auditing and QA Auditing** for more information on auditing-related operations.
15. Capture sufficient information in the audit trail record to be able to definitively identify the action, including parameters of the action, which took place.
16. Provide a mechanism for archiving audit trail information as the audit trail logs grow over time.
    a. The system shall be sized to allow ten (10) years of audit trails to be maintained before archiving.
    b. The archiving shall be configurable to take place based on the audit trail logs reaching a specified size.
    c. The archiving shall be configurable to take place based on the audit trail entries reaching a specified age.
17. Provide a mechanism for retrieving all audit trail information related to an object from an audit trail log and audit trail archives and presenting these in a seamless manner to the user.
18. Provide a mechanism for retrieving all audit trail information related to a user from an audit trail log and audit trail archives and presenting these in a seamless manner to the user.
    - For the purpose of this requirement, *user* is the user identifier for person-initiated actions and the system identifier for system initiated actions.
19. Provide a mechanism for retrieving all audit trail information related to a device name, the IP address, or MAC id from an audit trail log and audit trail archives and presenting these in a seamless manner to the user.
    - Some devices may not have device names. Searching on an IP address is likely to be useful only if a date range or time range is also specified.
20. Provide a means of limiting retrieved audit trail information for an object, device name, the IP address, or MAC id or user to a date range.
21. Be able to generate custom reports based on audit trail information.
22. Maintain an audit trail of all scan operations.
23. Maintain an audit trail of all operations involving any content that is captured by DIWS 2, including but not limited to, using the interfaces identified in Section 3.2 Capture, Requirement 20.
24. Maintain an audit trail of all indexing operations.
25. Maintain an audit trail of all quality control (e.g., rotation, de-speckle) operations.

26. Maintain an audit trail of all rendering operations.
27. Maintain an audit trail of all content transfer (e.g., import, export, exchange with subsystems or external systems) operations.
28. Maintain an audit trail of all content retrieval or manipulation operations.
29. Maintain an audit trail of the creation of any document.
30. Maintain an audit trail of each save of any document.
31. Maintain an audit trail of each edit of any document.
32. Maintain an audit trail of each workflow operation on any document where workflow operations are identified in Section 4.7 Workflow.
33. Maintain an audit trail of each approval of any document.
34. Maintain an audit trail of each publication of any document, where publishing operations are identified in Section 5.4 Publishing.
35. Maintain an audit trail of each assembly of any document where assembly operations are identified in Section 5.3 Document Assembly.
36. Maintain an audit trail of the deletion of any document.
37. Maintain an audit trail of attempts to perform any action for which there is an audit trail if that attempt was unsuccessful.
    - For example, a user attempting to delete a document would result in an audit trail entry, even when that attempt did not result in the deletion of the document.
38. Provide authorized users with the ability to:
    a. Access audit trail search functionality
    b. Save audit trail search results
    c. Forward audit trail search results to other users
39. Provide audit trail search functionality that allows all information saved in the audit trail to be searched:
    a. By date range
    b. By time range (e.g., 8:00 AM – 5:00 PM any day)
    c. By auditable action (e.g., unsuccessful deletion, successful creation)
    d. By person attempting or performing the action
    e. By document or document family

4.13 Journaling

For the journaling requirements, **DIWS 2 shall**:

1. Provide the ability for authorized administrators to enable or disable journaling, where journaling is defined as the automatic capturing, in a database, all changes made to application-related database tables.
   - For the purpose of this requirement, changes may be initiated directly by a user action or indirectly by a trigger or other mechanism.
   - For the purpose of the requirements in Section 4.13 Journaling, Journal tables are just another table within the database so they are able to grow as needed and are really only limited to the size of the associated tablespace. Journaling is typically accomplished by creating one or more triggers on the underlying tables. When a record in the underlying table is updated/deleted the data is written to the journal table. The journal tables are part of the system's auditing capabilities. Journal tables are used to in a variety of ways that include supporting reporting capabilities, supporting troubleshooting activities, and accurately responding to Legislative requests.
2. Provide a mechanism for automatically capturing all changes to all application-related tables, including the operation, timestamp, user identifier initiating the change, and the new values.
   - For the purpose of this requirement, a change is considered and insertion, update or deletion to any table row or part of a row.
   - For the purpose of this requirement, an operation is considered and insertion, update or deletion to any table row or part of a row.
   - For the purpose of this requirement, the timestamp includes the date and time the change took place.
   - For the purpose of this requirement, the new values are the values inserted, updated or deleted from the table.
3. Shall satisfy all performance and throughput requirements with journaling enabled.
4. Shall provide a mechanism to administer the space used by the journal tables.

4.14 General Auditing and QA Auditing

Auditing takes place in two forms:

- General auditing (“General Audits”) – often performed by legislative, MDOT, MVA, Federal and other oversight entities. The auditor performing these type of audits is referred to as the General Auditor.

- QA audits – typically performed within MVA by supervisors following up on employees.

The auditing requirements are organized into three categories:

- those requirements that are common to both General Audits and QA auditing
- those requirements that are unique to General Audits
- those requirements that are unique to QA auditing

For the common auditing requirements, **DIWS 2 shall**:

1. Define an MVA Audit Administrator who is allowed or restricted to defining audits for any combination of:
    a. General Audits
    b. QA Audits
2. Provide users that are assigned the MVA Audit Administrator role the ability to define an audit that is to be performed and an expiration date for the audit.
3. Provide users that are assigned the MVA Audit Administrator role the ability to change the expiration date for an audit.
4. Provide the ability to assign documents to an audit based on:
    a. Manual selection of documents
    b. Manual selection of cases
    c. Selection of a percentage of documents based on one or more index field values
5. Allow a case or document to be subject to multiple audits and provide the ability to maintain multiple audit status values for each case and document.
6. Allow all documents and cases associated with the audit to have auditor defined status values associated with the documents.
7. Provide a default set out audit status values that are available to the auditor, including:
    a. Selected
    b. Not started
    c. In progress
    d. Complete
    e. No audit performed
    f. Pending further investigation
8. Assign those cases selected for audit an audit status of "selected".
    - Note that this applies to cases, not the document in the cases.

9. Set the document audit status to "not started" for all documents within a case that are subject to an audit when a *case* has been identified for audit.
10. Set the document audit status to "not started" when a document has been identified for audit.
11. Change a case's audit status to "in progress" for audits once:
    a. An auditor begins examining documents within the case.
    b. The audit value of any document in the case being audited has been changed from "selected".
12. Upon examining a document, the auditor shall be provided the ability to assign the following audit status value to each document:
    a. Passed
    b. Failed
    c. Revisit
    d. Indeterminate
    e. Second Opinion Requested
    f. Not applicable
13. Once all documents subject to audit within a case have been assigned an audit value of passed, failed, or not applicable, the audit status of the case is marked "Complete".
14. Provide the ability to determine all cases and documents that have a specific audit status value, subject to date, case, auditor, and document filters.
15. Provide the ability to determine all the audit status values for all documents and cases associated with a specific audit that was or is being performed, subject to date, case, auditor, and document filters.
16. Provide the ability to export the list of all documents, and their audit status values, associated with an audit.
    - Note this is expected to leverage the External System integration capabilities identified in Appendix 10.
17. Provide the ability to capture multiple audit status values for all documents selected for audit.
    - Recognize that documents can be subject to multiple audits.
    - For the purpose of this requirement, the audit status value is meaningful when it can be associated with a specific audit that was or is being performed.
18. Allow an auditor to work on multiple cases at a time.

19. Allow audit roles to be defined that authorize auditors to have access to:
    a. Families of documents defined by combinations of one or more index field values.
    b. Families of cases defined by combinations of one or more index field values.
20. Ensure audit roles have read-only access, lacking the ability to modify, create, or alter, documents, cases or the index field values associated with documents and cases.
21. Only allow an auditor to perform audits on documents and cases where the auditor's role is authorized to perform audits on that family of documents and family of cases.
22. Allow an auditor to save work at any time.
23. Maintain audit trail information for all content accessed by an auditor in a manner consistent with Section **4.12 Audit Trail**.

For the General Audit requirements, **DIWS 2 shall**:

24. Provide the ability to allow an external system to mark cases for QA audit.
    - Note this is expected to leverage the External System integration capabilities identified in Appendix 10.
25. Provide the ability to integrate with MVA's external auditing system, Thomson Reuters AutoAudit®, and associated software for the purpose of performing internal audits.
26. Assign those cases selected for a QA audit an audit status of "QA".
27. Accept a file identifying the criteria for auditing one or more documents.
28. Assign those documents selected for a QA audit an audit status of "QA".
29. The file containing the identifying criteria for one or more documents can specify any combination of:
    a. Document type(s)
    b. Document index field(s)
    c. Meta data (indexing values)
30. Provide the ability to export all documents on the list of all documents associated with an audit.
    - Note this is expected to leverage the External System integration capabilities identified in Appendix 10.
31. Provide the ability to export an assembly of documents for audit.
    - Note this is expected to leverage the External System integration capabilities identified in Appendix 10.

32. Provide the ability to import a list of one or more audit status values associated with documents and cases that have been externally audited.
    - Note this is expected to leverage the External System integration capabilities identified in Appendix 10.
33. Provide the ability to update the audit status values in DIWS 2 using and import a list of audit status values associated with documents and cases that have been externally audited.
    - Note this is expected to leverage the external system integration capabilities identified in Appendix 10.
34. All changes to the cases or documents that are part of a General Audit can only be changed by an MVA audit administrator.
    - This requirement should be interpreted to mean that the MVA audit administrator role is authorized to add or remove cases and documents to the scope of the general audit. It should not be interpreted to mean that the content of the documents are being changed.
    - All General Audit cases should have an expiration or closure date because they have a specific purpose and that purpose should last for a defined period of time. Whereas, QA audits (performed by the MVA) may remain open indefinitely because they are tied to the daily work stream.

For the QA auditing requirements, **DIWS 2 shall**:

35. Provide the ability to identify families of cases for audit, where a "family of cases" are those cases associated with a workflow or transaction and further limited by a date range and group of workers.
    - For example, all ETR cases worked on Monday by workers assigned to last names beginning with the letters J-K-L.

36. Provide the ability to identify a pool of potential cases for audit within a family of cases using any combination of:

    a. a configurable interval specified in a positive integer of days
    b. statistical techniques, where statistically identified cases are cases that are stochastically selected
    c. a configurable percentage applied over a configurable period of time, where the percentages are configurable to two decimal points of precision for each family of cases and range from 0.00% to 100.00%

    For the purpose of this requirement:

    - An example is 3% of all vehicle title cases closed on a business day are subject to audit.

37. Provide the ability to include or exclude cases being considered for audit based on the configuration parameter of whether the case was closed manually, automatically or both.

38. Provide the ability to specify those document types within a case that are subject to review.

39. Provide auditors with a user interface that allows them to specify the audit role they are performing.

40. Provide auditors with a user interface that presents a work queue, which represents the total population of cases that they are able to audit within the audit role they are performing.

    - Since multiple auditors may be assigned to an audit role, it is possible that multiple people will be working on the total population of cases.

41. Provide auditors with a user interface that allows cases to be filtered based on the audit status, date range, auditor, and other index fields associated with the audit, case or document.

42. When an auditor selects a case to begin/continue auditing, display documents associated with that case that are subject to audit.

43. Present each document satisfying the family of cases, case and document type criteria to an auditor for examination.

44. Allow the auditor to view the documents and associated document index fields within a case that are not subject to audit if the case is still open for audit.

45. Allow the auditor to mark a document for audit that:

    a. Does not belong to a case
    b. Belongs to a case, but the case has not been identified for audit

4.15 Records Management and Legal Hold

DIWS 2 shall provide Records retention, Records management and Records planning. All Records within DIWS shall be assigned a Records retention classification. A Record shall be defined as "something that represents proof of existence and that can be used to recreate or prove state of existence, regardless of medium or characteristics. A Record is either created or received by an organization in pursuance of or in compliance with legal obligations, or in the transaction of business.[1] Records can be either tangible objects, such as paper documents like birth certificates, driver's licenses, and physical medical x-rays, or digital information, such as electronic office documents, data in application databases, web site content, and electronic mail (email)."

For the Records management requirements, **DIWS 2 shall**:

1. Allow a user to designate each document, of which some documents are images, or collection of documents as a record or non-record.
2. Allow a user to create, update and remove record schedules, which can be measured in any of the following durations:
    a. Days
    b. Weeks
    c. Months
    d. Years
    e. End of current quarter
    f. End of current year
    g. End of next quarter
    h. End of next year
3. Allow users to assign each Record to the applicable Records schedule.
4. Allow the automatic determination of a record based on document type. This determination includes:
    a. Whether a document is a record
    b. Whether a document is a non-record
    c. The assignment a record to the default Records schedule associated with the document type for the initial version of a document
    d. The assignment a record to the Records schedule associated with prior versions of a document
5. Allow the automatic assignment of Records to the applicable Records schedule based on document type.

[1] ARMA International. "Glossary of Records and Information Management Terms, 3rd Edition". ARMA International. Retrieved September 2013.

6. Allow record retention rules to be suspended for content that has been identified as pending manual review.
   - The intent of this requirement is to allow users in an external system to have an opportunity to review content that was captured electronically (e.g., by fax or e-mail) and to be able to remove Records (e.g., menus, vacation advertisements, inappropriate content, and spam) that should not be retained in the repository.
7. Allow authorized users to correct mistakes made in assigning Records to a record schedule.
8. Allow users to indicate whether a record is closed.
9. Identify the final disposition date, which is calculated from the date of closure.
10. Allow for the separation and removal of Records and non-Records for destruction.
11. Allow Records to be placed under one or more legal holds, each legal hold being distinguishable from another.
12. Automatically suspend record retention rules when content is placed under legal hold.
    a. For the purpose of this requirement, a document under legal hold shall not be deleted for any reason, including the automatic purging of documents related to Records retention.
13. Prevent Records placed under one or more legal holds from being deleted until all legal holds have been removed.
14. Allow one or more legal holds to be removed from Records.
15. Allow non-Records to be placed under one or more legal holds.
16. Prevent non-Records placed under one or more legal holds from being deleted until the all legal holds have been removed.
17. Allow one or more legal holds to be removed from non-Records.
18. Prevent Records and non-Records that are pending manual review from being placed under legal hold until the manual review is complete and the result of the manual review does not call for the removal of the record or non-record.
    - The intent of this requirement is to allow users in an external system to have an opportunity to review content that was captured electronically (e.g., by fax or e-mail) to be able to remove Records (e.g., menus, vacation advertisements, inappropriate content, and spam) that should not be retained in the repository.

19. Ensure that Records authorized for destruction are deleted in accordance with approved Records schedules and are not recoverable following their deletion.

20. Provide the ability to configure the deletion process for certain content types to immediately hide the content followed by the physical removal of the content after a configurable number of days. This type of deletion is referred to as a logical deletion or marked for deletion.

    - For the purpose of this requirement, "to immediately hide content" should result in the content not appearing for any user, except for a user that is a member of a role that is authorized to see deleted content.
    - For the purpose of this requirement, "the physical removal of the content" is the traditional deletion of content from the repository.

21. Provide users that are members of the role that is authorized to see deleted content with the ability to see this content in searches and to retrieve this content.

22. Provide users that are members of the role that is authorized to see deleted content with the ability to restore this content.

    - For the purpose of this requirement, "restore this content" means effectively undeleting the content. The content, its document type and metadata is restored to the state that existed before the content was deleted.

23. Provide the ability for users that are members of the role that is authorized to see deleted content to immediately perform the physical removal of the content that is marked for deletion.

    - For the purpose of this requirement, "the physical removal of the content" is the traditional deletion of content from the repository.
    - For the purpose of this requirement, content placed under legal hold shall not be deleted for any reason, including the automatic removal of Records related to a Records schedule.

24. Maintain the integrity of Records.

    a. Records shall be protected from alteration, damage or destruction, whether intentional or unintentional.
    b. The metadata and audit trails associated with Records shall be protected from alteration, damage or destruction, whether intentional or unintentional.
    c. Records shall remain usable.

25. Prevent unauthorized alteration or erasure of the Records.

26. Allow only authorized personnel access to the Records in the system.

27. Allow only authorized personnel to perform administrative operations on Records.

28. Allow Record schedule durations to be measured in days, weeks, months or years.

29. Allow for the automatic destruction of any content item that has not been designated as a record or non-record.

    - For the purpose of this requirement, an example would be content that was provided by an external user that was not approved by the MVA within a prescribed timeframe. This is one approach for reducing the likelihood that inappropriate content might slide into the repository.

30. Allow for the automatic destruction of certain Records that have not been assigned to a Records schedule.

    - For the purpose of this requirement, an example would be content that was provided by an external user that was not approved by the MVA within a prescribed timeframe. This is one approach for reducing the likelihood that inappropriate content might slide into the repository.

5. ECM Advanced Requirements

The ECM system also contains functionality that is likely to be exclusively outside the capture functionality. This advanced functionality allows content to be managed and manipulated and includes:

- Repository Management
- Retrieval
- Document Assembly
- Publishing
- Correspondence Management
- Printing
- Correspondence Tracking

5.1 Repository Management

DIWS 2 shall provide a repository where all unstructured content shall be stored and managed within the ECM system. For the repository capabilities, **DIWS 2 shall**:

1. Provide the ability to manage multiple content types.
2. Provide the ability to manage multiple content subtypes, where the content subtype inherits the properties of a parent content type or parent content subtype.
3. Provide the ability to nest an unlimited number of content subtypes.
   - There is no intention to limit the number of levels of nesting or the number of subtypes at any level.
   - Subtype values are required to be unique only when the subtypes share the same parent. This does not apply to grandparents or more distant relationships.
4. Provide the ability to manage a minimum of 4,000 unique content types.
   - For the purpose of this requirement, the 4,000 unique content types includes all levels of content subtypes.
5. Provide the ability to support a common set of index fields required for all documents.
6. Provide the ability to support content types inheriting the index fields required for all documents.
7. Provide the ability to support a set of index fields required for all documents of a particular content type.

8. Provide the ability to support a set of index fields that are optional for all documents of a particular content type.
9. Provide the ability to support a set of index fields that are a combination of required and optional for all documents of a particular content type.
10. Provide the ability to support content subtypes inheriting the index fields of the parent content type.
11. Provide the ability to include one or more index fields where it is required that the value be provided in that index field(s) for any documents of a particular content subtype.
12. Provide the ability to include one or more index fields where it is optional that a value be provided in that index field(s) for any documents of a particular content subtype.
13. Provide the ability to support content subtypes inheriting the index fields of the parent content subtype.
14. Provide the ability to enforce the rule that any index field where it is required that the value be provided in that index field(s) for a content type shall be required for all levels of the content subtypes.
15. Provide the ability to support enforcing the rule that any field that is optional for a content type shall be either optional or required for all levels of content subtypes.
    - Example: A content type named *case document* is defined as having two index fields: *case number* that is required and *case origination date* that is optional. This means that all subtypes must have *case number* as a required index fields. This also means that all subtypes must have *case origination date* as either a required index field or as an optional index field.
    - A content subtype named *vehicle case document* is created from *case document* content type, *vehicle case document* must inherit the two index fields that are defined in the *case document* content type. However, *vehicle case document* can also require another mandatory index field named *VIN*.
    - A second content subtype named *driver case document* is created from the *case document* content type, *driver case document* must inherit the two index fields that are defined in the *case document* content type. However, the *driver case document* can also require that the *case origination date* index field is mandatory and includes another mandatory index field named *person identifier*.

16. Provide the ability to release captured documents into the main repository.
    - See Section 3.6 Release for additional requirements on releasing captured documents.
17. Provide the ability to save all captured documents into a repository.
18. Provide the ability to store a document in the repository using a Web-based GUI.
19. Provide the ability to store a document in the repository using an API.
20. Provide only authorized users with the ability to store a document.
21. Provide the ability to update a document in the repository using a Web-based GUI.
22. Provide the ability to update a document in the repository using an API.
23. Provide only authorized users with the ability to update a document.
24. Provide the ability to delete a document in the repository using a Web-based GUI.
25. Provide the ability to delete a document in the repository using an API.
26. Provide only authorized users with the ability to delete a document.
27. Provide the ability to manage documents in a repository. Manage is defined as store, retrieve, update, and delete.
28. Provide the ability to manage documents of any format.
    - Examples of some of the many formats are Microsoft Office formats, image formats, audio formats, and video formats.
29. Provide the ability to provide version control on all managed documents.
30. Provide the ability to provide multiple version trees for all version controlled documents.
    - A version tree is a data structure in which each version is attached to one or more versions directly beneath it. Normally, we have version 1, 2, 3, 4, 5, etc. However, the version tree may split at a version where the paths from that point are different. For example, after version 3, two authors may use version 3 for very different purposes and continued to version their documents independent of each other. Tends to be a common feature in ECM systems.
31. Allow content of unlimited size to be stored in the repository.

32. Provide the ability to manage non-resident content using the repository.
    - For the purpose of this requirement, *nonresident content* refers to content that is stored outside for the repository (e.g., paper documents) and the location is a physical location or contact rather than an electronic storage location.
33. Allow the contents of the repository to be partitioned on physical storage by business area.
34. Allow the application-specific content to be segregated from other content in the database.
35. Provide the ability to manage a collection of one or more templates for each content type.
36. Provide the ability for a document to be *checked out* to allow one user to perform updates and edits to the document.
37. Provide the ability for a document to be *checked in* to allow a user to:
    - save updates and edits to a document
    - allow the saved changes available to other users
    - make the document available to other users to check out to make their updates and edits
38. Provide the ability for a user to save changes made to a document that is checked out and keep the document checked out.
39. Provide the ability for a user to check in a document and abandon any changes made to the document.
    - This is sometimes referred to as abandoning the reservation.
40. Provide the ability for an administrator to check in a document on behalf of another user.
    - All changes made to the document will be lost.
41. Provide the ability to request an e-mail notification when a checked out document is checked in.
42. Provide the ability to automatically send e-mail notifications to users who have requested a notification when a checked out document is checked in.
43. Scan all content for malware using MVA designated tools prior to the content being saved, updated or otherwise modified in the DIWS repository.

5.2 Retrieval

DIWS 2 shall provide an image, document and content retrieval capability for retrieving content that is stored or managed in the repository.

For the retrieval capabilities, **DIWS 2 shall**:

1. Provide the ability to allow only authorized uses to retrieve a document.
2. Provide the ability to retrieve a document in the repository using a Web-based GUI.
3. Provide the ability to retrieve a document in the repository using an API.
4. Provide the ability to retrieve all related images when a multi-page scanned document is stored as a set of single page image files.
5. Provide the ability to retrieve the latest checked in version of a document through use of a link or URL.
6. Provide the ability to retrieve a specific version of a document through use of a link or URL.
7. Provide the ability to retrieve a Redaction Rendition of a document based on user role.
    - For the purpose of this requirement, certain users may see a redacted PDF. An example is clerk may see a redacted rendition of a document that contained Sensitive Data that they were not authorized or cleared to see.
8. Provide the ability to present a retrieved document by launching a document viewing tool, when the retrieval is intended for viewing.
9. Provide the ability to present a retrieved document by launching a document editing tool, when the retrieval is intended for editing.
10. Provide the ability to present a retrieved document by using the browser.
11. Provide the ability to automatically decrypt an encrypted file using decryption key or password saved in the metadata or elsewhere.
    - For the purpose of this requirement, “an encrypted file” refers to a file that was received as an encrypted file and a decryption key or password provided and saved with the file.
    - A typical example would be retrieving an encrypted document that was sent by an external user. The original document and the decryption information are retained for evidentiary purposes. Once inside MVA, there would be no reason to retain the user supplied encrypted file other than for evidentiary purposes.
12. Provide PDF linearization for faster viewing of PDF files.
    - PDF linearization is sometimes referred to as “Fast Web View”.
13. Provide the ability to view TIFF images as they are downloaded to the browser without having to wait for the download to complete.
    - This capability is similar to PDF linearization.

14. Be configurable to present e-mails with an abbreviated header or with the full header information.
    - An abbreviated header would look like the header the user sees in Microsoft Outlook. The full header includes the hidden fields (e.g., IP addresses).
15. Provide the ability to retrieve a document as a file.
    - This could be used by an external application that requests a document be returned as a file. The external application may have instructed DIWS as to where the file should be placed or DIWS may need to provide the external program with a URL to the location where the file was placed.
16. Provide the ability to retrieve a document as a pointer to a block of memory.
    - This could be used by an external application that requests a document be left in memory and a pointer to the content be returned to the external application.
17. Provide the authorized user with the ability to access the version tree for a document containing those document versions that they are authorized to view.
    - For the purpose of this requirement, "access" shall include retrieval (in all of it forms) and viewing (on all devices).
18. Provide the authorized user with the ability to access any version of a document that appears in a version tree.
    - For the purpose of this requirement, "access" shall include retrieval (in all of it forms) and viewing (on all devices).
19. Provide the ability to designate specific content as being accessible to everyone within the enterprise without presenting credentials.
    - An example of this content would be the daily newsletter.
20. Provide the ability to designate specific content as being accessible to anyone without presenting credentials.
    - An example of this content would be the content in the public domain such as directions to the facility or the hours of operation.

21. When multiple versions of a content exist and the user has not specified a version to retrieve or view, retrieve the version:
    a. that is the most recent version of the content, when the most recent version of the content is *not* checked out
    b. that is the most recent version of the content that is *not* checked out, when the most recent version of the content *is* checked out *and* the person requesting the content is not the person that has the content checked out
    c. that is the most recent version of the content, when the most recent version of the content *is* checked out and the person requesting the content *is* the person that has the content checked out
22. When multiple versions of content exist and the user has not specified a version to retrieve or view, retrieve the version of the content that is checked out if the retrieval request is made by the person that has the content checked out.
23. Provide the ability to specify one or more or all content formats for content retrieval, retrieving all of the specified formats that are available.
    - For the purpose of this requirement, retrieving multiple formats of the same content is important. It may necessary to retrieve a PDF file and a TIFF file if both are available.
24. Provide the ability to specify one or more content formats in order of preference for content retrieval, retrieving the first specified format that is available.
    - For the purpose of this requirement, the format of the content is important. It may be preferable to retrieve a PDF file, but if a PDF file is not available, a TIFF file would be acceptable.
25. Provide the ability to specify a thumbnail at a designated resolution for content retrieval.
    - The approach for satisfying this requirement may take many forms and it may be necessary to satisfy it in multiple ways. For example, it may be determined that it is necessary to store thumbnail renditions for some document types. In other instances, it may be practical to create a thumbnail rendition on the server. It may also be reasonable to provide a utility to create a thumbnail at the browser or on the other side of an external interface.
26. Provide an application that is configured for performing content retrieval for all DIWS 2 document types and content types, subject to the security, renditions, redactions, specified formats, and other restrictions defined within this TO.

27. Provide one or more applications that are configured for asynchronously retrieving content using smartphones and tablets when working remotely and at client/customer locations and for locally caching this content on the smartphone or tablet to be available for immediate use or later use.

    For the purpose of this requirement:

    a. It is often necessary to travel to an external site and use a smartphone or tablet to retrieve and view documents and images of people, equipment and facilities. It shall be possible to search for content and to retrieve content from DIWS 2 using communications capabilities built into the device.
    b. The application shall be smart enough to know when a communications signal is available to begin retrieving the content and to continually retry communications until all retrievals are successful.
    c. Due to the unpredictable nature of communications in the rural parts of the State, the requests shall be able to be made asynchronously relative to the retrievals. There may be 100 or more retrievals requested in the morning with the actual retrievals taking place throughout the day for later viewing.

5.3 Document Assembly

DIWS 2 shall provide the ability to assemble images, documents and other content into a document referred to as a saved assembly of documents. The instructions used to build the saved assembly of documents are called the document assembly instructions. As indicated by the requirements in this section, both the document assembly instructions and the resulting saved assembly of documents have many of the same characteristics that documents have.

For the document assembly capabilities, **DIWS 2 shall:**

1. Provide the ability to relate and assemble any number of single-page images, multi-page images, single page documents and multi-page documents into one document known as a "saved assembly of documents".
2. Provide the ability to include a "saved assembly of documents" into one or more "saved assembly(s) of documents".
3. Provide the ability to query all of the "saved assembly of documents" that an image or document is used in.
4. Provide the ability to save the machine executable instructions for assembling documents in a document known as “document assembly instructions”.
5. Provide the ability to create document assembly instructions.
6. Provide the ability to share document assembly instructions.

7. Provide the ability to modify previously saved document assembly instructions.
8. Provide the ability to delete previously saved document assembly instructions.
9. Provide the ability to apply version control to a saved assembly documents.
10. Provide the ability to save the document assembly instructions for future retrieval, editing and execution with version control.
11. Provide the ability to specify whether a specific version or the latest version of a document will be used in a document assembly.
12. Provide the ability to execute previously saved document assembly instructions and save the resulting assembled document in the repository.
13. Provide the ability to specify the order of the assembled documents in a saved assembly of documents.
14. Provide the ability to incorporate metadata into a document assembly.
15. Provide the ability to incorporate metadata as barcodes and other machine-readable formats into a document assembly.
16. Provide the ability to include an electronic signature into any document at a configurable location on the document.
17. Provide a configurable option to either include electronic signatures as a layer or integrated into an image or document.

5.4 Publishing

DIWS 2 shall provide the ability to publish images, documents and content to external interfaces and media in a variety of formats.

For the publishing capabilities, **DIWS 2 shall:**

1. Provide the ability to automatically publish documents to any external media, including:
    a. CDs
    b. DVDs
    c. Blu-ray
    d. Any attached storage.

    - This requirement only applies to those devices that have CDs, DVDs, etc., mounted locally or accessible on the network.

2. Provide the ability to publish across media when the size of the content exceeds the storage available on the media.
   - For example, 10 GB of documents may need to be written across three DVDs.
3. Provide the ability to publish documents in those formats identified in:
   - Section 4.1 Content Creation, Requirement 13
   - Section 4.1 Content Creation, Requirement 14
   - Section 4.1 Content Creation, Requirement 15
   - Section 4.1 Content Creation, Requirement 16
   - Section 4.1 Content Creation, Requirement 17.
4. Provide the ability to automatically publish documents to multiple formats and media with consistent index field values.
   - For the purpose of this requirement, example of consistent index field values are the document name, time and date. The expectation is that documents that differ only in format should have consistent index field values.
5. Provide the ability to manually save published documents in the repository for future retrieval.
6. Provide the ability to automatically save published documents in the repository for future retrieval.
7. Provide the ability to render an assembled document, as defined in Section 5.3 Document Assembly, to the following formats:
   a. PDF formats
   b. HTML formats
   c. XML formats
8. Provide the ability to render an image to
   a. PDF
   b. TIFF
   c. JPEG

5.5 Correspondence Management

DIWS 2 shall provide the ability to generate, manage, and deliver correspondence that incorporates data into correspondence templates. Correspondence templates are document templates used for generating correspondence.

For the correspondence management capabilities, **DIWS 2 shall:**

1. Provide the ability to manage a collection of templates for correspondence. These are called correspondence templates.
2. Provide the ability to merge data with a correspondence template.
   - For example, names, business names, addresses, VIN numbers, license information, metadata, and other data.
3. Provide the ability to merge barcode and QR code™ data with a correspondence template so that the barcode can be scanned from a printed copy of the correspondence.
   - Examples of possible barcode data include names, business names, addresses, VIN numbers, license information, metadata, and other data.
4. Provide the ability to save and index a correspondence template that has been merged with data.
5. Provide the ability to associate correspondence with a:
   a. driver (or driver license) as identified in Project Core, or
   b. vehicle as identified in Project Core.
   - The mechanism for associating correspondence with a driver or vehicle will need to be worked decided in the future. The association is likely to be based on one or more values in an index field. The values in the index field are likely going to be obtained from a barcode sheet that accompanies the correspondence or a barcode that is entered on the correspondence. However it is possible that some other mechanism such as manual entry at the time of indexing will take place.
6. Provide the ability to print correspondence with an appropriate envelope for mailing.
7. Provide the ability to automatically fax correspondence when selected by user.
   - Appropriateness is determined by the user or business index field values, nature of the correspondence and other factors.
8. Provide the ability to automatically e-mail correspondence when indicated by the user or business index field values, nature of the correspondence and other factors.
   - Appropriateness is determined by the user or business index field values, nature of the correspondence and other factors.

5.6 Printing

DIWS 2 shall provide the ability to print images, document and other content.

For the printing capabilities, **DIWS 2 shall:**

1. For a configurable list of documents or content types, record who the document was printed for when documents are printed on behalf of someone else or for someone else.
    - For example, in the Appeals area, documents are printed for the defendant or defendant's attorney (as well as the judge and AG's office).
2. Provide the ability to print mailing labels containing information (e.g., addresses or docket numbers) automatically extracted from a document (e.g., correspondence).
3. Record the identifier of the mailing address for documents that will have a mailing label attached.
4. Capture the following information as part of the audit trail (see Section 4.12 Audit Trail) for all documents that are printed:
    a. the document being printed
    b. when the print request was made
    c. the name of the person that made the print request
    d. optionally, the name of the person the print request was made for (e.g., in the case of a customer)
    - For purposes of this requirement, this (**d**) only applies when a document is printed for another person such as a customer.
    e. the print device the document was printed on
    f. parameters of the print request (e.g., color, copied, single-sided)
    g. optionally, whether the printed document is a certified copy
    - For purposes of this requirement, this (**g**) only applies when a certified copy of a document is printed.
5. Provide the ability to print certified copies of documents.
    a. Certified copies shall include documents that are one or more pages in length.
    b. Certified copies shall include the same certification number on each page of the document.
    c. Certified copies shall be printed only on printers authorized to print certified copies.
    d. Certified copies shall be configurable to be printed only either plain paper or certified stock.
    e. Certified copies shall be printed only by users authorized to print certified copies.
6. Provide the ability to print barcodes and QR codes™.
    - For the purpose of this requirement, the barcodes and QR codes™ often contain index field values taken from a document or document assembly.
7. Provide the ability to print using pre-printed forms.

8. Provide an application that is configured for performing content printing for all DIWS 2 document types and content types, subject to the security, renditions, redactions, and other restrictions defined within this TO.

5.7 Correspondence Tracking

DIWS 2 shall provide correspondence tracking consisting of the following capabilities for the sources and destinations illustrated in **Figure 2 Correspondence Tracking Sources and Destinations**:

a. Integration with the Governor's Office – These requirements address the capabilities required to address correspondence that has arrived at the MVA from the Governor's office or the Secretary's office.
b. Capturing Correspondence – These requirements address the capabilities required to address correspondence that has arrived at the MVA central and branch offices from sources other than the Governor's office or the Secretary's office.
c. Managing Correspondence within MVA – These requirements address the capabilities associated with creating the response to correspondence that has arrived at the MVA central and branch offices.
d. Responding to Correspondence – These requirements address the capabilities associated with delivering the response that was created to address correspondence that arrived at the MVA central and branch offices.
e. Tracking Correspondence Inside of the MVA – These requirements address the capabilities for tracking correspondence that has arrived at the MVA central and branch offices.
f. Tracking Correspondence Outside of the MVA – These requirements address the capabilities for tracking correspondence that has departed the MVA central and branch offices.

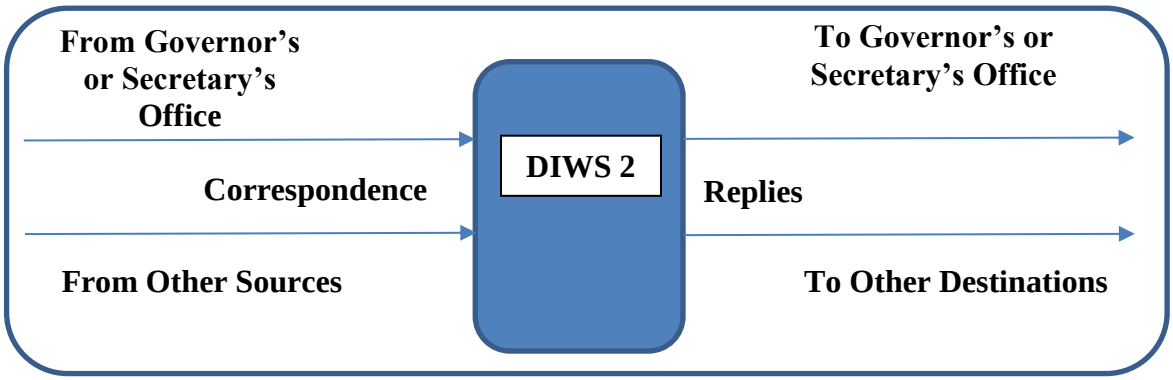

Figure 2 Correspondence Tracking Sources and Destinations

For the correspondence tracking requirements, Integration with the Governor's Office, **DIWS 2 shall**:

1. Provide the ability to update the status of a correspondence in Internet Quorum4.
2. Provide the ability to retrieve the status of all pending MVA correspondence from Internet Quorum4.
3. Provide the ability to retrieve the status of a specific correspondence item from Internet Quorum4.
4. Provide a content/document type for unsolicited correspondence that has arrived at MVA.
5. Provide the ability to change the content/document type of the unsolicited correspondence content/document type.
6. Provide the ability to scan and index unsolicited correspondence.
7. Provide the ability to assign a unique correspondence tracking identifier for each piece of unsolicited correspondence.
8. Provide the ability to have multiple pages per unsolicited correspondence, such as when a multi-page letter is received.
9. Provide the ability to have multiple correspondence documents associated with one unsolicited correspondence tracking identifier.
    - Such as when supporting documents are included with a letter.
10. Provide the ability to route unsolicited correspondence documents in one or more workflows.
11. Provide the ability to associate unsolicited correspondence with an existing case, where a case is defined by an attribute associated with a configurable list of document types.

For the correspondence tracking requirements, Capturing Correspondence, **DIWS 2 shall**:

12. Provide the ability to capture all correspondence and all attachments that arrive electronically (e.g., fax, e-mail, Web, and disk).
13. Provide the ability to scan all correspondence and attachments that arrive at MVA in a paper format.
14. Provide the ability to assign a unique correspondence tracking identifier to all correspondence and attachments that arrive at MVA.
15. Automatically instruct the scanner to separate checks from incoming correspondence.

16. Automatically capture the following index information for all checks identified as part of incoming correspondence:

    a. Check amount
    b. Check date
    c. Check number
    d. Check ABA routing number
    e. Check account number
    f. Check issuer
    g. Document batch the check was part of
    h. All other information that is common to scanned documents (e.g., scan date, scanner, scan operator, document format).

For the correspondence tracking requirements, Managing Correspondence within MVA, **DIWS 2 shall**:

17. Provide the ability to create a set of workflows to route correspondence and attachments that arrive at MVA.

18. Provide the ability to create an ad hoc workflow to route correspondence and attachments that arrive at MVA.

19. Provide the ability to automatically assign correspondence of a specific document type, and the associated attachments, that arrive at MVA to an appropriate workflow.

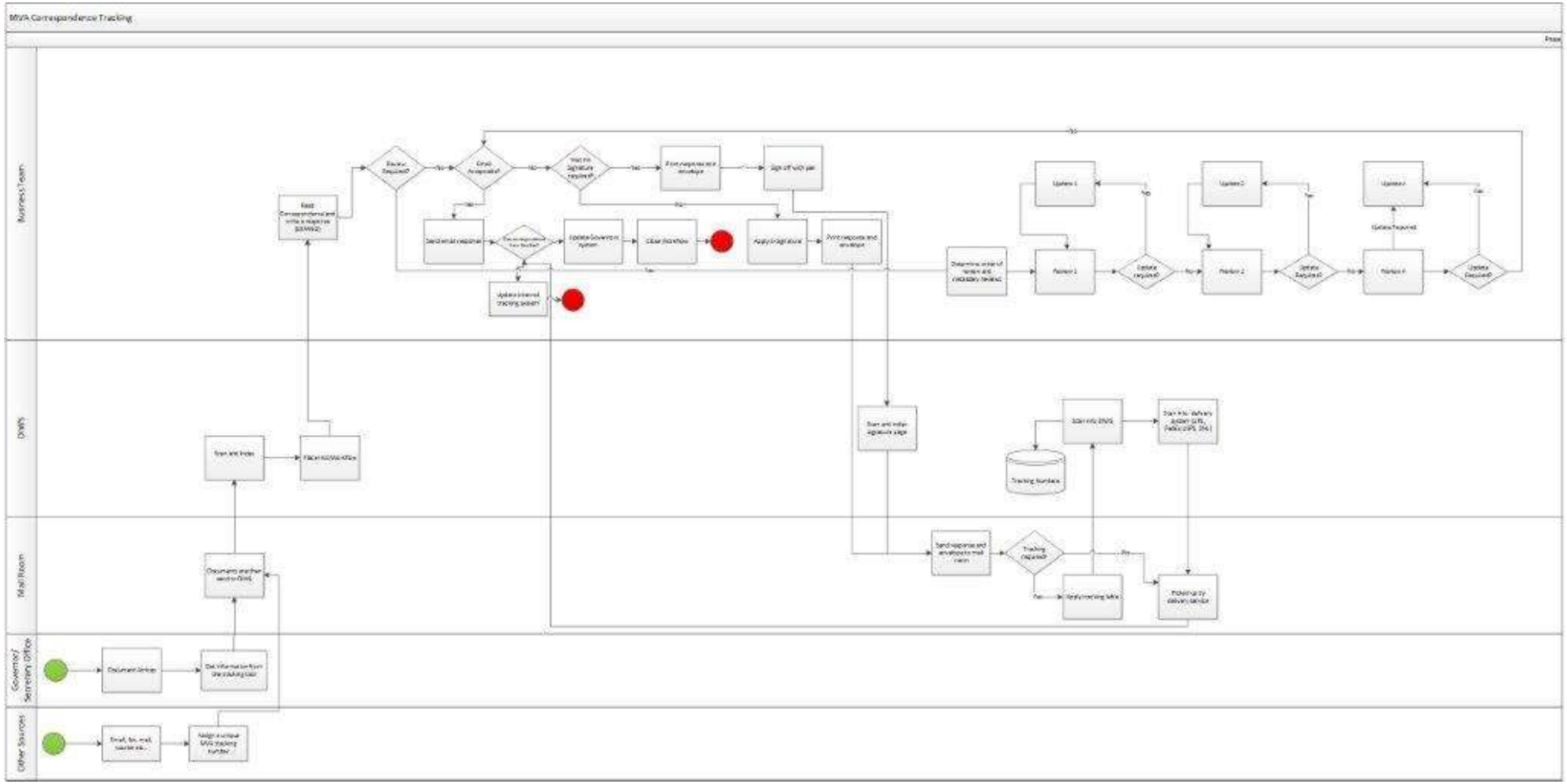

Figure 3 Correspondence Tracking Intake, Capture and Response Workflow Components

Figure 4 Correspondence Tracking External Delivery Company Status Monitoring

20. Provide the workflow illustrated in **Figure 3 Correspondence Tracking Intake, Capture and Response Workflow Components**.
21. Provide the workflow illustrated in **Figure 4 Correspondence Tracking External Delivery Company Status Monitoring**.
22. Provide the ability to manually assign all correspondence and attachments that arrive at MVA to an appropriate workflow.
23. Provide the ability to route all correspondence and attachments that arrive at MVA in a workflow.
24. Automatically notify the appropriate staff whenever a transition to a step in the correspondence workflow takes place.
    - Notifications would be expected to be sent to all members of a group associated with a workflow step as part of the transition from one workflow step to another workflow step.
25. Automatically remind the appropriate staff whenever correspondence has not been started within a configurable period of time.
    - For the purpose of this requirement, a period of time may be measured in hours or days.
    - Reminders would be expected to be sent to all members of a group if the workflow step has not been started within a configurable period of time.
26. Automatically remind the appropriate staff whenever correspondence has not been completed within a configurable period of time.
    - For the purpose of this requirement, a period of time may be measured in hours or days.
    - Reminders would be expected to be sent to all members of a group if the workflow step has not been completed within a configurable period of time.
27. Provide the ability for administrators and users to enable and disable automatic notifications and reminders for correspondence tracking, for all notifications and reminders defined in Section 5.7 Correspondence Tracking, for specific users and specific types of reminders and notifications.
    a. For the purpose of this requirement, each reminder and notification that has been defined by a requirement shall be considered a type of reminder or notification.
28. Automatically route correspondence, attachments, and replies for business and legal reviews using workflows when necessary.

29. Automatically update the status of external correspondence tracking systems based on the progress of correspondence in a workflow.
30. Include all other workflow requirements included in the Workflow section of DIWS 2 Appendix 5.
31. Manage all information captured as part of the correspondence tracking capabilities in accordance with Records management and Record retention policies defined in Section 4.14 Records Management and Legal Hold.
    - For the purpose of this requirement, the correspondence and the data associated with tracking the correspondence shall be preserved in accordance with MVA record retention policies.
    - For example, the USPS tracking information indicating a package was signed for would be maintained with for the period of time specified by Records management capabilities specified in Section **4.15 Records Management and Legal Hold**.

For the correspondence tracking requirements, responding to correspondence, **DIWS 2 shall**:

32. Provide the ability to apply an electronic signature to MVA.
    - MVA replies are electronic responses to correspondence received by the MVA. Outgoing replies are paper responses to correspondence received by the MVA.
33. For outgoing replies that require a wet-ink signatures, provide the ability to print replies for wet-ink signature after all reviews and approvals have been performed.
34. Provide the ability to scan replies with wet-ink signatures, save and associate them with the case.
35. Provide the ability to print properly addressed envelopes for replies that will be delivered by couriers and other non-electronic transport.
36. Print a tracking cover sheet for all replies requiring a delivery tracking number.
37. Provide the ability to place a time limit on electronic signatures.
    a. Electronic signatures for correspondence shall conform to the requirements also specified in 4.3 Electronic Forms and Signatures
    b. There shall be a mechanism to revoke a user's ability to apply electronic signatures for specified document types based on an effective date.

For the correspondence tracking requirements, Tracking Correspondence Inside of the MVA, **DIWS 2 shall**:

38. Provide the ability to query the status of any correspondence that is (or was) in a DIWS workflow and has an assigned correspondence tracking identifier or other tracking number (e.g., an Internet Quorum4 tracking number).
39. Provide the ability to automatically execute a report at a configurable interval on the status of all correspondence that is (or was) in a DIWS workflow and has an assigned correspondence tracking identifier or other tracking number (e.g., an Internet Quorum4 tracking number).
40. Provide the ability to automatically execute a report at a configurable interval on the status of all correspondence that was sent to MVA and has an Internet Quorum4 tracking number.
41. Provide the ability to automatically execute a report at a configurable interval of all checks received within correspondence.
    a. The checks received report shall be configurable as either a deposit slip or as an inventory list.
42. Provide the ability to manually execute all reports identified in this section.
43. Provide the ability to save correspondence tracking report results to a configurable folder in the repository.

For the correspondence tracking requirements, Tracking Correspondence Outside of the MVA, **DIWS 2 shall**:

44. Provide the ability to send correspondence with tracking numbers using USPS, Federal Express, UPS, and others.
45. Provide the ability to automatically interrogate the delivery services for the status of all correspondence sent with tracking numbers and record the tracking numbers, the tracking record, and the date the tracking record was most recently updated.
46. Provide the ability to configure the frequency with which the delivery services are automatically interrogated.
47. Provide the ability to automatically begin integrating the delivery services when a delivery number is assigned.
48. Provide the ability to automatically cease interrogating the delivery services when the correspondence has reached its destination.
49. Capture the information obtained from interrogating the delivery services as part of the correspondence tracking information maintained in DIWS 2.
50. Provide the ability to query the status of any correspondence that is being sent with a tracking number.

51. Provide the ability to automatically execute a report on the status of all correspondence that is being tracked at a configurable interval and save the report results to a configurable folder in the repository.

52. Provide the ability to manually execute all reports identified in this section.

6. Nonfunctional Requirements

There are areas for which DIWS 2 has specified requirements that are not considered entirely functional in nature. For purposes of categorization, these requirements are referred to as nonfunctional requirements. Nonfunctional requirements apply across the ECM (except where expressly indicated), including the capture functionality. These nonfunctional requirements include:

- Architecture
- Capacity
- Performance
- Integration
- Devices
- Product Roadmap
- Migration

6.1 Architecture

DIWS 2 shall be based on a solid architecture to achieve the functional, capacity, performance and integration requirements set forth in this task order. For the purpose of the requirements identified in this section, general architectural diagrams that illustrate a configuration capable of the satisfying the DIWS 2 requirements are sufficient.

For the architecture requirements, **the Offeror shall:**

1. Propose a high-level conceptual architecture diagram identifying the entities and the relationships between the entities to achieve the functionality and capacity requirements of DIWS 2.
2. Propose a high-level logical architecture diagram identifying the main components, their interconnections, and flows between the components for the proposed DIWS 2 solution.
3. Propose a high-level physical architecture diagram identifying the hardware and software components required configuration required to achieve the functionality and capacity requirements of DIWS 2 for the production environment.

4. Provide a bill of materials (see Appendix 18 – Offeror Hardware and Software Bill of Material) identifying the hardware and software infrastructure components required for all environments of the proposed solution for implementation at the MVA data center. Note: if data migration is offered as a hosted service, list data migration in response to Requirement 6 below.

    a. The hardware and software required for all environments mentioned in Appendix 1 Execution Requirements, Section 2.6 Architecture & System Environments, Specific Environments, shall be included in the bill of materials.
    b. The purpose for each device in the bill of materials shall be clearly stated (e.g., Production, database server).
    c. The number, size, speed, and type of processors/cores shall be clearly identified for servers, desktops, laptops, tablets and other infrastructure computing devices.
    d. The quantity/size, speed, and type of memory shall be clearly identified for servers, desktops, laptops, tablets and other infrastructure computing devices.
    e. The quantity/size, speed, and type of storage shall be clearly identified for SANs, servers, desktops, laptops, tablets and other infrastructure computing devices.
    f. The quantity and speed of networking connections shall be clearly identified for firewalls, load balancers, servers, desktops, laptops, tablets and other infrastructure computing devices.
    g. The infrastructure software components are limited to the operating system, databases, and other prerequisite and requisite software.

    - The State may provide the hardware at the Agency facility or at a cloud facility.
    - References to desktops, laptops, tablets and other computing requirements in items c, d, e, f, and g, exclude end-user devices. The intent is to identify the hardware and software required for hosting the proposed solution in the MVA data center.

5. The State may optionally decide to host the solution at a cloud facility. Provide a list of differences in the proposed solution if the State were to host the proposed solution using hardware located in the Amazon Web Service cloud.

    - For example, identify changes to staffing, the impact on performance, changes to system availability, additional or different hardware or software, and any other differences.
    - For this requirement, the State seeks information required to consider hosting the solution using an IaaS model.

6. If an off-site, hosted solution is proposed for data migration activities, describe"

    a. the environment;
    b. the safeguards for protecting State content; and
    c. the mechanism for transferring content between the legacy systems, the migration environments, and the test and production systems in the MVA data center

For the architecture requirements, **DIWS 2 shall:**

7. Support 32-bit clients (operating system and hardware) at the performance levels specified in Section 6.3 Performance.
8. Support 64-bit clients (operating system and hardware) at the performance levels specified in Section 6.3 Performance.
9. Support 64-bit servers (operating system and hardware) at the performance levels specified in Section 6.3 Performance.

6.2 Capacity

DIWS 2 shall provide the ability to support the specified number of users and devices, store the specified quantity of content, and perform the specified number of transactions. Further, DIWS shall be sized to grow each of these metrics at the specified size, or at 10% per annum if a growth rate is not specified.

For the capacity requirements, **DIWS 2 shall:**

1. Be initially sized to support the projected size of all metrics specified in Section 6.2 Capacity at the end of ten (10) years.
2. Support **27TB** of image content, at a growth rate of **15%** compounded annually, beginning January 2016.
3. Be able to store and manage **125TB** or more of image content during the life of the contract.
4. Support **395 million** images, at a growth rate of **15%** compounded annually, beginning January 2016.
5. Be able to store and manage **900 million or more** images during the life of the Contract.

6. Support **10TB** of application-specific, non-metadata, data stored in the database.
   - This data stored in the database includes data such as the supporting data for Human Resource, Accounts Payable and Procurement applications that is specified in other appendixes with the DIWS 2 TO.
7. Support **1,600** named users, at a growth rate of **5%** compounded annually, beginning January 2016.
   - This number includes the following number of External System users that are a significant user of DIWS.
8. Support **1,000** concurrent users, at a growth rate of **5%** compounded annually, beginning January 2016.
   - For purposes of this requirement, a concurrent user is a user that performs an operation within **60** seconds of another user.
9. Support **five (5)** high-volume, bulk scanners.
   - High-volume scanners are defined as scanners that can scan at a rate of not less than **one hundred-twenty (120)** double-sided pages per minute, 300 dpi, 24-bit color, for up to 500 consecutive pages.
10. Support the capture of **50,000** pages per day *per* bulk scanner.
    - A "day" is defined as an eight-hour Business Day.
11. Support **5** concurrent bulk scan operators working concurrently with all other activities.
    - For purposes of the requirements in this section, the time for bulk scanning is to be measured at the bulk scanning/back office location while other activities are being performed at locations typical for those activities and at loads specified for those activities.
12. Support **one hundred sixty (160)** operation/counter scanners at the MVA counters located in multiple locations.
    - Operational scanners are defined as scanners that can scan at a rate of not less than **forty (40)** double-sided pages per minute, 300 dpi, 24-bit color, for up to 200 consecutive pages.
13. Support the capture of **10,000** pages per day *per* operational/counter scanners.
14. Support **100** concurrent operation/counter scan operators working concurrently with all other activities.
15. Support **one hundred-fifty (150)** convenience/desktop scanners at the back office desks located in multiple locations.
    - Desktop scanners are defined as scanners that can scan at a rate of not less than **twenty-five (25)** double-sided pages per minute, 300 dpi, 24-bit color, for up to **fifty (50)** consecutive pages.

16. Support the capture of **200** pages per day *per* convenience/desk scanners.
17. Support **100** concurrent convenience/desktop scan operators working concurrently with all other activities.
18. Support **15** documents per second being scanned at the operator stations, with an average storage time of one second and a maximum retrieval of three seconds.
    - For purposes of the requirements in this section, the time for scanning at the operator stations is to be measured at the operations/counter location(s) while other activities are being performed at locations typical for those activities and at loads specified for those activities.
19. Support **20** concurrent indexing operators indexing a least six documents per minute per operator working concurrently with all other activities.
    - For purposes of the requirements in this section, the time for indexing operations is to be measured at the indexing or back office location while other activities are being performed at locations typical for those activities and at loads specified for those activities.
    - For the purpose of this requirement, "working concurrently" should be interpreted as pressing the index button with all index values for an image or document being sent to the repository.
20. Support **20** documents per second being served to the repository for storage, with storage being completed on average in two seconds with a maximum of three seconds.
    - For purposes of the requirements in this section, the time for documents being served to the repository for storage is to be measured at the operations counter location(s) while other activities are being performed at locations typical for those activities and at loads specified for those activities.
21. Support **70** documents per second being retrieved from the repository for viewing, with an average retrieval time of one second and a maximum retrieval of three seconds.
    - Timing is to be measured at an operations/counter location.
22. Provide the ability to support **twenty (20)** initial e-mail accounts, and up to **one hundred (100)** e-mail accounts, for automatically capturing incoming and outgoing e-mails.
23. Provide the ability to support **ten (10)** initial fax numbers, and up to **fifty (50)** fax numbers, for automatically capturing incoming and outgoing faxes.

24. Provide the ability to support **five hundred (500)** initial FTP/SFTP accounts and folders, and up to **5,000** FTP/SFTP accounts and folders, for automatically capturing *incoming* FTP traffic.
    - For the purpose of this requirement, an incoming FTP/SFTP account is used by an MVA business unit to accept content from external users and systems. Typically, one account is assigned to each external user or system. Each FTP/SFTP account allows a specific customer, supplier, vendor or other entity to transmit content to the MVA. Some FTP/SFTP accounts will exist for a limited time (e.g., while an RFP is open for response) after which time the account will be made inaccessible.
    - For the purpose of this requirement, one incoming FTP/SFTP folder is associated with each incoming FTP/SFTP account to ensure information sent to the MVA is separated by source.
25. Provide the ability to support **twenty (20)** initial FTP/SFTP accounts and folders, and up to **one hundred (100)** FTP/SFTP accounts and folders, for automatically capturing *outgoing* FTP traffic.
    - For the purpose of this requirement, an outgoing FTP/SFTP account is used by an MVA business unit to send content to external users and systems. Typically, one account would be assigned to each business area and could be used to communicate with an unlimited number of customers, suppliers, vendors or other entities.
26. Be provided with a sufficient licenses to support the capacity parameters specified in Section 6.2 Capacity.

27. Provide the ability for the DIWS 2 external interface as defined in DIWS 2 RFP, Appendix 10, to sustain the loads defined in the following use case profiles:
    a. (#C1) Capture General Content – 180 concurrent transactions per minute
    b. (#C2) Retrieval General Content – 180 concurrent transactions per minute
    c. (#C3) Capture Solicited Correspondence – 180 concurrent transactions per minute (capture using scanning, e-mail, fax, and FTP/SFTP)
    d. (#C4) Capture Unsolicited Correspondence – 180 concurrent transactions per minute (capture using scanning, e-mail, fax, and FTP/SFTP)
    e. (#C5) Manual Verification of Content – 60 concurrent transactions per hour
    f. (#C6) Assemble Documents – 100 concurrent transactions per hour
    g. (#C7) Delete Documents – 100 concurrent transactions per day
    h. (#C8) Change Retention Period – 100 concurrent transactions per day
    i. (#C9) Create Redacted Documents – 100 concurrent transactions per hour (automated redaction of three fields)
    j. (#C10) Modify Document/Content Type – 100 concurrent transactions per hour
    k. (#C11) Modify Metadata – 100 concurrent transactions per hour
    l. (#C12) Transmit Content – 100 concurrent transactions per hour
    m. (#C13) Search for Content – 180 concurrent transactions per minute
    n. (#C14) Create Content via Interchange with an External System – 180 concurrent transactions per hour
    o. (#C15) Create Temporary Content Type from Barcode Sheet – 180 concurrent transactions per day
    p. (#C16) Mobile Capture – 100 concurrent transactions per hour
    q. (#C17) Mobile Search and Retrieval – 1,000 concurrent transactions per hour
    r. (#C18) Data Extraction from Images – 100 concurrent transactions per hour.
    s. (#C19) Rapid Bulk Migration/Import – 1,000,000 images per weeknight (8:00 PM – 4:00 AM); AND 100,000,000 images over 10 weeks – (five batches of one million per weeknight, five batches of one million per weekend).
    t. (#C20) General and QA Auditing Status Retrieval – 24 concurrent transactions per minute
    u. (#C21) General and QA Auditing Status Update – 72 concurrent transactions per minute

- Item “s” applies to the external interface defined in Appendix 10 and not to the migration activities defined in Appendix 9.

28. DIWS 2 shall be operational every calendar day of the year and 24 hours every day, in accordance with the following:
    a. The DIWS 2 shall be designed to meet a 99.99% system availability requirement, exclusive of Planned Downtime for system maintenance and upgrades. (Also see Appendix 3, Section 4.3 O&M Support Services, Requirement 4.)
    b. Planned Downtime shall be scheduled outside of Operational Hours, outside of any batch processing window, and shall not require the DIWS 2 System to be unavailable or limited in functionality for more than 1 hour per week.
    c. This system availability requirement shall apply to all user interfaces and the External Systems Integration (see Appendix 10 Section 2.8 External Interfaces, Requirement 8).
    d. Planned Downtime system maintenance and upgrades shall only occur outside of Operational Hours, outside of any scheduled batch processing window, and shall not require the DIWS 2 to be unavailable or limited in functionality for more than one (1) hour per week.
    e. This system availability shall include end-to-end System availability of all software, hardware and communications interfaces between the DIWS 2 and all other systems that the Offeror identified in its response to this solicitation OR that the Contractor has included in its requirements and design.

For the capacity requirements, **the Offeror shall:**

29. Specify the hardware and software licenses required to satisfy ten (10) year capacity projections.
    - As it relates to this requirement, MVA will provide the required hardware based on recommendations it receives in the reviewed and approved capacity planning deliverable.
    - In the event the MVA decides to delay acquiring the hardware required for all or part of the ten (10) year growth, this requirement shall be considered satisfied based on meeting a prorated capacity tied to the level of hardware MVA acquires.
    - In the event the MVA decides to delay acquiring the software licenses required for all or part of the ten (10) year growth, this requirement shall be considered satisfied based on meeting a prorated capacity tied to the number of software licenses that MVA acquires.

6.3 Performance

DIWS 2 is expected to perform at the levels specified by the requirements in this section when loaded to the capacity specified in Section **6.2 Capacity**. When growth rates are mentioned in the Section **6.2 Capacity**, the DIWS shall perform at specified levels in this section at all times during the specified growth period.

For the performance requirements, **DIWS 2 shall:**

1. Provide response time of **0.45** seconds for retrieving and presenting a single page image file.
   - For the purpose of this requirement, the image file shall be "A" size, 8 bit greyscale, 300 dpi.
   - The time shall begin when the request is made and shall stop when the image is fully viewable on the screen.
   - The time shall be measured at a desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.
2. Provide response time of **0.45** seconds for retrieving and presenting the first page of a three page image file.
   - For the purpose of this requirement, the each image in the three image file shall be "A" size, 8 bit greyscale, 300 dpi.
   - The time shall begin when the request is made and shall stop when the image is fully viewable on the screen.
   - The time shall be measured at a desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.
3. Provide response time of **0.55** seconds for retrieving and presenting the second and third pages of a three page image file.
   - For the purpose of this requirement, the each image in the three image file shall be "A" size, 8 bit greyscale, 300 dpi.
   - The time shall begin when the first page of the image file is fully viewable on the screen and shall stop when the second and third images are fully viewable on the screen.
   - The time shall be measured at a DIWS 2 desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.

4. Provide response time of **0.40** seconds for retrieving a one page image file.
   - For the purpose of this requirement, the each image in the three image file shall be "A" size, 8 bit greyscale, 300 dpi.
   - The time shall begin when the API or Web service is invoked and shall stop when name of the file containing the images is provided to application making the request.
   - The time shall be measured from a non-DIWS 2 laptop, desktop or server, as directed by the MVA Project Manager.
5. Provide response time of **0.80** seconds for retrieving a three page image file.
   - For the purpose of this requirement, the each image in the three image file shall be "A" size, 8 bit greyscale, 300 dpi.
   - The time shall begin when the API or Web service is invoked and shall stop when name of the file containing the images is provided to application making the request.
   - The time shall be measured from a non-DIWS 2 laptop, desktop or server, as directed by the MVA Project Manager.
6. Provide response time of **0.15** seconds for presenting a drop down or selection list to a user for any indexing any field during document indexing.
   - The time shall be measured from a DIWS 2 laptop or desktop and shall apply to all index fields for all document and content types.
7. Provide the ability to satisfy the response time values all retrieval operations, regardless of purpose.
   - For the purpose of this requirement, the retrieval times specified in the performance requirements should be satisfied for laptop users, desktop users, mobile device users, external interface users, index users, quality assurance users.
8. Provide a response time of **0.5** seconds for storing one document containing up to 100KB in the repository.
   - The time shall begin when the user clicks the button and shall stop when an indicator showing success has been returned to the user.
   - These times do no need to include time for redacting, rendering and other operations, unless these operations are required to be performed at the time the document is stored.
   - The time shall be measured at a DIWS 2 desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.

9. Provide a response time of **1.2** seconds for storing three documents containing up to 300KB in the repository.
   - The time shall begin when the user clicks the button and shall stop when an indicator showing success has been returned to the user.
   - These times do no need to include time for redacting, rendering and other operations, unless these operations are required to be performed at the time the document is stored.
   - The time shall be measured at a DIWS 2 desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.
10. Provide a response time of **4.0** seconds for storing ten documents containing up to 1,000KB in the repository.
   - The time shall begin when the user clicks the button and shall stop when an indicator showing success has been returned to the user.
   - These times do no need to include time for redacting, rendering and other operations, unless these operations are required to be performed at the time the document is stored.
   - The time shall be measured at a DIWS 2 desktop or workstation at either the operations counter or desk, as directed by the MVA Project Manager.

11. Provide the ability for the DIWS 2 external interface as defined in DIWS 2 RFP, Appendix 10 External Systems Integration, to respond at the levels defined in the following use case profiles, concurrent with all other loads (see Section 6.2 Capacity) on the system from laptops, desktops, mobile devices, fax machines, e-mail and FTP/SFTP:

    a. (#C1) Capture General Content – **0.40** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.50** seconds for one 100KB document.
    b. (#C2) Retrieve General Content – **0.45** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.30** seconds for one 100KB document.
    c. (#C3) Capture of Solicited Correspondence – **0.45** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.30** seconds for one 100 KB document.
    d. (#C4 Manual Verification of Content – **0.15** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.20** seconds.
    e. (#C5) Capture of Unsolicited Correspondence – **0.45** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.30** seconds for one 100 KB document.
    f. (#C7) Delete Documents – **0.10** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.20** seconds for one 100 KB document.
    g. (#C5) Capture of Unsolicited Correspondence – **2,000** concurrent transactions within Normal MVA Business Hours.
    h. (#C8) Change Retention Period – **0.25** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.35** seconds
    i. (#C10) Change Document/Content Type – **0.50** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.70** seconds for one 100 KB document.
    j. (#C11) Modify Metadata – **0.15** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.20** seconds for one 100 KB document.
    k. (#C13) Search for Content – **0.10** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.20** seconds for ten results searching 200 million records.

12. This requirement has been removed.

13. Provide the following response times for performing OCR/ICR on images that are up to 8-1/2”x11” per page, at 300 dpi, bi-level or 8-bit greyscale, 11 point fonts, with five OCR/ICR operations being performed concurrently for :
    a. One page at – **0.50** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are within completed within **0.70** seconds.
    b. Two pages at – **0.70** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are within completed within **0.90** seconds.
    c. Three pages at – **0.90** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are within completed within **1.10** seconds.
14. Provide the following response times for performing content/document type recognition on images that are up to 8-1/2”x11” per page, at 300 dpi, bi-level or 8-bit greyscale, 11 point fonts, with five content/document type recognition operations being performed concurrently:
    a. One page at – **0.50** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.70** seconds.
    b. Two pages at – **0.70** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.90** seconds.
    c. Three pages at – **0.90** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **1.10** seconds.
15. Provide the following response times for performing information extraction from images of a known content/document type that are up to 8-1/2”x11” per page, at 300 dpi, bi-level or 8-bit greyscale, 11 point fonts, 15 fields, with five information extraction operations being performed concurrently:
    a. One page at – **0.50** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.70** seconds.
    b. Two pages at – **0.70** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.90** seconds.
    c. Three pages at – **0.90** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.10** seconds.
16. Provide the following response times for performing information extraction from images of an unknown valid content/document type that are up to 8-1/2”x11” per page, at 300 dpi, bi-level or 8-bit greyscale, 11 point fonts, 15 fields, with five information extraction operations being performed concurrently:
    a. One page at – **0.60** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **0.80** seconds.
    b. Two pages at – **0.80** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **1.00** seconds.
    c. Three pages at – **1.00** seconds on average and 95.4499736% (i.e., 2σ) of the transactions are completed within **1.20** seconds.

17. Automatically capture and store the time required for all activities in Section 6.3 Performance that have a performance time specified.
    - This requirement is intended to create a log of times that can be used for reporting system performance over time. It should be interpreted as "capture and store" for daily operations, not just for performance testing.
18. Measure the performance time for all document operations *after* the first document operation at a workstation, or in a browser has completed.
    a. For the purpose of all performance times in Section 6.3 Performance taken at a workstation, the workstation shall be defined as any MVA desktop, MVA laptop, or MVA tablet device that was placed into service within the past two years.
    b. For the purpose of all performance times in Section 6.3 Performance taken at a browser, the browser shall be defined as any browser identified in Appendix 11, Section 6 User Interface, requirements 13-16, operating on an MVA desktop, MVA laptop, or MVA tablet device that was placed into service within the past two years.
    - Examples of document operations include viewing, quality control operations, printing, OCR operations, rendering operations, and other operations that act on content.
    - The intent of this requirement is to exclude delays that occur only once per user session. Examples of these types of delays are the time required to perform document operations. Ideally, the loading of the tools required to perform document operations would be handled at the time the user begins their session, but there is no requirement for loading tools prior to need.
    - This requirement is not in conflict with Section 6.3 Performance, requirement **17** that requires all performance times to be captured and stored. This requirement allows the performance times for the initial document operation in any session to be excluded from performance measurement calculations and reporting.
19. Exclude delays directly attributable to the WAN and VPN if the Contractor is able to satisfy all of the following conditions:
    a. The Contractor is able to definitively calculate the time for WAN and VPN delays.
    b. The WAN delay only occurs on the State's inter-site WAN used for communication between two MVA sites.
    c. The WAN delay is not for a Glen Burnie user located at the Glen Burnie facilities.
20. Perform at response times that are within double the performance measurements specified in Section 6.3 Performance, for Contractor's providing solutions residing in externally hosted data centers (e.g., the cloud).

21. Perform at the levels specified by the requirements in Section 6.3 Performance when loaded to the capacity specified in Section 6.2 Capacity.

6.4 Integration

DIWS 2 shall provide the ability to integrate with external systems. This integration shall allow DIWS 2 to access external systems for obtaining data as well as sending and receiving content. (See Section 3.5 Indexing Requirement 35.) This integration shall also allow DIWS 2 to be accessed by external systems for the purposes of storing content, retrieving content, searching for content, receiving and transmitting content, content assembly and publishing, accessing document and imaging peripherals, migration, and other activities specified, required or implied by the requirements in the DIWS 2 RFP and the approved DIWS 2 requirements documents.

The following integration, identified elsewhere in the RFP and TO, shall be provided at the time the capability identified in the associated appendix is delivered:

a. Appendix 6 – Functional Requirements: Accounts Payable, Section 2.6 External Interfaces
b. Appendix 7 – Functional Requirements: Human Resources, Section 2.6 External Interfaces
c. Appendix 8 – Functional Requirements: Procurement, Section 2.6 External Interfaces
d. Appendix 10, External System Integration Requirements.

For providing integration, **DIWS 2 shall:**

1. Provide the ability to access external interfaces using Web services.
   - For example, accessing master data for validating metadata values.
   - See related Web services requirements in Appendix 11, Section 4 Interoperability and Integration and Appendix 11, Section 5 Regulatory and Security.
2. Provide the ability to access external interfaces using published APIs.
   - For example, accessing master data for validating metadata values.
3. Provide the ability for external applications to access and utilize all capabilities and functionality outlined in the toolbox requirements (Appendix 5) via Web services and APIs.

4. Provide the ability to retrieve index field values related to driver and driver license documents and their index field values from an external system(s) for use in any field.
   - An example of where this capability is used is in the indexing of content that arrives in the mailroom. After scanning, some basic field validation is expected to be available during content indexing.
   - Examples of driver index field values include, but are not limited to:
     - Customer identifier
5. Provide the ability to verify index field values related to driver and driver license documents and their index field values as being valid.
   - Also see related usages in Appendix 10 External Systems Integration and see Appendix 5 Section 3.5 Indexing Requirement 35.
6. Provide the ability to retrieve index field values related to vehicle documents and their index field values from an external system(s) for use in any field.
   - Examples of vehicle index field values include, but are not limited to:
     - Vehicle title
     - Registration identifier
     - Vehicle identification number ("VIN")
7. Provide the ability to verify index field values related to vehicle documents and their index field values as being valid.
8. Provide the ability to retrieve index field values related to human resource documents and their index field values from an external system(s) for use in any field.
   - Examples of human resource index field values include, but are not limited to:
     - Employee identifier, name, address and other information
     - Dates of employment
     - Contract information
9. Provide the ability to verify index field values related to human resource documents and their index field values as being valid.
10. Provide the ability to retrieve index field values related to accounts payable documents and their index field values from an external system(s) for use in any field.
    - Examples of accounts payable index field values include, but are not limited to:
      - Invoice number
      - Purchase order number
      - Vendor identifier, name, address, and other information
      - Vendor contact information
      - Contract information

11. Provide the ability to verify index field values related to accounts payable documents as being valid.
12. Provide the ability to retrieve index field values related to procurement documents from an external system(s) for use in any field.
    - Examples of procurement index fields include, but are not limited to:
      - Contract identifier
      - RFI identifier
      - RFP identifier
      - Vendor identifier, name, address, and other information
      - Vendor contact information
      - Contract information
13. Provide and support data validation against XML data.
14. Support data validation against mainframe data
15. Support data validation against local database tables
16. Support data validation against non-local database tables
17. Support data validation using Web interfaces to external systems
18. Support data validation using Web services
19. Support an API that accepts a file containing meta data and file URLs for content that is to be stored in the repository.
20. Support an API that accepts a memory resident data structure containing meta data and file URLS for content that is to be stored in the repository.
21. Support an API that presents dialog box for scanning and indexing an image.
22. Support an API that returns content in a file to the calling application.
23. Support an API that returns content in a memory resident data structure to the calling application.
24. Support an API that presents content in a pop-up leveraging a viewing tool.
25. Support an API that accepts a set of parameters containing metadata for performing repository searches.
26. Support an API that accepts a set of parameters for performing full text repository searches.
27. Support an API that accepts a set of parameters for combined index field value and full text searches.
28. Provide the ability to integrate with Microsoft Exchange **2010**.
29. Provide the ability to seamlessly integrate with Microsoft **Office 2013** products.

30. Ability to integrate with the latest two versions of SalesForce.
31. Provide the ability to integrate with **Imprivata OneSign Agent 4.8.003.33** for single sign on.
32. Provide The ability to integrate with MDOT FMIS.
    - FMIS is an MDOT developed application. The minimal integration is identified in Appendix 6, Section 2.6 External Interfaces. This integration may need to be accomplished through a terminal emulator.
33. Provide The ability to integrate with MDOT HRIS.
    - HRIS is an MDOT developed application. The minimal integration is identified in Appendix 7, Section 2.6 External Interfaces. This integration may need to be accomplished through a terminal emulator.
34. Provide the ability to work with Active Directory **2012**.
    - See related Active Directory requirements in Appendix 11, Section 8. Application Domain.
35. Support Microsoft Server **2012**.
36. Support future versions of Microsoft Server within one year of the version being released.
37. Provide the ability to operate in the Microsoft Windows **7 32-bit** environment.
    - There are many State applications that continue to require Windows 7 and many of these only execute in a 32-bit environment.
38. Support Microsoft Internet Explorer, version **9**.
39. Support Microsoft Internet Explorer, version **10**.
40. Support Microsoft Internet Explorer, version **11**.
41. Support future versions of Microsoft Internet Explorer within six months of the version being released.
42. Support Microsoft Edge (browser).
43. Support Java at level **1.8.0.45 JRE** and later.
44. ` Support of the Microsoft MS SQL Server database, version **2012**.
    - For the purpose of this requirement, *MS SQL* should be considered a strong preference, not a requirement. The Offeror can make a compelling reason for an alternative database if the Offeror believes it would be in the best interest of the State to consider and alternative database.

45. For VPN, support the Cisco ASA for remote access VPN tunnels using Entrust tokens and also have a JUNIPER 6500 SSL Appliance for a Web VPN portal.
    a. Support Cisco AnyConnect – 3.1.04066.
46. Support of the McAfee Agent - 4.8.0.1938 for antivirus software on the client devices.
47. Support of the McAfee VirusScan Enterprise – 8.8.0.1247for antivirus software for the ECM servers.
48. Support Vormetric Data Encryption Expert, version 5.2.3 for encrypting content at rest.
49. Integrate with Internet Quorum4 for to support correspondence management as defined in Section 5.5 Correspondence Management.
50. Leverage the LMS software product, Cornerstone on Demand for help text and other user readable information.
    - At this time Cornerstone on Demand has not been fully deployed. If Cornerstone on Demand is not deployed in a manner that allows it to be integrated for managing help text and other user readable information, this requirement will not apply.
51. Integrate with MDOT's electronic fax product, GFI FaxMaker, version 2015.
52. Provide feeds, on a configurable interval, of all new driver's license images and supporting metadata sent to the facial recognition system.
    - The current interval is once each day, but the interval should be configurable from one minute to **999** days.
53. Provide Simple Network Management Protocol (SNMP) interfaces.
54. Allow the MVA Project Manager to substitute a supported version of any software identified in Section 6.4 Integration, when the specified version of the software will no longer be supported when the software enters production.

6.5 Devices

DIWS 2 shall work with desktop, laptop, smart phones, tablets, and other devices capable of providing a user interface. All functionality that is available through a desktop or laptop shall also be available through a smart phone, tablet, and other user interface devices. All functionality that is available through a smart phone, tablet, or other smart device shall also be available through a desktop or laptop.

For the device support requirements, **DIWS 2 shall:**

1. Support Android-based smart phones running Android v5.0 ("Lollipop") and later.
   - For purposes of this requirement, when a specific version of an operating system is mentioned, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.
2. Support Android-based tablets running Android v5.0 and later ("Lollipop")
   - For purposes of this requirement, when a specific version of an operating system is mentioned, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.
3. Support Apple smart phone devices running the iOS operating system.
4. Support Apple tablet devices running the iOS operating system.
5. Support Apple watch devices integrated with the iOS operating system.
6. Support smart phone devices running the Android operating system.
7. Support tablet devices running the Android operating system.
8. Support watch devices integrated with the Android operating system.
9. Support desktop and laptop devices running the Windows 7 operating system.
   - For purposes of this requirement, when a specific version of an operating system is mentioned, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.
10. Support desktop and laptop devices running the Microsoft Windows 8 operating system.
    - For purposes of this requirement, when a specific version of an operating system is mentioned, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.
11. Support desktop and laptop devices running the Microsoft Windows 10 operating system.
    - For purposes of this requirement, when a specific version of an operating system is mentioned, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.

12. Support desktop and laptop devices running the latest version of the Microsoft Windows operating system within one year of the operating system being released.
    - For purposes of this requirement, the latest patches, fixes, and enhancements for that version that are available at the time DIWS goes into production shall apply.
13. Ensure that devices are mobile aware for sending content.
    - For the purpose of this requirement, "Mobile aware" means that a device is aware of its location and the attributes of that location. For example, a user may have captured images on a tablet device or smart phone that automatically upload from the device to DIWS 2 when the device has a signal and is able to connect to the MVA network and DIWS 2.
14. Ensure that devices are mobile aware for receiving content.
    - For the purpose of this requirement, "Mobile aware" means that a device is aware of its location and the attributes of that location. For example, a user may have a request pending to retrieve images on a tablet device or smart phone that automatically download from DIWS 2 to the device when the device has a signal and is able to connect to the MVA network and DIWS 2.

6.6 Product Roadmap

The MVA environment continues to evolve as business needs evolve and technology matures. For those hardware and software components that MVA expects to use in the future, the Offeror shall provide a Product Roadmap within the delivered documentation on when and how these components shall be incorporated into the requisite products and the earliest date that these comments could be available for incorporation into DIWS 2 and applications built on DIWS 2. The requirements in this section are an extension to RFP Section 3.4.5.1.4 Product Roadmap.

For the Product Roadmap requirements, **the Offeror shall:**

1. Include a Product Roadmap that identifies when the next two major releases of all prerequisite and requisite products shall be supported by the underlying product and available for use by DIWS 2 and applications built on DIWS 2. The Product Roadmap shall also include:

    a. Browsers as indicated in Section 6.6 Product Roadmap, Requirement 3.
    b. Devices as indicated in Section 6.6 Product Roadmap, Requirement 4.
    c. MS Office as indicated in Section 6.6 Product Roadmap, Requirement 5.
    d. Standards as indicated in Section 6.6 Product Roadmap, Requirement 6.

    - For purposes of this requirement, the requisite and prerequisite products shall include:

        e. all software products installed with DIWS 2
        f. all smart phones, tablets and other smart devices
        g. all hardware and software listed in Section 6.5 Devices or Section 6.6 Product Roadmap, excluding laptop and desktop devices

    - For purposes of this requirement, the next two major releases of requisite and prerequisite products are considered those releases that have been publicly announced by the requisite and prerequisite product owners or privately disclosed to the MVA.
    - Include all information identified in the RFP Section 3.4.5.1.4 Product Roadmap.

For the Product Roadmap requirements, **the Contractor shall:**

2. Provide a Product Roadmap that identifies when the next two major releases of all prerequisite and requisite products shall be supported by the underlying product and available for use by DIWS 2 and applications built on DIWS 2.

    a. A draft version of the Product Roadmap shall be delivered when the design documentation is provided.
    b. A final version of the Product Roadmap shall be delivered when the first production release of DIWS 2 goes live.

    - For purposes of this requirement, the requisite and prerequisite products shall include:
        c. all software products installed with DIWS 2
        d. all smart phones, tablets and other smart devices
        e. all hardware and software listed in Section 6.5 Devices or Section 6.6 Product Roadmap, excluding laptop and desktop devices
    - For purposes of this requirement, the next two major releases of requisite and prerequisite products are considered those releases that have been publicly announced by the requisite and prerequisite product owners or privately disclosed to the MVA.
    - For purposes of this requirement, the Product Roadmap may be an updated version of the Product Roadmap that was previously delivered by the Offeror.
    - Include all information identified in the RFP Section 3.4.5.1.4 Product Roadmap.

3. Indicate on the Product Roadmap when all announced versions of the Browsers identified in Appendix 11, Section 6 User Interface, requirements 13-16, will be supported.

4. Indicate on the Product Roadmap when all announced versions of the devices and operating systems identified in Section 6.5 Devices, will be supported.

5. Indicate on the Product Roadmap when all announced versions of Microsoft Office will be supported.

6. Indicate on the Product Roadmap when compliance with the following standards shall be available, including the level of the standard if applicable:

    a. Content Management Interoperability Services (CMIS)
    b. Business Process Modeling Notation (BPMN) 2.0 Business Process Modeling Notation (BPMN) 2.0
    c. DoD 5015.2

6.7 Migration

At the time this RFP is being distributed, DIWS 2 contains several applications that must be migrated from the Legacy DIWS environment to the DIWS 2 environment. These applications contain content (e.g., images), metadata used to index the content, and application-specific Structured Data that is stored in a number of database tables.

Although it is possible that the business managers may elect to have a subset of the content and data migrated from the Legacy DIWS to DIWS 2, the assumption should be that all content and data shall be migrated.

Additional content migration requirements specific to the content are located in:

- Appendix 6 Functional Requirements: Accounts Payable
- Appendix 7 Functional Requirements: Human Resources
- Appendix 8 Functional Requirements: Procurement
- Appendix 9 Legacy Migration

For the general content migration requirements, **DIWS 2 shall:**

1. Migrate existing structured content (e.g., data such as HR and AP records) from Legacy DIWS for use in DIWS 2.
2. Migrate existing unstructured content (e.g., images) from Legacy DIWS for use in DIWS 2.
3. Migrate existing Records retention information (e.g., last access, retention schedule) from Legacy DIWS for use.
4. Ensure all of the existing structured content (database records) for an application (e.g., HR or AP) is migrated.
5. Ensure all of the existing unstructured content (e.g., images and documents) for all applications (e.g., HR or AP) is migrated.
6. Perform quality assurance on all migrated records to ensure the correctness, completeness and other integrity of the migrated information.
7. Detect and correct data quality issues in existing structured content and unstructured content, working with MVA staff to suggest corrections.
8. Provide a configurable COTS tool, supplied by the Offeror at its own cost, for the movement, validation and verification of all information associated with migration.

9. Provide a repeatable process incorporating an iterative approach for performing the migration.
   - For the purpose of this requirement, it is recognized that migrations are often approached in an iterative manner with corrections and adjustments made to the migration rules that result in successive improvements and a reduction in errors with each iteration.
10. Provide tools to enable content from non-DIWS systems to be migrated into DIWS 2, as described in Appendix 9, Legacy Migration.
11. This requirement has been removed.
12. This requirement has been removed.

7. Response to Toolbox Requirements

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

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

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

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

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

In addition to completing the Toolbox response table below, Offerors shall complete the worksheets in the Excel spreadsheet (see Appendix 17 Offeror Response) that correspond to this Appendix.

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
3.1	Scanning	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tools software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
3.2	Capture	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tools software that you are proposing and how and when you would meet these requirements. b. Describe the hardware and software you are proposing for capturing content arriving via all mechanisms identified Section 3.2 Capture, Requirement 20.	
3.3	Incoming FTP/SFTP	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tools software that you are proposing and how and when you would meet these requirements. b. Describe the hardware and software you are proposing for capturing content arriving via incoming FTP/SFTP communications.	
3.4	Quality Assurance	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
3.5	Indexing	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tools software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
3.6	Release	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application software and tools that you are proposing and how and when you would meet these requirements.	
4.1	Content Creation	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tools software that you are proposing and how and when you would meet these requirements.	
4.2	Field Validation	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.3	Electronic Forms	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. b. Describe the hardware and software you are proposing for electronic forms functionality.	
4.4	Searching	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
4.5	Navigation	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.6	Redaction	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. b. Recognizing that automatic redaction may have limitations, describe the capabilities and practical effectiveness of the redaction tools you are proposing and the extent to which these can be used to redact the information identified in the various requirements. c. Describe the hardware and software you are proposing for automated redaction and that this hardware and software supports automated redaction.	
4.7	Workflow	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
4.8	Reports and Queries	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. b. Describe the hardware and software you are proposing for reports and queries.	
4.9	Administration	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.10	Self-Administration	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.11	Security and Privacy	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
4.12	Audit Trail	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. Where appropriate, cross reference your response with your response to audit requirements in Appendix 11 Technical. b. Explain how you will maintain an integrated audit trail between the ECM system and scanning/capture subsystem.	
4.13	Journaling	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.14	General Auditing and QA Auditing	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
4.15	Records Management and Legal Hold	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.1	Repository Management	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
5.2	Retrieval	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.3	Document Assembly	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.4	Publishing	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.5	Correspondence Management	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.6	Printing	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
5.7	Correspondence Tracking	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
6.1	Architecture	a. Provide a conceptual architecture diagram for your proposed solution. b. Provide a logical architecture diagram for your proposed solution. c. Provide a physical architecture diagram for your proposed solution. d. Provide the bill of materials for all environments of the implemented solution. If data migration is offered as a service, include the details on safeguards and mechanisms for transferring content between legacy environments, the hosted migration environment, and the DIWS 2 environments in the MVA data center. e. Provide the list of differences for the bill of materials if DIWS 2 is hosted on the Amazon Web Service cloud.	
6.2	Capacity	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. b. Provide your approach for automating the testing of the requirements contained in this section. c. Indicate how you will ensure the system is able to achieve the capacity requirements in this section. d. Indicate how you will achieve the system availability requirements.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
6.3	Performance	a. Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section when the system is loaded at the levels specified in Section 6.2 Capacity. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements. b. Provide your approach for automating the testing of the requirements contained in this section. c. Indicate how you will ensure the system is able to achieve the performance requirements in this section. d. Suggest comparable metrics for any metrics you are not able to capture, per Requirement 17. e. Indicate how you propose to automate the collection and reporting of the performance measurements/metrics.	
6.4	Integration	a. Provide a brief overview of how you will satisfies the requirements in this section. b. Discuss how you suggest ensuring content in the repository is free from viruses and other malware. For example, how are the threats posed for content that contains a zero-day virus that is stored in the repository? Even though the content was scanned at the time it was stored, the virus was missed because a signature file did not exist at that time. c. How do you suggest ensuring image files do not contain viruses? For example, renamed executables, viruses embedded in metadata, etc., that are often used in conjunction with other malware.	

Response Requirements **Appendix 10 DIWS 2 External Systems Integration**			
Appdx Ref	**Topic Title**	**Response Requirements**	**Page Limit**
6.5	Devices	Provide a brief overview of how your out-of-the-box application and tools satisfy the requirements in this section. Specifically identify all requirements in this section that are not met using the out-of-the-box application and tool software that you are proposing and how and when you would meet these requirements.	
6.6	Product Roadmap	a. Provide a brief overview of how you will satisfies the requirements in this section. b. Provide the requested Product Roadmap that identifies when the next two major releases of all prerequisite and requisite products shall be supported by the underlying product	
6.7	Migration	Provide a brief overview of how you will satisfies the requirements in this section. a. There is an expectation that migration tools will be included as part of the out-of-the-box application and that these tools will be leveraged to perform migrations in a repeatable manner.	
	Requirements not Met	The State assumes that the Contractor will meet all requirements described in Appendix 5 of the Task Order. Identify any areas that cannot be met and why these areas cannot be met.	