Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

Department of Buildings and General Services
Office of Purchasing & Contracting
133 State Street, 5th Floor | Montpelier VT 05633-8000
802-828-2211 phone |802-828-2222 fax
http://bgs.vermont.gov/purchasing

Agency of Administration

SEALED BID

REQUEST FOR PROPOSAL

Department of Public Safety (DPS) Computer Aided Dispatch and Records Management System (CAD RMS) Replacement

ISSUE DATE	**November 20, 2026**
BIDDERS CONFERENCE	**December, 1, 2026 – 2:00 (EST)**
JOIN:	**https://teams.microsoft.com/meet/2301542029121060p=zQq5sbvw4F1MqQkNdG**
MEETING ID:	**230 154 202 912 106 0**
PASSCODE:	**cD2tx7NQ**
QUESTIONS DUE	**December 7, 2026 – 4:00 (EST)**
RFP RESPONSES DUE BY	**December 30, 2026 – 4:30 PM (EST)**

PLEASE BE ADVISED THAT ALL NOTIFICATIONS, RELEASES, AND ADDENDUMS ASSOCIATED WITH THIS RFP WILL BE POSTED AT:

http://www.bgs.state.vt.us/pca/bids/bids.php

THE STATE WILL MAKE NO ATTEMPT TO CONTACT INTERESTED PARTIES WITH UPDATED INFORMATION. IT IS THE RESPONSIBILITY OF EACH BIDDER TO PERIODICALLY CHECK THE ABOVE WEBPAGEFOR ANY AND ALL NOTIFICATIONS, RELEASES AND ADDENDUMS ASSOCIATED WITH THIS RFP.

STATE CONTACT: **Kyle Emerson, State Purchasing Agent**

E-MAIL: **SOV.ThePathForward@vermont.gov**

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1. **OVERVIEW:**

1.1. **SCOPE AND BACKGROUND:** Through this Request for Proposal (RFP) the Department of Public Safety (DPS) (hereinafter the "State") is seeking to establish contracts with one or more companies that can provide a Computer Aided Dispatch and Records Management System (CAD RMS).

1.2. **CONTRACT PERIOD:** Any Contract(s) arising from this RFP will be for a period of 5 years following implementation. The State anticipates the start date for such contract(s) will be 06/01/2027.

1.3. **SINGLE POINT OF CONTACT:** All communications concerning this RFP are to be addressed in writing to the State Contact listed on the front page of this RFP. Actual or attempted contact with any other individual from the State concerning this RFP is strictly prohibited and may result in disqualification.

1.4. **BIDDERS' CONFERENCE:** A mandatory bidders' conference will be held remotely at the date and time indicated on the front page of this RFP.

1. If there is a remote bidders' conference, and call-in information is not provided on the front page of the RFP, all potential bidders must send an e-mail to the State Contact with Bidder's firm and contact info and shall then be provided call-in details.

1.5. **QUESTION AND ANSWER PERIOD:** Any bidder requiring clarification of any section of this RFP or wishing to comment on any requirement of the RFP must submit specific questions in writing no later than the deadline for question indicated on the first page of this RFP. Questions may be e-mailed to the point of contact on the front page of this RFP. Questions or comments not raised in writing on or before the last day of the question period are thereafter waived. At the close of the question period a copy of all questions or comments and the State's responses will be posted on the State's web site http://www.bgs.state.vt.us/pca/bids/bids.php . Every effort will be made to post this information as soon as possible after the question period ends, contingent on the number and complexity of the questions. All information provided by vendors during this process will be public and bidders shall not provide confidential information, except as described in 4.1 below.

1.6. **CHANGES TO THIS RFP:** Any modifications to this RFP will be made in writing by the State through the issuance of an Addendum to this RFP and posted online at http://www.bgs.state.vt.us/pca/bids/bids.php . Modifications from any other source are not to be considered.

2. **DETAILED REQUIREMENTS/DESIRED OUTCOMES:**

2.1. The State of Vermont is interested in obtaining bids to meet the following business need(s): an integrated, statewide Computer-Aided Dispatch and Records Management solution with API-first integration to partner agency systems, federal reporting, and E-911 for all participating agencies. The system will replace multiple more localized dispatch systems and help the Department meet federal compliance standards. In addition, the system will improve interoperability between various services in the state including, but not limited to, law enforcement, fire, EMS, dispatch centers and other partner state agencies.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Desired Outcome	Success Indicator
Establish a statewide, reliable, secure, and interoperable CAD/RMS solution per the intent of State of Vermont Legislative Act 78.	A statewide CAD/RMS solution in operation across participating dispatch centers and law enforcement agencies. The target date follows the Phase 1 schedule; FY31 is the current working assumption.
Modernize the CAD/RMS system with no operational gap in records management through the legacy system transition.	Records management available without interruption from the legacy contract expiration through cutover of the successor system; no unplanned RMS outage over four hours during the transition; officer-safety cautions and person history carried across the transition.
Maintain federal compliance (CJIS Security Policy, NIBRS, NERIS, and the dispatch-record obligations that feed NEMSIS) through and beyond the transition.	No federal compliance audit findings related to the modernization; multiple clean CJIS audits after cutover; the dispatch record delivered to the EMS reporting platforms inside the State submission window.
Improve inter-agency interoperability across dispatch centers, law enforcement, fire, EMS, and partner state agencies.	API-first integration with every named partner agency; a measurable drop in manual data exchange.

2.2. The State of Vermont seeks to achieve the following Business Value(s):

1. Customer Service Improvement: One statewide CAD RMS should allow emergency agencies and responders to act more quickly and with better real-time information and a reduction of manual data exchange.
2. Compliance: One statewide CAD RMS will allow state agencies and departments to meet legislative requirements
3. Risk Reduction: A unified CAD RMS will provide first responders with more timely and accurate information in emergency situations.
4. Risk Reduction: Maintain federal compliance (CJIS Security Policy, NIBRS, NERIS, and the dispatch-record obligations that feed NEMSIS) through and beyond the transition.

2.3. BUSINESS AND NONFUNCTIONAL REQUIREMENTS

The State's Business Requirements and Nonfunctional Requirements are provided with the Bidder Response Form. The Bidder must consider these Business Requirements and Nonfunctional Requirements (including any associated assumptions and acceptance criteria) as a baseline. The Bidder understands, expects, agrees, and accepts that the Business Requirements and Nonfunctional Requirements may evolve between the date of this RFP and any resulting draft Statement of Work or Contract as a result of iterative analysis performed by the State between the date of this RFP and the drafting of any resulting Statement of Work or

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Contract. The Bidder understands, expects, agrees, and accepts that the Business Requirements and Nonfunctional Requirements will evolve throughout the course of the project execution as (a) the needs of the State are refined and clarified through collaborative elicitation and analysis, and (b) the State gains an understanding of the capabilities and limitations of the Bidder's solution. Per Global Administrative Requirement GR-00011, the Bidder must collaborate with the State to elicit Business Requirements and Nonfunctional Requirements at sufficient detail to ensure the Completed Solution meets the needs of the State. Any significant change in scope must be managed through the Contract Change Management Process as detailed in Attachment A of the standard State of Vermont IT Contract Template.

2.4. Business Rules: The selected bidder will be required to identify, develop, and document all applicable business rules in accordance with the State of Vermont guidance and standards.

3. **GENERAL REQUIREMENTS:**

3.1. **PRICING:** Bidders must price the terms of this solicitation at their best pricing. Any and all costs that Bidder wishes the State to consider must be submitted for consideration. If applicable, all equipment pricing is to include F.O.B. delivery to the ordering facility. No request for extra delivery cost will be honored. All equipment shall be delivered assembled, serviced, and ready for immediate use, unless otherwise requested by the State.

1. Prices and/or rates shall remain firm for the initial term of the contract. The pricing policy submitted by Bidder must (i) be clearly structured, accountable, and auditable and (ii) cover the full spectrum of materials and/or services required.
2. **Cooperative Agreements**. Bidders that have been awarded similar contracts through a competitive bidding process with another state and/or cooperative are welcome to submit the pricing in response to this solicitation.

3.2. **STATEMENT OF RIGHTS:** The State shall have the authority to evaluate Responses and select the Bidder(s) as may be determined to be in the best interest of the State and consistent with the goals and performance requirements outlined in this RFP. The State of Vermont reserves the right to obtain clarification or additional information necessary to properly evaluate a proposal. Failure of bidder to respond to a request for additional information or clarification could result in rejection of that bidder's proposal. To secure a project that is deemed to be in the best interest of the State, the State reserves the right to accept or reject any and all bids, in whole or in part, with or without cause, and to waive technicalities in submissions. The State also reserves the right to make purchases outside of the awarded contracts where it is deemed in the best interest of the State.

1. **Best and Final Offer (BAFO).** At any time after submission of Responses and prior to the final selection of Bidder(s) for Contract negotiation or execution, the State may invite Bidder(s) to provide a BAFO. The state reserves the right to request BAFOs from only those Bidders that meet the minimum qualification requirements and/or have not been eliminated from consideration during the evaluation process.
2. **Presentation.** An in-person or webinar presentation by the Bidder may be required by the State if it will help the State's evaluation process. The State will factor information presented during presentations into the evaluation. Bidders will be responsible for all costs associated with providing the presentation.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

3.3. **CONFLICTS OF INTEREST:**

1. **Organizational Conflict of Interest (OCOI):** An OCOI arises when a bidder as a business entity has interests (for example, customers, partners, contracts) that could undermine, or reasonably be perceived to undermine, its faithful and unbiased performance of a contract with the State that may result from this solicitation.

2. **Personal Conflict of Interest (PCOI):** A PCOI arises when an interest held by an individual, agent or employee of a bidder could undermine, or reasonably be perceived to undermine, its faithful and unbiased performance of a contract with the State that may result from this solicitation.

3. **Requirements**: The State does not seek to contract with any individual or business entity having a conflict of interest which cannot be mitigated to the State's satisfaction. To ensure the State's awareness of actual, potential, or reasonably perceived PCOIs and OCOIs, bidders shall:

   a) Prior to submitting a proposal, conduct an internal review of its current affiliations and activities and identify actual, potential, or reasonably perceived PCOIs or OCOIs relative to a contract with the State that may result from this solicitation.
   b) Disclose in your proposal any actual or potential PCOI or OCOI or the existence of any facts that may cause a reasonably prudent person to perceive a PCOI or OCOI with respect to a contract with the State that may result from this solicitation. Disclose, also, any actions proposed to mitigate the PCOI or OCOI.

4. The State shall have sole discretion to determine whether a PCOI or OCOI can be mitigated to the State's satisfaction and may discuss the conflict with the bidder if and to the extent the State deems discussion necessary to its determination. The State reserves the right to (a) reject from further consideration any proposal having a PCOI or OCIO that cannot be mitigated to the State's full satisfaction and (b) terminate a contract upon discovery that a contractor failed to disclose facts pertaining to a PCOI or OCOI in its proposal, or otherwise misrepresented relevant information to the State.

3.4. **WORKER CLASSIFICATION COMPLIANCE REQUIREMENTS**: In accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), Bidders must comply with the following provisions and requirements.

1. Self Reporting: For bid amounts exceeding $250,000.00, Bidder shall complete the appropriate section in the attached Certificate of Compliance for purposes of self-reporting information relating to past violations, convictions, suspensions, and any other information related to past performance relative to coding and classification of workers. The State is requiring information on any violations that occurred in the previous 12 months.

2. Subcontractor Reporting: For bid amounts exceeding $250,000.00, Bidders are hereby notified that upon award of contract, and prior to contract execution, the State shall be provided with a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54). This requirement does not apply to subcontractors providing supplies only and no labor to the overall contract or project. This list MUST be updated and provided to the State as additional subcontractors are hired. A sample form is available online at http://bgs.vermont.gov/purchasing-contracting/forms. **The subcontractor reporting form is not required to be submitted with the bid response.**

3.5. **ADDITIONAL ASSURANCES REQUIRED BY FEDERAL OR STATE LAW**

The following additional assurances required under Federal or State regulations shall be incorporated into any Contract resulting from this RFP. Where CJIS Security Policy requirements and State of Vermont requirements address the same subject, the more stringent requirement shall apply.

3.5.1. CJIS Security Addendum (Required)

All Vendors performing work under a Contract resulting from this RFP shall comply with the CJIS Security Policy Addendum, including requirements governing physical security, personnel security, authentication, encryption, remote work limitations, and incident reporting.

3.5.2. Remote Work Requirements

All remote work must be performed within U.S. territory, consistent with CJIS Security policy requirements. VPNs utilized to allow a remote worker to perform work via a device physically located within the U.S. while working outside the U.S. are not allowed.

The Contract shall include:

- The CJIS Security Policy Addendum in its entirety.
- A signed CJIS Security Policy Addendum Certification for each assigned Contractor resource.

3.6. **EXECUTIVE ORDER 05-16: CLIMATE CHANGE CONSIDERATIONS IN STATE PROCUREMENTS**:

For bid amounts exceeding $25,000.00 Bidders are requested to complete the Climate Change Considerations in State Procurements Certification, which is included in the Certificate of Compliance for this RFP.

After consideration of all relevant factors, a bidder that demonstrates business practices that promote clean energy and address climate change as identified in the Certification, shall be given favorable consideration in the competitive bidding process. Such favorable consideration shall be consistent with and not supersede any preference given to resident bidders of the State and/or products raised or manufactured in the State, as explained in the Method of Award section. But, such favorable consideration shall not be employed if prohibited by law or other relevant authority or agreement.

3.7. **METHOD OF AWARD:** Awards will be made in the best interest of the State. The State may award one or more contracts and reserves the right to make additional awards to other compliant bidders at any time if such award is deemed to be in the best interest of

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

the State. All other considerations being equal, preference will be given first to resident bidders of the state and/or to products raised or manufactured in the state, and then to bidders who have practices that promote clean energy and address climate change, as identified in the applicable Certificate of Compliance.

1. **Evaluation Criteria:** Consideration shall be given to the Bidder's project approach and methodology, qualifications and experience, ability to provide the services within the defined timeline, cost, and/or success in completing similar projects, as applicable, and to the extent specified below.

Evaluation Factors	Total Points for this factor
Vendor Profile: Experience, Financial Strength, References	25%
Vendor Proposal / Solution, Response to the State's Functional and non-functional requirements, Maintenance and Support Services, Vendor Demonstration	40%
Implementation Services, Project Management Approach, and Technical Services	10%
Pricing, total cost, flexible pricing model, flexible terms, etc…	25%
Acceptance of State Terms and Conditions	Pass/Fail
Adherence to Mandatory Bidding Requirements	Pass/Fail

3.8. **CONTRACT NEGOTIATION**: Upon completion of the evaluation process, the State may select one or more bidders with which to negotiate a contract, based on the evaluation findings and other criteria deemed relevant for ensuring that the decision made is in the best interest of the State. In the event State is not successful in negotiating a contract with a selected bidder, the State reserves the option of negotiating with another bidder, or to end the proposal process entirely.

3.9. **COST OF PREPARATION:** Bidder shall be solely responsible for all expenses incurred in the preparation of a response to this RFP and shall be responsible for all expenses associated with any presentations or demonstrations associated with this request and/or any proposals made.

3.10. **CONTRACT TERMS:** The selected bidder(s) will be expected to sign a contract with the State, including the Standard Contract Form, Attachment C and Attachment D as attached to this RFP for reference.

3.11. **Business Registration.** To be awarded a contract by the State of Vermont a bidder (except an individual doing business in his/her own name) must be registered with the Vermont Secretary of State's office https://sos.vermont.gov/corporations/registration/and must obtain a Contractor's Business Account Number issued by the Vermont Department of Taxes http://tax.vermont.gov/ .

The contract will obligate the bidder to provide the services and/or products identified in its bid, at the prices listed.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

3.12. **Payment Terms.** Percentage discounts may be offered for prompt payments of invoices; however, such discounts must be in effect for a period of 30 days or more in order to be considered in making awards.

3.13. **Retainage.** In the discretion of the State, a contract resulting from this RFP may provide that the State withhold up to 20% percent of the total amount payable for some or all deliverables, such retainage to be payable upon satisfactory completion and State acceptance in accordance with the terms and conditions of the contract.

3.14. **Quality.** If applicable, all products provided under a contract with the State will be new and unused, unless otherwise stated. Factory seconds or remanufactured products will not be accepted unless specifically requested by the purchasing agency. All products provided by the contractor must meet all federal, state, and local standards for quality and safety requirements. Products not meeting these standards will be deemed unacceptable and returned to the contractor for credit at no charge to the State.

3.15. **DEMONSTRATION:** An in-person or webinar demonstration by the Bidder may be required by the State if it will help the State's evaluation process. The State will factor information presented during demonstrations into the evaluation. Bidder will be responsible for all costs associated with the providing the demonstration.

3.16. **INDEPENDENT REVIEW:** Certain State information technology projects require independent expert review as described under 3 V.S.A. § 3303(d). Such review, if applicable, will inform the State's decision to award any contract(s) resulting from this RFP.

4. **CONTENT AND FORMAT OF RESPONSES:** The content and format requirements listed below are the minimum requirements for State evaluation. These requirements are not intended to limit the content of a Bidder's proposal. Bidders may include additional information or offer alternative solutions for the State's consideration. However, the State discourages overly lengthy and costly proposals, and Bidders are advised to include only such information in their response as may be relevant to the requirements of this solicitation.

4.1. **Unsolicited Bidder-Confidential Information Prohibited.** Bidders are hereby expressly directed not to include any confidential information in their proposal submissions, except as specifically permitted below. By submitting a proposal in response to this RFP, vendors acknowledge and agree to abide by the terms and conditions outlined in this document, including the prohibition on submitting confidential information. This prohibition reduces the burden on the State while preventing vendor-confidential information from entering the public record.

4.2. **Disclosure under Public Records Act.** All information received by the State in response to this solicitation will become part of the contract file and subject to public disclosure in accordance with the State's Public Records Act, 1 V.S.A. § 315 et seq. The State may also choose to publicly post responses to this solicitation and the resulting agreement(s), following conclusion of this procurement process.

4.3. **Unsolicited Confidential Materials.** The State intends to redact or withhold only those confidential materials specifically requested below or in the Bidders Response Form attached to this RFP (if one is used). All other materials, including those marked as confidential by bidders, are subject to disclosure if requested under the Public Records Act, or public posting.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

4.4. **State Not Responsible for Disclosure of Unmarked Bidder-Confidential Information.** It is the sole responsibility of the bidder to ensure that, other than where specifically directed or permitted by this RFP and accordingly marked as described below, no information that should not be publicly disclosed is included in their proposal materials, including any 1) trade secrets or intellectual property, 2) proprietary financial or business information, 3) personal information, or 4) any other information that should not be disclosed to the public. For example, bidders should avoid including specific details of their proprietary technologies or methodologies that they consider confidential, and any references to previous client engagements should be presented in a manner that does not disclose the client's confidential information.

4.5. The bid should include a Cover Letter and Technical Response and Price Schedule.

4.6. **COVER LETTER:**

Exceptions to Contract Terms and Conditions. Bidders are expected to accept State terms, conditions, and templates as set forth in the sample contract attached to this RFP. By submitting a proposal in response to this RFP, bidders are confirming their concurrence unless, and then only to the extent bidder proposes exceptions in the Bidders Response Form attached to this RFP (if one is used) or otherwise in the cover letter to bidder's proposal. However, the State is not bound to accept any exceptions and taking such exceptions may cause a proposal to be not in the best interests of the State. If exceptions are not noted in the response to this RFP but raised during contract negotiations, the State reserves the right to cancel the negotiation if deemed to be in the best interests of the State.

4.7. **TECHNICAL RESPONSE.** In response to this RFP, a bidder shall:

1. Provide details concerning your form of business organization, company size and resources.
2. Describe your capabilities and particular experience relevant to the RFP requirements.
3. If you have experience working with the State of Vermont, identify all current or past State projects. Provide the name of the Vermont department or agency and the project title or a brief description of the work. Do not include references or statements from State of Vermont agencies or employees.
4. Identify the names of all subcontractors you intend to use, the portions of the work the subcontractors will perform, and address the background and experience of the subcontractor(s), in response to the questions described above in this section.

4.8. **REFERENCES.** Provide the names, addresses, and phone numbers of at least three companies with whom you have transacted similar business in the last 12 months. You must include contact names who can talk knowledgeably about performance. Do not list a State of Vermont agency or employee as a reference.

4.9. **REPORTING REQUIREMENTS:** Provide a sample of any reporting documentation that may be applicable to the Detailed Requirements of this RFP.

4.10. **PRICE SCHEDULE:** Bidders shall submit their pricing information in the Price Schedule attached to the RFP.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

4.11. **CERTIFICATE OF COMPLIANCE:** This form must be completed and submitted as part of the response for the proposal to be considered valid.

4.12. **STATE OF VERMONT BIDDER RESPONSE FORM:** This form must be completed and submitted as part of the response for the proposal to be considered valid. The State of Vermont Bidder Response Form provides a standard format and content for bidder proposals. When required, this form will prompt Bidders to supply the information required in the above RFP sections 4.6 through 4.10. Note: In addition to completing the State of Vermont Bidder Response Form, Bidders are required to provide the specific attachments that are described within the Bidder Response Form.

4.13. **REQUIRED CJIS COMPLIANCE ATTESTATIONS**

The proposal must include a formal attestation confirming that all proposed personnel will:

- Execute a CJIS Security Policy Addendum
- Complete a fingerprint-supported background check with the Vermont Crime Information Center (VCIC)
- Complete annual CJIS training using the State provided online training solution, CJIS Online.

5. **SUBMISSION INSTRUCTIONS:**

5.1. **CLOSING DATE:** Bids must be received by the State by the due date specified on the front page of this RFP. Late bids will not be considered.

1. The State may, for cause, issue an addendum to change the date and/or time when bids are due. If a change is made, the State will inform all bidders by posting at the webpage indicated on the front page of this RFP.
2. There will not be a public bid opening. However, the State will record the name, city and state for any and all bids received by the due date.

5.2. **ELECTRONIC BIDS ONLY:** All bids under this RFP must be submitted electronically in accordance with the submission requirements herein.

1. Electronic bids will be accepted via email submission to SOV.ThePathForward@vermont.gov. The subject line of the email submission must reference the Project Title as indicated on the front page of this RFP.

5.2.1.1. Bids must consist of a single email with a single, digitally searchable PDF attachment containing all components of the bid. Multiple emails and/or multiple attachments will not be accepted.

5.2.1.2. There is an attachment size limit of 40 MB. It is the Bidder's responsibility to compress the PDF file containing its bid if necessary in order to meet this size limitation. It is also the Bidder's responsibility to ensure that their own email system can send and receive messages up to this size.

6. **BID SUBMISSION CHECKLIST:**

- ✓ Cover Letter
- ✓ Redacted Technical Response, if applicable
- ✓ State of Vermont Bidder Response Form and Attachments

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

- Technical Response (included in Bidder Response Form)
- References (included in Bidder Response Form)
- Price Schedule (included in Bidder Response Form)
- Certificate of Compliance (included in Bidder Response Form)
- DPS_CAD-RMS Modernization_RFP_Functional Requirements-User Stories.pdf (included in Bidder Response Form)
- DPS_CAD-RMS Modernization_RFP_General Admin Requirements-GRQs.pdf (included in Bidder Response Form)
- DPS_CAD-RMS Modernization_RFP_Nonfunctional Requirements-NFRs.pdf (included in Bidder Response Form)

✓ CJIS Compliance Attestation

✓ AI Disclosure

7. **ATTACHMENTS:**

7.1. Standard State Contract with its associated attachments, including but not limited to, Contract Attachment C: Standard State Provisions for Contracts and Grants (February 13, 2026) and Attachment D: Information Technology System Implementation Terms and Conditions (December 9, 2025).

7.2. Attachment F: CJIS Security Policy Addendum

7.3. Attachment G: AI Usage Disclosure

7.4. Attachment H: RFP Glossary

7.5. Attachment I: Logical Architecture Diagram

7.6. Exhibit C: State of Vermont Bidder Response Form

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

STANDARD CONTRACT FOR TECHNOLOGY SERVICES

1. ***Parties.*** This is a contract for services between the State of Vermont, _____ (hereinafter called "State"), and _____, with a principal place of business in _____, (hereinafter called "Contractor"). Contractor's form of business organization is _____. It is Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, Contractor is required to have a Vermont Department of Taxes Business Account Number.

2. ***Subject Matter.*** The subject matter of this contract is services generally on the subject of _____. Detailed services to be provided by Contractor are described in Attachment A.

3. ***Maximum Amount.*** In consideration of the services to be performed by Contractor, the State agrees to pay Contractor, in accordance with the payment provisions specified in Attachment B, a sum not to exceed $_____.00.

4. ***Contract Term.*** The period of Contractor's performance shall begin on _____, 20__ and end on _____, 20__.

5. ***Prior Approvals.*** This Contract shall not be binding unless and until all requisite prior approvals have been obtained in accordance with current State law, bulletins, and interpretations.

6. ***Amendment.*** No changes, modifications, or amendments in the terms and conditions of this contract shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.

7. ***Termination for Convenience.*** This contract may be terminated by the State at any time by giving written notice at least thirty (30) days in advance. In such event, Contractor shall be paid under the terms of this contract for all services provided to and accepted by the State prior to the effective date of termination.

8. **Primary Contacts.** The Parties will keep and maintain current at all times a table of contacts and escalation contacts for this Agreement, that include primary points of contact and reporting structure to the executive leader which are presently as follows:

a. For the Contractor:

Name	Title	Phone	Email
	Primary Point of Contact		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

	President of Company		

b. For the State:

Name	Title	Phone	Email
Denise Reilly-Hughes	Secretary and CIO, Agency of Digital Services (ADS)		

9. ***Attachments***. This contract consists of ___ pages including the following attachments which are incorporated herein:

Attachment A – Statement of Work
- Exhibit 1 – State Technical and Functional Requirements
- Exhibit 2 – Preliminary Implementation Master Schedule
- Exhibit 3 – State Third Party Software
- Exhibit 4 – Contractor Software
- Exhibit 5 – State Service Level Terms

Attachment B – Payment Provisions
Attachment C – "Standard State Provisions for Contracts and Grants" a preprinted form (revision date 02/13/2026)
State of Vermont – Federal Terms Supplement (non-construction)
Attachment D – Other Terms and Conditions for Information Technology Contracts
Attachment D1 - Insurance Coverage
CJIS Terms of Use
FBI CJIS Security Addendum
Attachment __ – [OTHER DEPARTMENT ATTACHMENTS, AS APPLICABLE]

10. ***Order of Precedence***. Any ambiguity, conflict or inconsistency between the documents comprising this contract shall be resolved according to the following order of precedence:

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1) Standard Contract
2) CJIS Terms of Use
3) FBI CJIS Security Addendum
4) Attachment D1 Insurance Coverage
5) Attachment C (Standard State Provisions for Contracts and Grants)
6) State of Vermont – Federal Terms Supplement (non-construction)
7) Attachment D IT System Implementation Terms
8) Attachment A with Exhibits
9) Attachment B
10) List other attachments as applicable

11. Business Associate Agreement. If the State determines that the Contractor will create, receive, maintain or transmit Protected Health Information on behalf of a HIPAA covered entity, including EMS agencies or hospitals, the State's Business Associate Agreement will be added to this Contract by amendment and will take precedence immediately above Attachment C. The Contractor agrees to execute it without change and at no additional cost.

WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT

By the State of Vermont:	By the Contractor:
Date: _____	Date: _____
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT A
SPECIFICATIONS OF WORK TO BE PERFORMED

1. PURPOSE

This Contract sets forth the terms and conditions under which Contractor agrees to provide to the State with a [web-based,] Contractor-supported _____ (the "Solution"). The Solution shall _____.

The Contractor shall provide [development and design services, project and operations management, support and maintenance, consulting, training, engineering and application development , monitoring, support, backup and recovery, change management, technology updates and upgrades and other professional services as described herein] (individually and collectively referred to herein as the "Services"), as necessary for the State's productive use of the Solution as further set forth in this Contract. This Contract specifies the obligations of each party with additional provisions detailed in the attached Attachments and Exhibits.

1.1 EXECUTIVE OVERVIEW OF SERVICES. Provide brief description of solutions being procured and it's use at the State.

2. EXISTING SYSTEMS.

[DESCRIBE]

3. OBJECTIVE

This Contract identifies the tasks required by each party to implement and support the Solution through the following major activities: [development of project management planning documentation; requirements collection and validation, Solution design, data migration, configuration, integration and testing; deployment and training; operations, support, and maintenance services], all as detailed herein.

The project will be executed in phases as described herein.

The successful outcome of the project is defined by the following:

- completed in accordance with this Contract and applicable project management planning documentation;
- Resolution of all material functional and operational deficiencies prior to deployment in the production environment;
- completed within budget;
- configured to meet all specified requirements and needs of the State;
- the Solution meets and adheres to all requirements and timeframes set forth in service level terms set forth herein;
- the Solution is fully documented, including but not limited to requirements specifications, architecture, design, configuration, operational environment and user manuals; and
- trained State staff and stakeholders.

4. PERIOD OF INSTALLATION AND IMPLEMENTATION AND TRAINING

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

The period of installation and implementation and training shall not exceed _____ months from the date of this Contract. Support and maintenance shall begin [upon Solution deployment] and shall continue through the Contract Term as the same may be extended by the parties.

5. DEFINITIONS. Capitalized terms used in this Contract not specifically defined in the text shall have the following meanings:

(a) **"Certificate of Acceptance"** means written certification, delivered to Contractor and signed by an authorized representative of the State, stating that any Defects in a particular Phase or the Solution discovered after implementation and testing have been corrected as required under this Contract, and that the Phase complies in all material respects with all of the applicable Requirements.

(b) **"Certificate of Completion" means** written certification, delivered to the State and signed by an authorized representative of Contractor, stating that any Defects in a particular Phase or the Solution discovered after implementation, testing and Acceptance have been corrected as required under this Contract, and that the Phase or Solution complies in all material respects with all of the applicable Solution Requirements. The State must provide written acceptance to Contractor of any and all Certificates of Completion for them to become effective.

(c) "**Contractor Personnel**" means and refers to Contractor's employees and employees of Contractor's permitted subcontractors or permitted agents assigned by Contractor to perform Services under this Contract.

(d) **"Defect"** means any failure by the Solution or any Phase or component thereof to conform in any material respect with applicable Requirements.

(e) **"Defect Correction"** means either a modification or addition that, when made or added to the Solution, establishes material conformity of the Solution to the applicable Requirements, or a procedure or routine that, when observed in the regular operation of the Solution, eliminates the practical adverse effect on the State of such nonconformity.

(f) "**Documentation**" means any and all descriptions and specifications of the Requirements included herein or created or developed hereunder, operational, functional and supervisory reference guides, manuals and instructive materials, in whatever form and regardless of the media on which it may be contained, stored or transmitted, which is developed, prepared, used or otherwise available from Contractor and/or Contractor's suppliers, in connection with and applicable to the provision, use, operation and support of the Services hereunder. Documentation shall be sufficient to enable State personnel to understand, operate, use, access, support, maintain, update and modify Services, notwithstanding that Contractor is or may be responsible for any or all of the foregoing obligations. Documentation shall also include all standards applicable to the Services, including those applicable to: (i) Contractor for its own comparable items or services; (ii) the State for its own comparable items or services; and (iii) such standards and guidelines as the parties mutually agree apply to the Services involved.

(g) "**Final Acceptance**" means the issuance of Certificate of Acceptance executed by the

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

State which specifies the mutually agreed upon Go Live Date for the Solution.

(h) "**Facilities**" means the physical premises, locations and operations owned or leased by the State (a "State Facility") or the Contractor (a "Contractor Facility"), and from or through which the Contractor and/or its permitted contractors will provide any Services.

(i) **"Go Live Date."** The date that the all or any part of the entire Solution is first available for use by the State in an operational, non-test environment, utilizing actual production data.

(j) "**Phases."** A particular portion of the Solution, as set forth in the Implementation Master Schedule or as may be modified in accordance with this Contract. Unless modified by written agreement of the parties, the five project Phases are [Solution Definition and Design, Requirements Gathering, Customization, Deployment, Training and Maintenance and Support].

(k) "**Requirements**" means the State's baseline Functional and Technical Requirements attached as Exhibit 1 to Attachment A of this Contract.

(l) "**Service Level**" means the specific level of performance Contractor is required to comply with and adhere to in providing the Services in conformity with the Requirements, consistent with the criteria and parameters specified in this Contract. Service Level Terms are set forth in Exhibit ___ within Attachment A to this Contract.

6. PROJECT MANAGEMENT

The scope of work as detailed below describes the services, deliverables and key assumptions. Contractor will develop an overall project schedule that details the tasks, timelines, and deliverables for the fully integrated solution.

6.1. CONTRACTOR PROJECT MANAGEMENT AND SUPPORT

6.1.1 CONTRACTOR'S PROJECT MANAGER

Contractor will designate an individual to serve as the "**Contractor Project Manager**" who will: (i) be a senior employee within Contractor's organization, with the information, authority and resources available to properly discharge the responsibilities required hereunder; (ii) serve as primary point of contact and the single-point of accountability and responsibility for all Contract-related questions and issues and the provision of Services by Contractor; (iii) have day-to-day responsibility for, and authority to manage, State customer satisfaction; (iv) devote full time and dedicated efforts to managing and coordinating the Services; and (v) be located at State Facilities or such other appropriate location as Contractor and the State may mutually agree.

Contractor's Project Manager shall be responsible for all tasks necessary to manage, oversee, and ensure success of the project. These tasks include documenting requirements, developing and updating project plans, assigning staff, scheduling meetings, developing and publishing status reports, addressing project issues, risks, and change orders, and preparing presentations for the State.

Contractor's project manager shall be responsible for the successful delivery of all Contractor tasks and subtasks defined in the Project Management Plan (as defined herein). Progress will be monitored and plans adjusted, as necessary, in project status meetings. The Project Management

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Plan deliverables (for both State and Contractor tasks) shall be updated by the Contractor, subject to review and approval of the State, and reports printed for each status meeting.

Contractor's project manager shall be responsible for developing and implementing the following project management documentation:

Deliverable	Description	Update Frequency
Project Charter	The Project Charter provides basic information about the project. It includes a: Scope Statement (what's in and out of scope); list of Project Deliverables; high level Project Timeline; Key Roles & Responsibilities; known Risks, Assumptions and/or Constraints. It should be signed off on by the State.	Once unless there are changes
Project Management Plan	The Project Management Plan will dictate specifics on how the Contractor Project Manager will administer the project and will include the following documentation: 1. Change Management Plan (will dictate how changes will be handled including any Service level terms on over/under estimates) 2. Communication Management Plan (will dictate what will be communicated, to who, and how often) 3. Requirements Management Plan (will dictate the approach that the requirements will be gathered, approved, and maintained) 4. Human Resources Management Plan (will dictate what resources will be assigned to the project, for how long, under what allocation, who they report to, and how to handle changes to the resource plan) 5. Procurement Management Plan (will dictate how the vendor(s) will interact with the project and expectations regarding vendor relations with State resources) 6. Quality Management Plan (will dictate the quality controls over the work being done on the project as well as determine Key Performance Indicators – this document is not limited to deliverables) 7. Risk and Issues Management Plan (will dictate how risks and issues will be managed over the course of the project) 8. Scope Management Plan (will dictate how the scope will be maintained to prevent "scope creep")	

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Formal Acceptance Criteria	Criteria that establishes what the acceptance and rejection criteria of each document on this list.	
Formal Acceptance Sign Off	Obtain sign-off at the completion of each project deliverable as defined by the formal acceptance criteria.	
Change Requests	Formal document which outlines any changes to the Contract scope, schedule, budget, and resources.	
Change Requests Log	Tracks the specific change requests approved and their impact to the project scope, budget and schedule.	
Budget Log	Outlines original Contract costs by deliverable with billed and paid-to-date information.	
Risk Log	A log of all risks (opened or closed) that could impact the project. Risks should be outlined by their impact and their potential to occur. All risks should have an owner.	
Issue/Action Items/Decision Log	A Log of open and resolved/completed Issues. Issues should be outlined by their impact, owner, date of occurrence, and remediation strategy.	
Decision Log	A log of all decisions made over the course of the project. Decisions should have a date and name of decider.	
Requirements Documents	Finalized list of the project requirements to be approved by the State. The approach is dictated by the Requirements Management Plan (see Project Management Plan), and can include: • Stated requirements document (SRD): The SRD contains current state process flows, user stories, and business rules and states the business need at a high level. • Business requirements document (BRD): The BRD contains a medium level of requirements as well as required metrics of project success. • Functional requirements document (FRD): The FRD contains detailed requirements that can be handed off to the Contractor for execution.	
Test Plans	A description of the testing approach, participants, sequence of testing and testing preparations	Once
Test Cases & Results	The specific test cases to be tested and the testing results. Test Cases tie back to the project requirements (to ensure each one has been met).	Create once then update with Results

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Implementation Master Schedule	The IMS outlines how the project will go-live and will include a mini-project plan for the exact events that need to occur assigned to the resources that need to do them and the timeframe for when they need to get done. (See Section 4.4 for more detail.)	Once per implementation
Project Status Reports	Provides an update on the project health, accomplishments, upcoming tasks, risks and significant issues. The Status Report and the project color being report shall be developed in consultation with the State business lead and State project manager, as set forth in greater detail in Section 4.2.2.	Weekly
Project Phase Audit/Gate Check	At the end of each Phase, the Contractor Project Manager shall submit an audit of all deliverables and milestones achieved during the Phase to the State Project manager for review.	Once per phase.
Meeting Agenda/ Minutes	All scheduled meetings will have an agenda and minutes. The minutes shall contain risk issues, action items, and decision logs. Minutes shall be transcribed over to the main logs.	Per occurrence
End of Project Metrics	These are metrics that reflect how well the project was performed. Metrics will be outlined in the Quality Management Plan	
Lessons Learned	A compilation of the lessons learned having 20/20 hindsight. Lessons learned shall be delivered in an Excel template and collected from each of the State and Contractor project team members to get a full 360 degree view of the project in retrospect.	Once
Closeout Report	This report will include all the lessons learned, project metrics, and a summary of the project's implementation and outcome in operation.	Once

Contractor shall use State templates for the foregoing, unless otherwise approved by the State. The State Project Manager shall be responsible for the review and acceptance of project management documentation.

Contractor's project manager shall assist the State's project manager (upon request) in creating materials for periodic presentations to State project sponsors and key stakeholders. Contractor's project manager may be required to present information to, and answer questions from, State stakeholders at these presentations.

6.1.2 PROJECT MANAGEMENT AND SUPPORT

The Contractor will apply PMI (Project Management Institute's PMBOK) principles to ensure on-time and within-budget delivery of the Solution, while meeting all of the Requirements in this Contract. The State will approve all project management methods and tools used during the project. These project management methods and tools are considered project deliverables.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

6.1.3 KEY PROJECT STAFF

Contractor will perform and support the Services consistent with this Contract and the Solution Requirements. Contractor Personnel will be properly educated, trained and qualified for the Services they are to perform and Contractor will put appropriate training in place to meet initial and ongoing training requirements of Contractor Personnel assigned to perform Services.

(a) Contractor shall be responsible, at its own cost and expense, for any and all recruitment, hiring, Contractor-specific training, education and orientation for all Contractor Personnel assigned or to be assigned to perform Services or support the Requirements.

(b) All Contractor Personnel, in addition to any Contractor security policies and procedures, shall be required to comply with the security requirements in this Contract

(c) Contractor shall conduct its hiring process in compliance with all applicable Federal and State laws to include, but not be limited to, anti-discrimination laws.

(i) **Eligibility for Employment:** Contractor shall verify that all prospective employees are eligible for employment in the United States.

(ii) **Criminal Records:** Contractor or an agent of Contractor shall perform criminal background checks on all prospective employees utilizing a national criminal database acceptable to the State. Before any Contractor Personnel begin work on the Services x) such background check shall have returned a “no record” result or, y) to the extent that the result revealed that a felony record or records exist for a given individual, the associated conviction(s) shall be unrelated to the work to be performed as specified under the Equal Employment Opportunities Commission’s EEOC Enforcement Guidance regarding the employment of convicted felons issued April 25, 2012. Contractor shall provide the State with notice of proposed Contractor Personnel with felony or misdemeanor convictions that involve a crime against a person; a crime involving the use or misuse of computer network; a crime involving weapons, explosives or arson; a crime involving trade secret/proprietary information; a crime involving theft, dishonesty, embezzlement, breach of fiduciary duty, identity theft, or other financial-related crimes; a felony conviction for drug possession; or a crime involving the distribution or trafficking of illegal drugs and/or controlled substances.

(d) All Contractor Personnel providing or assigned to provide Services or otherwise in a position to obtain or have access to State Information, shall execute a non-disclosure agreement in a form acceptable to the State.

(e) The timing for transfer, reassignment or replacement of Contractor Personnel will be coordinated with requirements for timing and other elements of the Services so as to maintain continuity in the performance of the Services and avoid interruption or disruption to the Services or any failures to maintain Service Levels.

Contractor shall assign the following Contractor staff (“Key Project Staff”), to meet the Requirements of this Contract:

[INSERT]

Contractor will cause the Contractor Personnel filling the Key Project Staff positions to devote full time and dedicated effort to the provision of the Services and the achievement of Service Levels required for the Services, unless a lesser allocation during certain Project Phases may be agreed in writing.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

6.1.5 KEY PROJECT STAFF CHANGES
Contractor shall not change the project assignment of _____, _____, and _____ for the period of project implementation. Contractor shall not change other members of Key Project Staff without providing the State written justification, a comprehensive transition plan and obtaining prior written approval of the State. State approvals for replacement of Key Project Staff will not be unreasonably withheld.

The replacement of Key Project Staff shall have comparable or greater skills and applied experience than being replaced and be subject to reference and background checks described above. If Contractor removes Key Project Staff for any reason without the State's approval, Contractor agrees to replace the new Key Project Staff member if performance is unacceptable to State and provide the first thirty (30) days of a replacement resource with equivalent skill at no charge.

Notwithstanding the foregoing, the State acknowledges that Key Project Staff may become unavailable due to termination of employment for any reason, through disability or death, illness, or through leave of absence such as FMLA or National Guard duty for example. In such circumstances, Contractor shall promptly notify the State in writing of the impending or actual departure of any Key Personnel and of the qualifications and identity of proposed replacement Key Project Staff. The State has the right to reasonably disapprove of any replacement Key Project Staff.

6.1.6 CONTROL OF CONTRACTOR PERSONNEL**.** Contractor shall be fully responsible for the management, compensation, and performance of all Contractor Personnel, and the filing of any and all returns and reports and the withholding and/or payment of all applicable federal, State, and local wage tax, or employment-related taxes, including, but not limited to, income taxes, gross receipt taxes, taxes measured by income, social security taxes, and unemployment taxes for Contractor and Contractor's employees. Notwithstanding the foregoing, Contractor's employees shall adhere to the State's policies and procedures, of which Contractor is made aware while on State Premises, and shall behave and perform in a professional manner. The State, may, in its reasonable discretion, require Contractor to replace any Contractor Personnel, including but not limited to Key Project Staff, working hereunder who does not adhere to, behave, and perform consistent with the State's policies and procedures, or otherwise engages in unprofessional or unethical conduct, or abuses any illegal substance or alcohol, or engages in illegal activities or consistently underperforms. The State shall provide written notice to Contractor of the requirement of replacement, or with whom there are irresolvable personality conflicts. Contractor shall use reasonable efforts to promptly and expeditiously replace Key Project Staff and replace all other personnel within fifteen (15) business days of receipt of the written notice unless otherwise mutually agreed. The State's right to request replacement of Contractor personnel hereunder relates solely to the removal of individuals from work on this Contract with the State and does not create an employment relationship. Nothing in this Contract authorizes the State to direct the Contractor's termination of the employment of any individual.

6.1.7 CONTRACTOR THIRD PARTY CONTRACTS**.** The State acknowledges and understands that Contractor will enter into third party contracts with the following Contractor subcontractors: (i) _____ for _____; (ii) _____ for _____; and (iii) _____ for the performance of Services hereunder. Contractor shall deliver a copy of all such third party contracts to the State for review

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

upon request. The State hereby consents to the use by Contractor of these subcontractors, provided however that any such consent is not deemed acceptance of the terms of any subcontracts by the State.

6.2. PROJECT PLANNING

The State and Contractor Project Managers will arrange for kick-off dates and procedures for managing the project – such as reporting status and resolving issues. This will provide an opportunity to introduce all key members of the project teams and walk through the project management plan and key milestones.

6.2.1. MEETING PROTOCOLS

For regular weekly project status meetings, Contractor's Project Manager shall provide a meeting agenda and any handouts at least one business day in advance of the scheduled meeting.

6.2.2. PROJECT DOCUMENT STORAGE

The Contractor will establish a SharePoint site, or some other collaboration mechanism, that is accessible to the Contractor and the State. This will provide a common area for Contractor's project documents, artifacts, and deliverables. Access to all SharePoint sites (or other medium of collaboration) and all project material contained therein shall be delivered to the State upon completion of the project.

6.2.3. STATUS REPORTS

Contractor's Project Manager shall provide project documentation and collaboration to meet the State's vendor reporting requirements. If requested, the Contractor shall use the State's Status Report template. If no template is provided to the Contractor, the status information shall include, at a minimum: all planned tasks accomplished for the reporting period planned tasks that are incomplete, or behind schedule in the previous week (with reasons given for those behind schedule); all tasks planned for the upcoming two weeks; an updated status of tasks (entered into the Master Project Work Plan and attached to the status report – e.g., percent completed, resources assigned to tasks, etc.); and the status of any corrective actions undertaken. The report will also contain items such as the current status of the project's technical progress and contractual obligations; achievements to date; risk management activities; unresolved issues; requirements to resolve unresolved issues; action items; problems; installation and maintenance results; and significant changes to Contractor's organization or method of operation, to the project management team, or to the deliverable schedule, where applicable. For all project services performed on a time and materials basis, as provided herein, the Contractor shall also provide details on staff hours, cost per activity, all expenditures and a summary of services performed for the reporting period.

The State Project Manager and Contractor's Project Manager will come to agreement on the exact format of the project documentation and collaboration reports, at or before the project kick-off meeting.

Each report shall include a project dashboard at the top outlining the overall status of the project in terms of the standard triple constraint: cost, time, resources (using a legend or icon of green, yellow, and red based upon the following definitions):

- Green – on track to deliver committed scope by committed deadline with committed resources/funding.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

- Yellow – not on track to deliver committed scope by committed deadline with committed resources/funding, but have a plan to get back to green.
- Red – not on track and currently do not have a plan to get back to green. Need project management intervention or assistance.

In the event of yellow or red overall project status, there should be a specific task(s) and/or issue(s) identified as yellow or red which are the root cause of the overall project status being yellow or red. These items shall be presented in sufficient detail to determine the root-cause. The Status Report shall provide a link to the Risks and Issues Log for more detail.

The report shall include a budget section outlining original contract costs by deliverable with billed and paid-to-date information by deliverable and in total.

6.3 IMPLEMENTATION MASTER SCHEDULE

The Contractor has compiled a preliminary "baseline" implementation master schedule ("IMS") using the best available knowledge at the time of Contract signing which is attached to this Attachment A as Exhibit 2. The Contractor shall update the IMS after execution of this Contract during the Project Development as required pursuant to the terms herein (e.g., updated tasks and task descriptions, updated meeting dates, updated resource assignments, updated milestone dates). Any such changes shall be communicated in writing by the Contractor to the State Contract Manager by executing a new or revised IMS or other documentation acceptable to the State. Such changes are subject to State review and approval. The parties shall work together to implement the IMS changes in accordance with the terms of this Contract; provided, however, in no event shall revisions to the IMS be deemed to amend this Contract. Changes to project scope, term or maximum amount shall require a Contract amendment.

The IMS is an ongoing tool for anticipating and tracking changes to expectations for all project tasks, deliverables and milestones. The complete IMS is an integrated plan – that is, it includes actions and deliverables from all project areas – both Contractor and State. The complete IMS, which includes the detailed tasks and milestones, shall reside in [Microsoft Project (.mpp) format (Version 2007 or higher)] and will be shared in the ongoing communication meetings to discuss changes. State shall sign off on all deliverables from each Phase of the IMS before subsequent phase work is initiated. Once sign off is complete, Contractor and State will assess readiness to proceed with next phase.

7. SCOPE OF SERVICES.

7.1 DESCRIPTION OF SERVICES. Contractor agrees to provide and shall perform the Services described herein in accordance with and subject to the terms and conditions set forth in this Contract.

7.2 **Project Major Phases** **[DESCRIBE PROJECT PHASES AND DELIVERABLES FOR EACH PHASE; THIS SECTION SHOULD INCLUDE PAYMENT MILESTONES WHICH ARE THEN REITERATED IN ATTACHMENT B WITH PAYMENT AMOUNTS]**

The Contractor shall, at a minimum, provide State access to a [web-based] Solution that meets the tools and functionality requirements of the State set forth in Exhibit 1 to this Attachment A. Contractor shall use system development and configuration control methodologies and the

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

desirable sequence of project major Phases as described herein. Estimated dates in the following table shall be finalized in the IMS as described in Section 6.3, "Implementation Master Schedule."

PHASE	ESTIMATED DATES	PHASE DESCRIPTION
[Initiation]		Kick-off meeting, Planning and preparation of project management planning documentation.
[Requirements Gathering]		Contractor performs necessary requirements gathering to finalize functional and technical requirements and identify gaps between State requirements and Solution capabilities.
[Implementation]		Contractor installs and configures the Solution in a Test environment.
[Testing]		State subject matter experts perform Solution testing in in a test (not live) environment accordance with Contractor-developed Test plans.
[Training]		Contractor performs training of State personnel (train the trainer or train the user).
[Legacy Data Migration]		Contractor shall perform all necessary legacy data migrations using State-approved migration plan and data mapping templates.
[Deployment]		Contractor implements the tested and State-approved Solution in the production environment for additional State testing and Go-Live.
[Post-Implementation Support]		Contractor to provide Post Implementation Support.

7.3. **State-Caused Delays.** Contractor acknowledges that the State may not be able to meet the time frames specified in an IMS or that the State may determine that it is necessary to delay and/or modify the timing and sequencing of the implementation as provided in the IMS. While the State is committed to the project and shall use reasonable efforts to provide staff and resources necessary to satisfy all such time frames, the State shall not be held responsible or deemed in default for any delays in Solution implementation provided the State uses its reasonable efforts to accomplish its designated responsibilities and obligations as set forth in the IMS. In addition, the State may, at its option, delay implementation and installation of the Solution, or any part thereof. Notwithstanding any provision to the contrary, if the State Significantly Delays implementation of the Solution, either party may make a Change Request in accordance with Section 10, "Change Order Process," and, if required, an amendment to this Contract. Contractor agrees to adjust the IMS and Payment Milestones deadlines to take into account any State-caused delays; provided, however, that Contractor shall continue to perform any and all activities not affected by such State-

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

caused delay. In the event the State's adjustment to the IMS causes Contractor scheduling conflicts or personnel unavailability, the State and Contractor shall prepare a revised mutually agreeable IMS which may delay the commencement and completion dates of the project and shall take into consideration the readjusted time frames and any necessary resequencing of the activities. Such readjustment, rescheduling or modification of the Project shall be at no additional cost to the State if the delays are less than or equal to thirty (30) days.

For purposes of this Section, a "Significant Delay" shall mean any delay that in itself will cause a slippage of thirty (30) calendar days or more in a Go Live date.

7.4 **Third Party Resources**. From time to time State may request that Contractor obtain and provide to the State, at the State's expense, third party Resources related to the Services but outside the scope of what Contractor is then obligated to provide hereunder, including the benefit of any volume purchasing discounts, pricing or terms available to the State or its supplier. Contractor shall notify the State at the time of any such request of any relationships Contractor may have with such suppliers that may be of benefit to the State in this respect. To the extent that State may have a more favorable relationship with any third party supplier, upon notice from State, Contractor agrees to consider such Resources from State's designated supplier. Contractor will not add an administrative fee or other markup to any third party Resources it procures on behalf of or for the benefit of State and the Services provided hereunder.

7.5 **State Third Party Software.** A list of all Third Party Software licensed by the State for purposes of Contractor's performance of the Services is attached to this Attachment A as Exhibit 3. Contractor will assume operational and financial responsibility for such Third Party Software and any related maintenance obligations to the same extent as if Contractor were the licensee of such Third Party Software. Contractor will cease use of such Third Party Software upon expiration or termination of this Contract.

8. ACCEPTANCE

8.1. **Acceptance Testing by the State Following Implementation.** After Contractor provides written notice to the State that it has completed a Phase of the Solution, the State shall, in accordance with the Formal Acceptance Criteria agreed by the parties, and with full cooperation and assistance from Contractor, conduct all such inspections and tests of the Phase as the State may deem necessary or appropriate to determine whether any Defects exist in the Phase as implemented and whether the Phase as installed materially complies with all of the Installation Test Specifications and Phase specifications as set forth in the Requirements and detailed IMS. Such inspections and tests shall be over a duration mutually agreed upon by the State and Contractor, per Phase, from the date a notice of completion is issued (the "Acceptance Period"). Contractor shall correct all Defects during the Acceptance Period, demonstrate to the State that correction of such Defects has been made, and after so demonstrating correction, shall issue to the State a written Certificate of Completion indicating that no Defects are known to exist in the Phase and/or Solution. The State shall be deemed to have accepted and approved the particular Phase or Solution only upon the State's delivery to Contractor of a signed, written Certificate of Acceptance indicating that the Phase or the Solution, as the case may be, as completed, materially performs in accordance with the Requirements.

If at the end of the Acceptance Period, the State has not issued a signed Certificate of Acceptance

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

to Contractor for that Phase or the Solution, the State may, in its sole discretion, extend the Acceptance Period; provided, however, that the State shall respond within five (5) business days of a written request by Contractor issued after the end of the original Acceptance Period to provide Contractor with the State's status of approval or disapproval for that Phase or the Solution. Any rejection must be in writing and specify the reason for the rejection and must be based upon the continued existence of a Defect in the Phase or Solution or failure of the Phase or Solution to materially perform in accordance with the Requirements. The Certificate of Acceptance shall not be unreasonably withheld by the State. If a Certificate of Acceptance for a Phase or the Solution is signed and delivered by the State, Contractor shall sign said Certificate, with both parties receiving a copy thereof.

9. THIRD PARTY COOPERATION

The State may hire other independent contractors as it may require to assist with the project. Contractor will cooperate with the State and the third party, including provision of: (i) written Documentation requested by the State; (ii) commercially reasonable assistance and support services to such third party; and (iii) reasonable access to Contractor as necessary for such third parties to perform their work. The State shall use reasonable efforts to require such third parties to comply with Contractor's reasonable requirements regarding confidentiality, operations, standards, and security. Contractor shall support and maintain such third party work product, provided the service provider complies with any Documentation applicable to Contractor in respect of the Services involved.

10. CONTRACT/PROJECT CHANGE ORDER PROCESS

[NOTE: AS EXPLAINED HEREIN, THIS SECTION IS NOT APPLICABLE FOR ANY AND EVERY RFP AND SHOULD BE DELETED AS APPROPRIATE]

For projects involving IT Implementation services, where frequent and/or multiple minor changes to the project schedule or deliverables are anticipated, the following process may be utilized to effectuate such minor changes without undue project delays ("Change Orders").
Changes to a Contract during its term may incur additional costs and possible delays relative to the project schedule, or may result in less cost to the State (for example, the State decides it no longer needs a deliverable in whole or part) or less effort on the part of a selected vendor. A Change Order shall define the effort involved in implementing the change, the total cost or associated savings to the State, of implementing the change, and the effect, if any, of implementing the change on the project schedule.

Any change that alters the essential terms of the original contract, including any change that expands or decreases the statement of work, the contract duration, the payment terms and/or the contract maximum amount, shall require a Contract Amendment in accordance with State contracting policies and procedures. Under no circumstances may a Change Order be used where a Contract Amendment is otherwise required pursuant to the Contract Amendments, Approval and Execution process set forth in State Administrative Bulletin 3.5.

Change Orders will be developed jointly and every effort will be made to adhere to the approved Project Plan. The Project Manager for the State and the Project Manager for a Contractor will decide whether a Change Order is necessary. If a Change Order is necessary, the Project Manager for requesting party will prepare a Change Order Request detailing the impacts on

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

scope, schedule, deliverables, resources, and cost. The Change Order Request must be submitted to the non-requesting party for review. The non-requesting party will make its best efforts to either approve or deny the Change Order in writing within (10) business days. In no event shall any delay in the approval or denial of a Change Request constitute a deemed approval by the State.

The State will not pay for the effort involved in developing a Change Order. The Contractor shall bear the cost of estimating the cost or savings, time, and Contractor resources required to implement all Change Order Requests forthcoming from the State during the course of the Project.

All Change Orders that are mutually agreed upon must:

a. be in writing and describe, with specific reference to the applicable section(s) of the contract, what is being added, deleted or otherwise modified;
b. be signed by both the State and the Contractor;
c. include the original contract number and a sequential Change Order number;
d. include Contractor certifications regarding Taxes, Debarment, and Child Support, as detailed in State Administrative Bulletin 3.5, Section XIII(A)(c); and
e. be consolidated into a formal Contract Amendment whenever an amendment would otherwise be required by State Administrative Bulletin 3.5.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT B
PAYMENT PROVISIONS

The maximum dollar amount payable under this contract is not intended as any form of a guaranteed amount. The Contractor will be paid for products or services actually delivered or performed, as specified in Attachment A, up to the maximum allowable amount specified on page 1 of this contract.

1. Prior to commencement of work and release of any payments, Contractor shall submit to the State:
    a. a certificate of insurance consistent with the requirements set forth in Attachment C, Section 8 (Insurance), and with any additional requirements for insurance as may be set forth elsewhere in this contract; and
    b. a current IRS Form W-9 (signed within the last six months).
2. Payment terms are **Net 30** days from the date the State receives an error-free invoice with all necessary and complete supporting documentation.
3. Contractor shall submit detailed invoices itemizing all work performed during the invoice period, including the dates of service, rates of pay, hours of work performed, and any other information and/or documentation appropriate and sufficient to substantiate the amount invoiced for payment by the State. All invoices must include the Contract # for this contract. Invoices will be submitted within (5) five business days of the date the invoice was created.
4. Invoices shall be submitted to the State at the following address: _____
5. Contractor shall submit invoices to the State upon State Acceptance of a deliverable in accordance with the schedule for delivered products, or rates for services performed set forth below:

- Specify Milestone Deliverable Payment Schedule, retainage (if any) and release point(s).
- Hardware/Software
- Monthly Services
- Other Included Services
- Optional Services
- Withheld Amount

6. EXPENSES: The fee for services shall be inclusive of Contractor expenses.

    RETAINAGE: At the discretion of the State, _____% of the total amount payable will be withheld from invoice payments until satisfactory completion of deliverables or final acceptance The State will notify the Contractor when acceptable to provide the State with a separate invoice for the withheld retainage.

DESCRIBE how retainage will be structured.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT C: STANDARD STATE PROVISIONS FOR CONTRACTS AND GRANTS

REVISED FEBRUARY 13, 2026

1. Definitions: For purposes of this Attachment, "Party" shall mean the Contractor, Grantee, or Subrecipient, with whom the State of Vermont is executing this Agreement and consistent with the form of the Agreement. "Agreement" shall mean the specific contract or grant to which this form is attached.

2. Entire Agreement: This Agreement, whether in the form of a contract, State funded grant, or Federally-funded grant, represents the entire agreement between the parties on the subject matter. All prior agreements, representations, statements, negotiations, and understandings shall have no effect. Where an authorized individual is either required to click-through or otherwise accept, or made subject to, any electronic terms and conditions to use or access any product or service provided hereunder, such terms and conditions are not binding and shall have no force or effect. Further, any terms and conditions of Party's invoice, acknowledgment, confirmation, or similar document, shall not apply, and any such terms and conditions on any such document are objected to without need of further notice or objection.

3. Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial: This Agreement will be governed by the laws of the State of Vermont without resort to conflict of laws principles. Any action or proceeding brought by either the State or the Party in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. The Party irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. The Party agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State regarding its performance under this Agreement. Party agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial. 4. Sovereign Immunity: The State reserves all immunities, defenses, rights, or actions arising out of the State's sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State's immunities, defenses, rights, or actions shall be implied or otherwise deemed to exist by reason of the State's entry into this Agreement.

5. No Employee Benefits For Party: The Party understands that the State will not provide any individual retirement benefits, group life insurance, group health and dental insurance, vacation or sick leave, workers compensation or other benefits or services available to State employees, nor will the State withhold any state or Federal taxes except as required under applicable tax laws, which shall be determined in advance of execution of the Agreement. The Party understands that all tax returns required by the Internal Revenue Code and the State of Vermont, including but not limited to income, withholding, sales and use, and rooms and meals, must be filed by the Party, and information as to Agreement income will be provided by the State of Vermont to the Internal Revenue Service and the Vermont Department of Taxes.

6. Independence: The Party will act in an independent capacity and not as officers or employees of the State.

7. Defense and Indemnity: A. The Party shall defend the State and its officers and employees against all third-party claims or suits arising in whole or in part from any act or omission of the Party or of any agent of the Party in connection with the performance of this Agreement. The State

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

shall notify the Party in the event of any such claim or suit, and the Party shall immediately retain counsel and otherwise provide a complete defense against the entire claim or suit. The State retains the right to participate at its own expense in the defense of any claim. The State shall have the right to approve all proposed settlements of such claims or suits. B. After a final judgment or settlement, the Party may request recoupment of specific defense costs and may file suit in Washington Superior Court requesting recoupment. The Party shall be entitled to recoup costs only upon a showing that such costs were entirely unrelated to the defense of any claim arising from an act or omission of the Party in connection with the performance of this Agreement. C. The Party shall indemnify the State and its officers and employees if the State, its officers, or employees become legally obligated to pay any damages or losses arising from any act or omission of the Party or an agent of the Party in connection with the performance of this Agreement. D. Notwithstanding any contrary language anywhere, in no event shall the terms of this Agreement or any document furnished by the Party in connection with its performance under this Agreement obligate the State to (1) defend or indemnify the Party or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of the Party or any third party.

8. Insurance: During the term of this Agreement, Party, at its expense, shall maintain in full force and effect the insurance coverages set forth in the Vermont State Insurance Specification in effect at the time of incorporation of this Attachment C into this Agreement. The terms of the Vermont State Insurance Specification are hereby incorporated by reference into this Attachment C as if fully set forth herein. A copy of the Vermont State Insurance Specification is available at: https://aoa.vermont.gov/Risk-Claims-COI.

9. Reliance by the State on Representations: All payments by the State under this Agreement will be made in reliance upon the accuracy of all representations made by the Party in accordance with this Agreement, including but not limited to bills, invoices, progress reports, and other proofs of work.

10. False Claims Act: Any liability to the State under the Vermont False Claims Act (32 V.S.A. § 630 et seq.) shall not be limited notwithstanding any agreement of the State to otherwise limit Party's liability.

11. Whistleblower Protections: The Party shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority, or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, the Party shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to the Party or its agents prior to reporting to any governmental entity and/or the public.

12. Use and Protection of State Information:

A. As between the State and Party, "State Data" includes all data received, obtained, or generated by the Party in connection with performance under this Agreement. Party acknowledges that certain State Data to which the Party may have access may contain information that is deemed confidential by the State, or which is otherwise confidential by law, rule, or practice, or otherwise exempt from disclosure under the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. ("Confidential State Data").

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

B. With respect to State Data, Party shall: i. take reasonable precautions for its protection; ii. not rent, sell, publish, share, or otherwise appropriate it; and iii. upon termination of this Agreement for any reason, Party shall dispose of or retain State Data if and to the extent required by this Agreement, law, or regulation, or otherwise requested in writing by the State.

C. With respect to Confidential State Data, Party shall: i. strictly maintain its confidentiality; ii. not collect, access, use, or disclose it except as necessary to provide services to the State under this Agreement; iii. provide at a minimum the same care to avoid disclosure or unauthorized use as it provides to protect its own similar confidential and proprietary information; iv. implement and maintain administrative, technical, and physical safeguards and controls to protect against any anticipated threats or hazards or unauthorized access or use; v. promptly notify the State of any request or demand by any court, governmental agency or other person asserting a demand or request for Confidential State Data so that the State may seek an appropriate protective order; and vi. upon termination of this Agreement for any reason, and except as necessary to comply with subsection B.iii above in this section, return or destroy all Confidential State Data remaining in its possession or control.

D. If Party is provided or accesses, creates, collects, processes, receives, stores, or transmits Confidential State Data in any electronic form or media, Party shall utilize: i. ii. industry-standard firewall protection; multi-factor authentication controls; iii. encryption of electronic Confidential State Data while in transit and at rest; iv. measures to ensure that the State Data shall not be altered without the prior written consent of the State; v. measures to protect against destruction, loss, or damage of State Data due to potential environmental hazards, such as fire and water damage; vi. training to implement the information security measures; and vii. monitoring of the security of any portions of the Party's systems that are used in the provision of the services against intrusion.

E. No Confidential State Data received, obtained, or generated by the Party in connection with performance under this Agreement shall be processed, transmitted, stored, or transferred by any means outside the United States, except with the express written permission of the State.

F. Party shall notify the State within twenty-four hours after becoming aware of any unauthorized destruction, loss, alteration, disclosure of, or access to, any State Data.

G. State of Vermont Cybersecurity Standard Update: Party confirms that all products and services provided to or for the use of the State under this Agreement shall be in compliance with State of Vermont Cybersecurity Standard Update in effect at the time of incorporation of this Attachment C into this Agreement. The State of Vermont Cybersecurity Standard Update prohibits the use of certain branded products in State information systems or any vendor system, and a copy is available at: https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards and-directives.

H. In addition to the requirements of this Section 12, Party shall comply with any additional requirements regarding the protection of data that may be included in this Agreement or required by law or regulation.

13. Records Available for Audit: The Party shall maintain all records pertaining to performance under this Agreement. "Records" means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired by the Party in the performance of this Agreement. Records produced or acquired in a machine-readable electronic format shall be

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

maintained in that format. The records described shall be made available at reasonable times during the period of this Agreement and for three years thereafter or for any period required by law for inspection by any authorized representatives of the State or Federal Government. If any litigation, claim, or audit is started before the expiration of the three-year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

14. Nondiscrimination: A. Fair Employment Practices and Americans with Disabilities Act: Party agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable, and shall include this provision in all subcontracts for work performed in Vermont. Party shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by the Party under this Agreement. B. IT Accessibility Standards: Party acknowledges and agrees that any digital products, services, and content provided under this Agreement, whether supporting State programs or intended for the State's use, must adhere to the State's accessibility standards and guidelines as established by Section 504 of the Rehabilitation Act of 1973 and Title II of the Americans with Disabilities Act of 1990 (28 CFR Part 35) (hereinafter, for purposes of this subsection B, the “Rule”). The Rule requires communication and content on web platforms and mobile applications to meet or exceed specific success criteria and conformance requirements. The Rule applies to websites, software applications, electronic reports and output documentation, and training delivered in electronic formats (including, but not limited to, documents, videos, and webinars), and other digital content. Information concerning the Rule and the State’s Universal Digital Accessibility resources are available on the State’s Communications and Marketing Office website at: https://cmo.vermont.gov. i. Party warrants that the software, products, services, or subscriptions provided under this Agreement, whether supporting State programs or intended for the State's use (hereinafter, for purposes of this subsection B, “Products”) comply with the Rule and agrees to defend, indemnify, and hold harmless the State against any claims related to a Product’s non-compliance with the Rule. ii. When updates or upgrades are made to the Products available through this Agreement, the Party agrees: a) to develop functionality that supports accessibility in conformance with the Rule and, if any issues arise due to nonconformance with the Rule, to provide alternative solutions upon request at no additional cost to the State; and b) to document how the changes will impact or improve the Product’s accessibility and usability. This documentation, upon request, must be provided to the State in advance of the update or upgrade, occurring within an agreed timeframe sufficient for the State to review the changes and either approve them or request a remediation plan from the Party. iii. If agreed-upon updates fail to improve the Product’s accessibility or usability as planned, such failure shall be a material breach of this Agreement.

15. Offset: The State may offset any sums which the Party owes the State against any sums due the Party under this Agreement; provided, however, that any offset of amounts due the State of Vermont as taxes shall be in accordance with the procedures more specifically provided in 32 V.S.A. § 3113.

16. Taxes Due to the State: Party certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, the Party is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.

17. Taxation of Purchases: All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

18. Child Support: (Only applicable if the Party is a natural person, not a corporation or partnership.) Party states that, as of the date this Agreement is signed, Party is not under an obligation to pay child support or is in good standing with respect to or in full compliance with a plan to pay any and all child support payable under a support order. Party makes this statement with regard to support owed to any and all children residing in Vermont. In addition, if the Party is a resident of Vermont, Party makes this statement with regard to support owed to any and all children residing in any other state or territory of the United States.

19. Sub-Agreements: Party shall not assign, subcontract, or subgrant the performance of this Agreement or any portion thereof to any other Party without the prior written approval of the State. Party shall be responsible and liable to the State for all acts or omissions of subcontractors and any other person performing work under this Agreement pursuant to an agreement with Party or any subcontractor. In the case this Agreement is a contract with a total cost in excess of $250,000, the Party shall provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont and Grants Recovery and Reinvestment Act of 2009 (Act No. 54), as amended by Section 17 of Act No. 142 (2010) and by Section 6 of Act No. 50 (2011). Party shall include the following provisions of this Attachment C in all subcontracts for work performed solely for the State of Vermont and subcontracts for work performed in the State of Vermont: Section 10 ("False Claims Act"); Section 11 ("Whistleblower Protections"); Section 12 ("Confidentiality and Protection of State Information"); Section 14 ("Fair Employment Practices and Americans with Disabilities Act"); Section 16 ("Taxes Due the State"); Section 18 ("Child Support"); Section 20 ("No Gifts or Gratuities"); Section 22 ("Certification Regarding Debarment"); Section 30 ("State Facilities"); and Section 32.A ("Certification Regarding Use of State Funds").

20. No Gifts or Gratuities: Party shall not give title or possession of anything of substantial value (including property, currency, travel, and/or education programs) to any officer or employee of the State during the term of this Agreement.

21. Regulation of Hydrofluorocarbons: Party confirms that all products provided to or for the use of the State under this Agreement shall not contain hydrofluorocarbons, as prohibited under 10 V.S.A. § 586.

22. Certification Regarding Debarment: Party certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Party nor Party's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible, or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds. Party further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Party is not presently debarred, suspended, nor named on the State's Debarment List at: https://bgs.vermont.gov/purchasing-contracting/debarment.

23. Conflict of Interest: A. Organizational Conflict of Interest (OCOI): An OCOI arises when the Party as a business entity has an interest (for example, customers, partners, contracts) that could undermine, or reasonably be perceived to undermine, its faithful and unbiased performance of this Agreement. B. Personal Conflict of Interest (PCOI): A PCOI arises when an interest held by an agent or employee of the Party could undermine, or reasonably be perceived to undermine, the faithful and unbiased performance of this Agreement. C. Requirements: Party shall not have PCOIs or OCOI's with respect to this Agreement nor with respect to any other agreement(s) it

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

may hold with the State. To ensure that PCOIs and OCOIs do not exist, the Party shall: i. Conduct an internal review of its current affiliations and activities and employees and agents and identify actual, potential, or reasonably perceived PCOIs or OCOIs relative to this Agreement. ii. Maintain effective oversight to verify compliance with PCOI and OCOI prohibitions. iii. Prevent PCOIs, including not assigning or allowing an employee to perform any role or task under this Agreement for which the Party has identified a PCOI. iv. Inform employees and agents of their obligation to disclose PCOIs and to comply with the confidentiality provisions and any non disclosure agreement required by this Agreement. v. Make an immediate and full disclosure, in writing, to the State point of contact for this Agreement of any actual or potential PCOI or OCOI or the existence of any facts that may cause a reasonably prudent person to perceive a PCOI or OCOI with respect to this Agreement. D. Remedies: i. In the event the State determines that a PCOI or OCOI exists, the State will discuss the matter with the Party to determine whether the PCOI or OCOI can be mitigated to the State's satisfaction. ii. If the State does not deem mitigation practicable, the State may terminate all or a portion of this Agreement for default or pursue such other remedies as may be permitted by law or this Agreement. iii. If Party fails to disclose facts pertaining to the existence of a potential or actual PCOI or misrepresents relevant information to the State, the State may terminate this Agreement for default or pursue such other remedies as may be permitted by law or this Agreement.

24. Vermont Public Records Act: Party acknowledges and agrees that this Agreement, any and all information obtained by the State from the Party in connection with this Agreement, and any obligations of the State to maintain the confidentiality of information are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

25. Force Majeure: Neither the State nor the Party shall be liable to the other for any failure or delay of performance of any obligations under this Agreement to the extent such failure or delay shall have been wholly or principally caused by acts or events beyond its reasonable control rendering performance illegal or impossible (excluding strikes or lockouts) ("Force Majeure"). Where Force Majeure is asserted, the nonperforming party must prove that it made all reasonable efforts to remove, eliminate or minimize such cause of delay or damages, diligently pursued performance of its obligations under this Agreement, substantially fulfilled all non excused obligations, and timely notified the other party of the likelihood or actual occurrence of an event described in this paragraph.

26. Marketing: Party shall not use the State's logo or otherwise refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

27. Termination: A. Non-Appropriation: If this Agreement extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support this Agreement, the State may cancel this Agreement at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. In the case that this Agreement is funded in whole or in part by Federal funds, and in the event Federal funds become unavailable or reduced, the State may suspend or cancel this Agreement immediately, and the State shall have no obligation to pay Party from State revenues. B. Termination for Cause: Either party may terminate this Agreement if a party materially breaches its obligations under this Agreement, and such breach is not cured within thirty (30) days after delivery of the non breaching party's notice or such longer time as the non-breaching party may specify in the notice. C. Termination Assistance: Upon nearing the end

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

of the final term or termination of this Agreement, without respect to cause, the Party shall take all reasonable and prudent measures to facilitate any transition required by the State. All State property, tangible and intangible, shall be returned to the State upon demand at no additional cost to the State in a format acceptable to the State.

28. Continuity of Performance: In the event of a dispute between the Party and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

29. No Implied Waiver of Remedies: Either party's delay or failure to exercise any right, power, or remedy under this Agreement shall not impair any such right, power, or remedy, or be construed as a waiver of any such right, power, or remedy. All waivers must be in writing.

30. State Facilities: If the State makes space available to the Party in any State facility during the term of this Agreement for purposes of the Party's performance under this Agreement, the Party shall only use the space in accordance with all policies and procedures governing access to, and use of, State facilities, which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

31. Requirements Pertaining Only to Federal Grants and Subrecipient Agreements: If this Agreement is a grant that is funded in whole or in part by Federal funds: A. Requirement to Have a Single Audit: The Subrecipient will complete the Subrecipient Annual Report annually within 45 days after its fiscal year end, informing the State of Vermont whether or not a Single Audit is required for the prior fiscal year. If a Single Audit is required, the Subrecipient will submit a copy of the audit report to the Federal Audit Clearinghouse within nine months. If a single audit is not required, only the Subrecipient Annual Report is required. A Single Audit is required if the subrecipient expends $1,000,000 or more in Federal assistance during its fiscal year and must be conducted in accordance with 2 CFR Chapter I, Chapter II, Part 200, Subpart F. The Subrecipient Annual Report is required to be submitted within 45 days, whether or not a Single Audit is required. B. Internal Controls: In accordance with 2 CFR Part II, §200.303, the Party must establish and maintain effective internal control over the Federal award to provide reasonable assurance that the Party is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission. C. Mandatory Disclosures: In accordance with 2 CFR Part II, §200.113, Party must disclose, in a timely manner, in writing to the State, all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award. Failure to make required disclosures may result in the imposition of sanctions which may include disallowance of costs incurred, withholding of payments, termination of the Agreement, suspension/debarment, etc.

32. Requirements Pertaining Only to State-Funded Grants: A. Certification Regarding Use of State Funds: If Party is an employer and this Agreement is a State-funded grant in excess of $1,000, Party certifies that none of these State funds will be used to interfere with or restrain the exercise of Party's employee's rights with respect to unionization. B. Good Standing Certification (Act 154 of 2016): If this Agreement is a State-funded grant, Party hereby represents: (i) that it has signed and provided to the State the form prescribed by the Secretary of Administration for purposes of certifying that it is in good standing (as provided in Section 13(a)(2) of Act 154) with the Agency

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

of Natural Resources and the Agency of Agriculture, Food and Markets, or otherwise explaining the circumstances surrounding the inability to so certify; and (ii) that it will comply with the requirements stated therein.

(End of Standard State Provisions)

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT D
INFORMATION TECHNOLOGY SYSTEM IMPLEMENTATION
TERMS AND CONDITIONS (REV. 12/09/2025)

1. **NO SUBSEQUENT, UNILATERAL MODIFICATION OF TERMS BY CONTRACTOR**

Notwithstanding any other provision or other unilateral license terms which may be issued by Contractor during the Term of this Contract, and irrespective of whether any such provisions have been proposed prior to or after the issuance of an order for the products and services being purchased by the State, as applicable, the components of which are licensed under the Contractor Documents, or the fact that such other agreement may be affixed to or accompany the products and services being purchased by the State, as applicable, upon delivery, the terms and conditions set forth herein shall supersede and govern licensing and delivery of all products and services hereunder.

2. **TERM OF CONTRACTOR'S DOCUMENTS; PAYMENT TERMS**

Contractor acknowledges and agrees that, to the extent a Contractor Document provides for alternate term or termination provisions, including automatic renewals, such sections shall be waived and shall have no force and effect. All Contractor Documents shall run concurrently with the term of this Contract; provided, however, to the extent the State has purchased a perpetual license to use the Contractor's software, hardware or other services, such license shall remain in place unless expressly terminated in accordance with the terms of this Contract. Contractor acknowledges and agrees that, to the extent a Contractor Document provides for payment terms which differ from the payment terms set forth in Attachment B, such sections shall be waived and shall have no force and effect and the terms in Attachment B shall govern.

3. **OWNERSHIP AND LICENSE IN DELIVERABLES**

3.1 Contractor Intellectual Property.

As between the parties, and subject to the terms and conditions of this Contract, Contractor and its third-party suppliers will retain ownership of all intellectual property rights in the [System], and any and all derivative works made to the [System] or any part thereof, as well as all Work Product provided to the State ("**Contractor Proprietary Technology**"). The State acquires no rights to Contractor Proprietary Technology except for the licensed interests granted under this Contract. The term "**Work Product**" means all other materials, reports, manuals, visual aids, documentation, ideas, concepts, techniques, inventions, processes, or works of authorship developed, provided or created by Contractor or its employees or contractors during the course of performing work for the State (excluding any State Data or derivative works thereof and excluding any output from the [System] generated by the State's use of the [System], including without limitation, reports, graphs, charts and modified State Data, but expressly including any form templates of such reports, graphs or charts by themselves that do not include the State Data).

Title, ownership rights, and all Intellectual Property Rights in and to the [System] will remain the sole property of Contractor or its suppliers. The State acknowledges that the source code is not covered by any license hereunder and will not be provided by Contractor. Except as set forth in this Contract, no right or implied license or right of any kind is granted to the State regarding the [System] or any part thereof. Nothing in this Contract confers upon either party any right to use the other party's trade names and trademarks, except for permitted license use in accordance with this Contract. All use of such marks by either party will inure to the benefit of the owner of such marks, use of which will be subject to specifications controlled by the owner.

3.2 State Intellectual Property; User Name

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

The State shall retain all right, title and interest in and to (i) all content and all property, data and information furnished by or on behalf of the State or any agency, commission or board thereof, and to all information that is created under this Contract, including, but not limited to, all data that is generated under this Contract as a result of the use by Contractor, the State or any third party of any technology systems or knowledge bases that are developed for the State and used by Contractor hereunder, and all other rights, tangible or intangible; and (ii) all State trademarks, trade names, logos and other State identifiers, Internet uniform resource locators, State user name or names, Internet addresses and e-mail addresses obtained or developed pursuant to this Contract (collectively, "**State Intellectual Property**").

Contractor may not collect, access or use State Intellectual Property for any purpose other than as specified in this Contract. Upon expiration or termination of this Contract, Contractor shall return or destroy all State Intellectual Property and all copies thereof, and Contractor shall have no further right or license to such State Intellectual Property.

Contractor acquires no rights or licenses, including, without limitation, intellectual property rights or licenses, to use State Intellectual Property for its own purposes. In no event shall the Contractor claim any security interest in State Intellectual Property.

4. **CONFIDENTIALITY AND NON-DISCLOSURE; SECURITY BREACH REPORTING**

1. For purposes of this Contract, confidential information will not include information or material which (a) enters the public domain (other than as a result of a breach of this Contract); (b) was in the receiving party's possession prior to its receipt from the disclosing party; (c) is independently developed by the receiving party without the use of confidential information; (d) is obtained by the receiving party from a third party under no obligation of confidentiality to the disclosing party; or (e) is not exempt from disclosure under applicable State law.
2. **Confidentiality of Contractor Information.** The Contractor acknowledges and agrees that this Contract and any and all Contractor information obtained by the State in connection with the performance of this Contract are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq. The State will not disclose information for which a reasonable claim of exemption can be made pursuant to 1 V.S.A. § 317(c), including, but not limited to, trade secrets, proprietary information or financial information, including any formulae, plan, pattern, process, tool, mechanism, compound, procedure, production data, or compilation of information which is not patented, which is known only to the Contractor, and which gives the Contractor an opportunity to obtain business advantage over competitors who do not know it or use it.

The State shall immediately notify Contractor of any request made under the Access to Public Records Act, or any request or demand by any court, governmental agency or other person asserting a demand or request for Contractor information. Contractor may, in its discretion, seek an appropriate protective order, or otherwise defend any right it may have to maintain the confidentiality of such information under applicable State law within three business days of the State's receipt of any such request. Contractor agrees that it will not make any claim against the State if the State makes available to the public any information in accordance with the Access to Public Records Act or in response to a binding order from a court or governmental body or agency compelling its production. Contractor shall indemnify the State for any costs or expenses incurred by the State, including, but not limited to, attorneys' fees awarded in accordance with 1 V.S.A. § 320, in connection with any action brought in connection with Contractor's attempts to prevent or unreasonably delay public disclosure of Contractor's information if a final decision of a court of competent jurisdiction determines that the State improperly withheld such information and that the improper withholding was based on Contractor's attempts to prevent public disclosure of Contractor's information.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

The State agrees that (a) it will use the Contractor information only as may be necessary in the course of performing duties, receiving services or exercising rights under this Contract; (b) it will provide at a minimum the same care to avoid disclosure or unauthorized use of Contractor information as it provides to protect its own similar confidential and proprietary information; (c) except as required by the Access to Records Act, it will not disclose such information orally or in writing to any third party unless that third party is subject to a written confidentiality agreement that contains restrictions and safeguards at least as restrictive as those contained in this Contract; (d) it will take all reasonable precautions to protect the Contractor's information; and (e) it will not otherwise appropriate such information to its own use or to the use of any other person or entity.

Contractor may affix an appropriate legend to Contractor information that is provided under this Contract to reflect the Contractor's determination that any such information is a trade secret, proprietary information or financial information at time of delivery or disclosure.

5. **SECURITY OF STATE INFORMATION**

1. **Security Standards.** To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor represents and warrants that it has implemented and it shall maintain during the term of this Contract the highest industry standard administrative, technical, and physical safeguards and controls consistent with the latest version of NIST *Special Publication 800-53* and *Federal Information Processing Standards Publication* 200 and designed to (i) ensure the security and confidentiality of State Data; (ii) protect against any anticipated security threats or hazards to the security or integrity of the State Data; and (iii) protect against unauthorized access to or use of State Data. Such measures shall include at a minimum: (1) access controls on information systems, including controls to authenticate and permit access to State Data only to authorized individuals and controls to prevent the Contractor employees from providing State Data to unauthorized individuals who may seek to obtain this information (whether through fraudulent means or otherwise); (2) industry-standard firewall protection; (3) encryption of electronic State Data while in transit from the Contractor networks to external networks; (4) measures to store in a secure fashion all State Data which shall include, but not be limited to, encryption at rest and multiple levels of authentication; (5) dual control procedures, segregation of duties, and pre-employment criminal background checks for employees with responsibilities for or access to State Data; (6) measures to ensure that the State Data shall not be altered or corrupted without the prior written consent of the State; (7) measures to protect against destruction, loss or damage of State Data due to potential environmental hazards, such as fire and water damage; (8) staff training to implement the information security measures; and (9) monitoring of the security of any portions of the Contractor systems that are used in the provision of the services against intrusion on a twenty-four (24) hour a day basis.
2. **Security Breach Notice and Reporting.** The Contractor shall have policies and procedures in place for the effective management of Security Breaches, as defined below, which shall be made available to the State upon request.

In addition to the requirements set forth in any applicable Business Associate Agreement as may be attached to this Contract, in the event of any actual security breach or reasonable belief of an actual security breach the Contractor either suffers or learns of that either compromises or could compromise State Data (a "Security Breach"), the Contractor shall notify the State within 24 hours of its discovery. Contractor shall immediately determine the nature and extent of the Security Breach, contain the incident by stopping the unauthorized practice, recover records, shut down the system that was breached, revoke access and/or correct weaknesses in physical

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

security. Contractor shall report to the State: (i) the nature of the Security Breach; (ii) the State Data used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and (v) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. The Contractor shall provide such other information, including a written report, as reasonably requested by the State. Contractor shall analyze and document the incident and provide all notices required by applicable law.
In accordance with Section 9 V.S.A. §2435(b)(3), the Contractor shall notify the Office of the Attorney General, or, if applicable, Vermont Department of Financial Regulation ("DFR"), within fourteen (14) business days of the Contractor's discovery of the Security Breach. The notice shall provide a preliminary description of the breach. The foregoing notice requirement shall be included in the subcontracts of any of Contractor's subcontractors, affiliates or agents which may be "data collectors" hereunder.
The Contractor agrees to fully cooperate with the State and assume responsibility at its own expense for the following, to be determined in the sole discretion of the State: (i) notice to affected consumers if the State determines it to be appropriate under the circumstances of any particular Security Breach, in a form recommended by the AGO; and (ii) investigation and remediation associated with a Security Breach, including but not limited to, outside investigation, forensics, counsel, crisis management and credit monitoring, in the sole determination of the State.
The Contractor agrees to comply with all applicable laws, as such laws may be amended from time to time (including, but not limited to, Chapter 62 of Title 9 of the Vermont Statutes and all applicable State and federal laws, rules or regulations) that require notification in the event of unauthorized release of personally-identifiable information or other event requiring notification.
In addition to any other indemnification obligations in this Contract, the Contractor shall fully indemnify and save harmless the State from any costs, loss or damage to the State resulting from a Security Breach or the unauthorized disclosure of State Data by the Contractor, its officers, agents, employees, and subcontractors.

3. **Security Policies**. To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor will have an information security policy that protects its systems and processes and media that may contain State Data from internal and external security threats and State Data from unauthorized disclosure, and will have provided a copy of such policy to the State. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.
4. **Operations Security**. To the extent the Contractor or its subcontractors, affiliates or agents handles, collects, stores, disseminates or otherwise deals with State Data, the Contractor shall cause an SSAE 18 SOC 2 Type 2 audit report to be conducted annually. The audit results and the Contractor's plan for addressing or resolution of the audit results shall be shared with the State within sixty (60) days of the Contractor's receipt of the audit results. Further, on an annual basis, within 90 days of the end of the Contractor's fiscal year, the Contractor shall transmit its annual audited financial statements to the State.
5. **Redundant Back-Up.** The Contractor shall maintain a fully redundant backup data center geographically separated from its main data center that maintains near realtime replication of data from the main data center. The Contractor's back-up policies shall be made available to the State upon request. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

6. **Vulnerability Testing.** The Contractor shall run quarterly vulnerability assessments and promptly report results to the State. Contractor shall remediate all critical issues within 15 days, all high issues within 30 days, all medium issues within 60 days and low issues within 90 days. Contractor shall obtain written State approval for any exceptions. Once remediation is complete, Contractor shall re-perform the test.

6. CONTRACTOR'S REPRESENTATIONS AND WARRANTIES

1. **General Representations and Warranties.** The Contractor represents, warrants and covenants that:

i. The Contractor has all requisite power and authority to execute, deliver and perform its obligations under this Contract and the execution, delivery and performance of this Contract by the Contractor has been duly authorized by the Contractor.

ii. There is no outstanding litigation, arbitrated matter or other dispute to which the Contractor is a party which, if decided unfavorably to the Contractor, would reasonably be expected to have a material adverse effect on the Contractor's ability to fulfill its obligations under this Contract.

iii. The Contractor will comply with all laws applicable to its performance of the services and otherwise to the Contractor in connection with its obligations under this Contract.

iv. The Contractor (a) owns, or has the right to use under valid and enforceable agreements, all intellectual property rights reasonably necessary for and related to delivery of the services and provision of the Deliverables as set forth in this Contract; (b) shall be responsible for and have full authority to license all proprietary and/or third party software modules, including algorithms and protocols, that Contractor incorporates into its product; and (c) none of the Deliverables or other materials or technology provided by the Contractor to the State will infringe upon or misappropriate the intellectual property rights of any third party.

v. The Contractor has adequate resources to fulfill its obligations under this Contract.

vi. Neither Contractor nor Contractor's subcontractors has past state or federal violations, convictions or suspensions relating to miscoding of employees in NCCI job codes for purposes of differentiating between independent contractors and employees.

2. **Contractor's Performance Warranties.** Contractor represents and warrants to the State that:

i. All Deliverables will be free from material errors and shall perform in accordance with the specifications therefor for a period of at least one year.

ii. Contractor will provide to the State commercially reasonable continuous and uninterrupted access to the Service, and will not interfere with the State's access to and use of the Service during the term of this Contract;

iii. The Service is compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its documentation;

iv. Each and all of the services shall be performed in a timely, diligent, professional and skillful manner, in accordance with the highest professional or technical standards applicable to such services, by qualified persons with the technical skills, training and experience to perform such services in the planned environment.

v. All Deliverables supplied by the Contractor to the State shall be transferred free and clear of any and all restrictions on the conditions of transfer, modification, licensing, sublicensing and free and clear of any and all leins, claims, mortgages, security interests, liabilities and encumbrances or any kind.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

vi. Any time software is delivered to the State, whether delivered via electronic media or the internet, no portion of such software or the media upon which it is stored or delivered will have any type of software routine or other element which is designed to facilitate unauthorized access to or intrusion upon; or unrequested disabling or erasure of; or unauthorized interference with the operation of any hardware, software, data or peripheral equipment of or utilized by the State. Without limiting the generality of the foregoing, if the State believes that harmful code may be present in any software delivered hereunder, Contractor will, upon State's request, provide a new or clean install of the software. Notwithstanding the foregoing, Contractor assumes no responsibility for the State's negligence or failure to protect data from viruses, or any unintended modification, destruction or disclosure.

vii. To the extent Contractor resells commercial hardware or software it purchased from a third party, Contractor will, to the extent it is legally able to do so, pass through any such third party warranties to the State and will reasonably cooperate in enforcing them. Such warranty pass-through will not relieve the Contractor from Contractor's warranty obligations set forth herein.

3. **Limitation on Disclaimer.** The express warranties set forth in this Contract shall be in lieu of all other warranties, express or implied.
4. **Effect of Breach of Warranty.** If, at any time during the term of this Contract, software or the results of Contractor's work fail to perform according to any warranty of Contractor under this Contract, the State shall promptly notify Contractor in writing of such alleged nonconformance, and Contractor shall, at its own expense and without limiting any other rights or remedies of the State hereunder, re-perform or replace any services that the State has determined to be unsatisfactory in its reasonable discretion. Alternatively, with State consent, the Contractor may refund of all amounts paid by State for the nonconforming deliverable or service

7. **TRADE SECRET, PATENT AND COPYRIGHT INFRINGEMENT**

The State shall not be deemed to waive any of its rights or remedies at law or in equity in the event of Contractor's trade secret, patent and/or copyright infringement.

8. **REMEDIES FOR DEFAULT; NO WAIVER OF REMEDIES**

In the event either party is in default under this Contract, the non-defaulting party may, at its option, pursue any or all of the remedies available to it under this Contract, including termination for cause, and at law or in equity.

No delay or failure to exercise any right, power or remedy accruing to either party upon breach or default by the other under this Contract shall impair any such right, power or remedy, or shall be construed as a waiver of any such right, power or remedy, nor shall any waiver of a single breach or default be deemed a waiver of any subsequent breach or default. All waivers must be in writing.

9. **NO ASSUMPTION OF COSTS**

Any requirement that the State defend or indemnify Contractor or otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or license verification costs of Contractor, is hereby deleted from the Contractor Documents.

10. **TERMINATION**

Upon termination of this Contract for any reason whatsoever, Contractor shall immediately deliver to the State all State information, State Intellectual Property or State Data (including without limitation any Deliverables for which State has made payment in whole or in part) ("State Materials"), that are in the possession or under the control of Contractor in whatever stage of development and form of recordation such State property is expressed or embodied at that time.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

In the event the Contractor ceases conducting business in the normal course, becomes insolvent, makes a general assignment for the benefit of creditors, suffers or permits the appointment of a receiver for its business or assets or avails itself of or becomes subject to any proceeding under the Federal Bankruptcy Act or any statute of any state relating to insolvency or the protection of rights of creditors, the Contractor shall immediately return all State Materials to State control; including, but not limited to, making all necessary access to applicable remote systems available to the State for purposes of downloading all State Materials.

Contractor shall reasonably cooperate with other parties in connection with all services to be delivered under this Contract, including without limitation any successor provider to whom State Materials are to be transferred in connection with termination. Contractor shall assist the State in exporting and extracting the State Materials, in a format usable without the use of the Services and as agreed to by State, at no additional cost.

Any transition services requested by State involving additional knowledge transfer and support may be subject to a contract amendment for a fixed fee or at rates to be mutually agreed upon by the parties.

If the State determines in its sole discretion that a documented transition plan is necessary, then no later than sixty (60) days prior to termination, Contractor and the State shall mutually prepare a Transition Plan identifying transition services to be provided.

11. **ACCESS TO STATE DATA**:

The State may import or export State Materials in part or in whole at its sole discretion at any time (24 hours a day, seven (7) days a week, 365 days a year), during the term of this Contract or for up to [three (3) months] after the Term (so long as the State Materials remain in the Contractor's possession) without interference from the Contractor in a format usable without the Service and in an agreed-upon file format and medium at no additional cost to the State.

The Contractor must allow the State access to information such as system logs and latency statistics that affect its State Materials and or processes.

The Contractor's policies regarding the retrieval of data upon the termination of services have been made available to the State upon execution of this Contract under separate cover. The Contractor shall provide the State with not less than thirty (30) days advance written notice of any material amendment or modification of such policies.

12. **AUDIT RIGHTS**

Contractor will maintain and cause its permitted contractors to maintain a complete audit trail of all transactions and activities, financial and non-financial, in connection with this Contract. Contractor will provide to the State, its internal or external auditors, clients, inspectors, regulators and other designated representatives, at reasonable times (and in the case of State or federal regulators, at any time required by such regulators) access to Contractor personnel and to any and all Contractor facilities or where the required information, data and records are maintained, for the purpose of performing audits and inspections (including unannounced and random audits) of Contractor and/or Contractor personnel and/or any or all of the records, data and information applicable to this Contract.

At a minimum, such audits, inspections and access shall be conducted to the extent permitted or required by any laws applicable to the State or Contractor (or such higher or more rigorous standards, if any, as State or Contractor applies to its own similar businesses, operations or activities), to (i) verify the accuracy of charges and invoices; (ii) verify the integrity of State Data and examine the systems that process, store, maintain, support and transmit that data; (iii) examine and verify Contractor's and/or its permitted contractors' operations and security procedures and controls; (iv) examine and verify Contractor's and/or its permitted contractors' disaster recovery planning and testing, business resumption and continuity planning and testing, contingency arrangements and insurance coverage; and (v) examine Contractor's and/or its

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

permitted contractors' performance of the Services including audits of: (1) practices and procedures; (2) systems, communications and information technology; (3) general controls and physical and data/information security practices and procedures; (4) quality initiatives and quality assurance, (5) contingency and continuity planning, disaster recovery and back-up procedures for processes, resources and data; (6) Contractor's and/or its permitted contractors' efficiency and costs in performing Services; (7) compliance with the terms of this Contract and applicable laws, and (9) any other matters reasonably requested by the State. Contractor shall provide and cause its permitted contractors to provide full cooperation to such auditors, inspectors, regulators and representatives in connection with audit functions and with regard to examinations by regulatory authorities, including the installation and operation of audit software.

13. **DESTRUCTION OF STATE DATA**

At any time during the term of this Contract within (i) thirty days of the State's written request or (ii) [three (3) months] of termination or expiration of this Contract for any reason, and in any event after the State has had an opportunity to export and recover the State Materials, Contractor shall at its own expense securely destroy and erase from all systems it directly or indirectly uses or controls all tangible or intangible forms of the State Materials, in whole or in part, and all copies thereof except such records as are required by law. The destruction of State Data and State Intellectual Property shall be performed according to National Institute of Standards and Technology (NIST) approved methods. Contractor shall certify in writing to the State that such State Data has been disposed of securely. To the extent that any applicable law prevents Contractor from destroying or erasing State Materials as set forth herein, Contractor shall retain, in its then current state, all such State Materials then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Contract, and perform its obligations under this section as soon as such law no longer prevents it from doing so.

Further, upon the relocation of State Data, Contractor shall securely dispose of such copies from the former data location and certify in writing to the State that such State Data has been disposed of securely. Contractor shall comply with all reasonable directions provided by the State with respect to the disposal of State Data.

14. **CONTRACTOR BANKRUPTCY**.

Contractor acknowledges that if Contractor, as a debtor in possession, or a trustee in bankruptcy in a case under Section 365(n) of Title 11, United States Code (the "Bankruptcy Code"), rejects this Contract, the State may elect to retain its rights under this Contract as provided in Section 365(n) of the Bankruptcy Code. Upon written request of the State to Contractor or the Bankruptcy Trustee, Contractor or such Bankruptcy Trustee shall not interfere with the rights of the State as provided in this Contract, including the right to obtain the State Intellectual Property.

15. Artificial Intelligence and Automated Decision Systems

1. Definitions. For purposes of this section:

1.1. "AI Systems" means any automated decision or artificial intelligence systems as defined in 3 V.S.A. § 3305(a)(2) or § 5021.

1.2. "Process" or "processing" means any operation performed on footage or State Data by or through an AI System, including but not limited to: collecting, storing, accessing, transmitting, analyzing, scanning, classifying, tagging, indexing, searching, enhancing, recognizing (including facial recognition, object recognition, or license plate recognition), detecting patterns or anomalies, generating outputs or predictions, or submitting such data to any AI-enabled feature, tool, plugin, or third-party service.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

2. Disclosure Requirement. AI Systems used to process State Data must be limited solely to those disclosed in the completed AI Usage Disclosure Form (BGS Form 12-19-2025) previously submitted by the Contractor and approved by the State. If no form was submitted and approved, Contractor agrees that no AI Systems are or will be used to process State Data in any way.
3. Prior Approval. Contractor shall obtain the State's prior written approval before:
3.1. Modifying any previously approved use of AI Systems in connection with State Data; and
3.2. Permitting any subcontractor or agent acting on Contractor's behalf to use AI Systems in connection with State Data.
4. Prohibition on Use of State Data as Training Data. Contractor may not use State Data as training data, validation data, or any other input for the development, improvement, fine-tuning, or evaluation of any AI System, unless the State provides express prior written authorization specifically identifying:
4.1. The State Data to be used;
4.2. The AI System or model for which it will be used; and
4.3. The specific purpose for which it will be used.
5. Subcontractor and Agent Obligations. Contractor shall ensure that all subcontractors and agents acting on Contractor's behalf comply with the requirements of this section. Contractor remains solely responsible for any use of AI Systems or State Data by subcontractors or agents that violates this section.
6. Notification of Changes. Contractor shall notify the State in writing within ten (10) business days of becoming aware of any change in the AI Systems used to process State Data, including any change introduced by a third-party vendor or platform without Contractor's affirmative action.
7. Violation. Any use of AI Systems or State Data in violation of this section constitutes a material breach of this Contract.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT D1
INSURANCE COVERAGE

In addition to the insurance required in Attachment C to this Contract, before commencing work on this Contract and throughout the term of this Contract, Contractor agrees to procure and maintain:

Professional Liability coverage for services performed under this contract, with minimum coverage of $5,000,000 per claim, $5,000,000 aggregate.

Technology Professional Liability coverage for services performed under this contract, with minimum coverage of $5,000,000 per claim, $5,000,000 aggregate.

Cyber Liability coverage for services performed under this contract, with minimum coverage of $5,000,000 per claim, $5,000,000 aggregate.

Before commencing work on this Contract, Contractor must provide certificates of insurance to show that the foregoing minimum coverages are in effect.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT F
CRIMINAL JUSTICE INFORMATION SERVICES TERMS OF USE

Access to and use of criminal history record information and other sensitive information maintained in state and FBI-managed criminal justice information systems by the Contractor are subject to the following restrictions:

1. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein;
2. Without limiting the above, all contractors and staff, prior to being granted unescorted access to unencrypted CJIS data agree to sign the certification attached hereto; and
3. Without limiting the above, all contractors and staff, prior to being granted unescorted access to unencrypted CJIS data must have an approved fingerprint supported background check.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private
contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and
the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed
by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is
executed and all subsequent versions), as well as with policies and standards established by the
Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.
4.02 Security violations can justify termination of the appended agreement.
4.03 Upon notification, the FBI reserves the right to:
a. Investigate or decline to investigate any report of unauthorized use;
b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.
5.00 Audit
5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.
6.00 Scope and Authority
6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.
6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.
6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to
provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.
6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.
6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee	Date
Printed Name/Signature of Contractor Representative	Date
Organization and Title of Contractor Representative	

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Attachment G

Vendor AI Usage Disclosure | Agency of Digital Services

Requirement for Bidders to Disclose AI Usage in Proposals. Artificial intelligence (AI) can only be used to provide goods and services for the State if prior written approval is obtained from the State. Any use of AI must adhere to the State's Artificial Intelligence Code of Ethics, which can be found at https://digitalservices.vermont.gov/ai. This Code of Ethics restricts the use of AI for certain decisions and imposes various limitations. **Therefore, any bidder planning to use AI technologies in their proposal must address the following three questions in their response to this solicitation:**

1. **Technologies and Functions:**
   a. What specific AI technologies will be utilized for this proposal, and what are their intended functions?
2. **Decision Capabilities (See 3 V.S.A. § 3305):**
   a. What specific decisions will the AI system support or make?
   b. Will the system be used to make any automated final decisions?
   c. How will AI-generated decisions or outputs be evaluated by humans to ensure accuracy?
3. **Human Evaluation and Fail-Safe Mechanisms:**
   a. What human alternatives and fail-safe mechanisms are in place to ensure service continuity in case of AI failures?

If the State approves the use of AI, additional requirements may be included in the contract resulting from this solicitation and the State may require additional information before approving the use of AI. Examples of some of the additional information the State might inquire about are included below. **The below questions are included for information only. Responses to these questions are not required**.

Data Inputs and Outputs:

a. What types of data inputs does the system require, and how are these inputs generated and processed?
b. What types of data will the system generate during its operation?

Data Security and Privacy:

c. Does your proposed use (1) rely on commercially available AI models, or do you (2) develop or customize your own models? If you develop or customize your own models, address the following two items:
   i. Please cite any pertinent security risk management frameworks you use as guidance (e.g., NIST-RMF, ISO-27001, ENISA, etc.).
   ii. Do you conduct third-party audits of your AI systems (including training and deployment environments) to ensure compliance with security standards, and can you provide certifications or reports?
d. Will data input or generated during service delivery be shared with any other entity or used for any other purpose, such as training AI models?

Use-Case Risk Assessment:

e. Has a risk assessment for the specific proposed use-case of this model been conducted? Please indicate one of the following: [_] Yes, by a 3rd party; [_] Yes, internally; or [_] No.
f. If a risk assessment for this specific use-case has been conducted, please describe any risks that were identified and your proposed and/or enacted mitigation steps.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Post-Deployment Auditing/Monitoring :

g. Describe the proposed post-deployment audit/monitoring process.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT H
RFP Glossary

PROJECT GLOSSARY		
#	**TERM**	**DEFINITION**
1	Acceptance Criteria	Specific, testable conditions that must be met for a user story or requirement to be considered complete
2	ACFR	Annual Comprehensive Financial Report
3	ADA	Americans with Disabilities Act
4	ADO	Azure DevOps (Tool used to manage requirements, testing, defects, development, and deployment activities)
5	AFIS	Automated Fingerprint Identification System
6	AHS	Agency of Human Services
7	AHS 988	Suicide & Crisis Lifeline (Provides 24/7 crisis support by call, text, or chat for people experiencing mental health, suicide, or substanceuse-related crises. Vermont's crisis system coordinates 988 with services such as mobile crisis response)
8	ALI	Automatic Location Identification (Provides location information for an incoming emergency call)
9	ALS	Advanced Life Support
10	ANI	Automatic Number Identification (Provides the telephone number associated with an incoming emergency call)
11	API	Application Programming Interface (Allows systems to exchange data and information)
12	ASAP	Automated Secure Alarm Protocol (A standardized protocol/interface used by alarm-monitoring companies to transmit alarm information electronically to 911 centers)
13	ATIS	Advanced Traveler Information System
14	ATMS	Advanced Transportation Management System
15	AVL	Automatic Vehicle Location (Tracks and displays the real-time geographic location of field vehicles on a digital map for dispatchers)
16	Backlog	Prioritized list of requirements, user stories, and other work to be completed
17	Business Requirement	Describes what the business needs a solution to accomplish
18	Business Rule	Defines a rule or condition that guides business processes or system behavior

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

19	CAD	Computer-Aided Dispatch (system used to manage emergency calls, incidents, and response resources)
20	Call-Taker	Person responsible for receiving emergency calls and gathering information needed to support an appropriate response
21	CFS	Call for Service
22	Chain of Custody	Documented chronological record showing the collection, possession, transfer, storage, handling, and disposition of evidence
23	CJI	Criminal Justice Information (Information used by authorized criminal justice agencies and subject to applicable security requirements)
24	CJIS	Criminal Justice Information Services (FBI services and security requirements supporting the use and protection of criminal justice information)
25	CMV	Commercial Motor Vehicle
26	DDI	Design, Development, and Implementation

PROJECT GLOSSARY		
#	**TERM**	**DEFINITION**
27	Dispatch	Process of assigning, notifying, and coordinating public safety resources in response to an incident or call for service
28	DOC	Department of Corrections
29	DPS	Department of Public Safety
30	E911	Enhanced 911 (Emergency calling service that provides caller and location information to emergency communications centers)
31	E911 ALI	Enhanced 911 Automatic Location Identification (a core database and dispatch feature that automatically looks up and displays a caller's physical address on an emergency operator's screen when a 911 call is placed)
32	EIDD	Emergency Incident Data Document
33	EMD	Emergency Medical Dispatch
34	EMS	Emergency Medical Services
35	Entra ID	Microsoft’s identity and access management service used to manage user authentication and access to systems and applications
36	EOC	Emergency Operations Center (Central command and control facility responsible for strategic coordination, resource allocation, and macrolevel decision-making during a disaster or emergency)
37	ePCR	Electronic Patient Care Reporting (Digital record used by EMS to document patient assessments, vital signs, treatments, and transport details in the field)
38	Epic	High-level grouping of related features and user stories

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

39	FBI	Federal Bureau of Investigtion
40	FD	Fire Department
41	Feature	A system capability or grouping of related user stories within an Epic
42	FGDC	Federal Geographic Data Committee (FGDC standards are federal standards and guidelines for geographic information, particularly for geospatial data, metadata, data exchange, and data documentation.)
43	Follow-on Query	An authorized query initiated using information returned from a previous query (e.g., An Officer submits an initial query for John Smith; The system returns a person record that includes a driver's license number and vehicle information; Follow-on query: Search the vehicle registration database using the vehicle license plate returned from the John Smith search.)
44	Functional Requirement	Describes what the system must do, including required functions, processes, or capabilities
45	GIS	Geographic Information System (Provides mapping and location information)
46	HIPAA	Health Insurance Portability and Accountability Act
47	IFT	Inter-Facility Transport (Movement of patients between healthcare facilities)
48	Incident	An event or call for service recorded and managed within a public safety system
49	JAD	Joint Application Development (Collaborative sessions used to define and refine business and system requirements)
50	KPI	Key Performance Indicator (A measure used to track performance against a goal)

PROJECT GLOSSARY		
#	**TERM**	**DEFINITION**
51	LEP	Limited English Proficiency (Limited ability to read, speak, write, or understand English)
52	MCP	Mission Critical Partners
53	MDC/MDT	Mobile Data Computer/Mobile Data Terminal (Device used by field personnel to access incident and operational information)
54	MFA	Multi-Factor Authentication (Requires more than one method to verify a user's identity)
55	MIH	Mobile Integrated Health (A patient-centered care delivery model that uses mobile resources and interprofessional teams to provide healthcare services directly in a patient's home or community setting)
56	MSAG	Master Street Address Guide (A standardized database of valid street names, address ranges, and related location information used to support 9-1-1 call routing and address validation.)

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

57	Mutual Aid	Assistance provided by one public safety agency or jurisdiction to another
58	NDR	Non-Dispatchable Request (Non-emergency request for service that is documented in CAD but does not require the immediate assignment or dispatch of a field responder, such as a noise complaint, graffiti report, or similar public request)
59	NEMSIS	National Emergency Medical Services Information System (National standard for EMS data collection and reporting)
60	NERIS	National Emergency Response Information System (National system for collecting and reporting fire and emergency response data)
61	NFR	Non-Functional Requirement (Describes how the system must perform or the standards it must meet, such as security, accessibility, availability, performance, and scalability)
62	NG911	Next Generation 911 (Modern, internet-based 911 system that supports emergency communications and the exchange of voice, text, location, and other digital information)
63	NGI	Next Generation Identification
64	NIBRS	National Incident-Based Reporting System (FBI standard for reporting detailed crime and incident information)
65	NIMS	National Incident Management System
66	NSOR	National Sex Offender Registry
67	Odyssey File & Serve	Odyssey File & Serve is Vermont's statewide electronic court filing system used for submitting and serving documents
68	ORI	Originating Agency Identifier (Used to identify the reporting agency)
69	PAR	Personal Accountability Report (Roll call used by emergency services to verify the safety, location, and status of all personnel operating at an incident scene)
70	PD	Police Department
71	PHI	Protected Health Information
72	PII	Personally Identifiable Information
73	PSAP	Public Safety Answering Point (The 911 call center that receives emergency calls and processes/distributes emergency information)

PROJECT GLOSSARY		
#	**TERM**	**DEFINITION**

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

74	RBAC	Role-Based Access Control (A security model in which system access and permissions are assigned according to a user's authorized role or responsibilities)
75	RCL	Regional Co-Location
76	RFP	Request For Proposal (A formal document used to solicit proposals from vendors for products or services)
77	RMS	Records Management System (System used to create, maintain, search, and manage public safety records)
78	RTM	Requirements Traceability Matrix (Tracks requirements from definition through testing and completion)
79	RTO	Radio Telephone Operator
80	SAR	Suspicious Activity Report
81	SIEM	Security Information and Event Management
82	SIREN	Statewide Incident Reporting Network (Where EMS providers and first responders log Electronic Patient Care Reports (ePCRs) after responding to a 911 call)
83	SLA	Service Level Agreement (Defines expected levels of service, such as availability, response time, and system performance)
84	SME	Subject Matter Expert
85	SMTP	Simple Mail Transfer Protocol
86	SOP	Standard Operating Procedure
87	SRS	Summary Reporting System
88	SSAR	Self-Service Account Recovery (Allows users to recover access to their account without assistance from technical support)
89	SSO	Single Sign-On (Allows a user to access multiple systems using one sign-in)
90	TMD	Tactical Map Display
91	Traceability	Ability to track relationships between business requirements, functional and non-functional requirements, user stories, business rules, and test results
92	TTY	Teletypewriter (A device or phone setting that lets people who are deaf, hard of hearing, or speech-impaired send and receive typed messages over telephone lines)
93	UAT	User Acceptance Testing (Testing performed to confirm the solution meets business needs)
94	UCR	Uniform Crime Reporting
95	Unit	A specific response asset—such as a vehicle, a specific officer, or a crew—that is tracked, dispatched, and managed within the system.
96	Unit Status	Current operational status of a public safety resource, such as available, assigned, en route, on scene, or unavailable

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

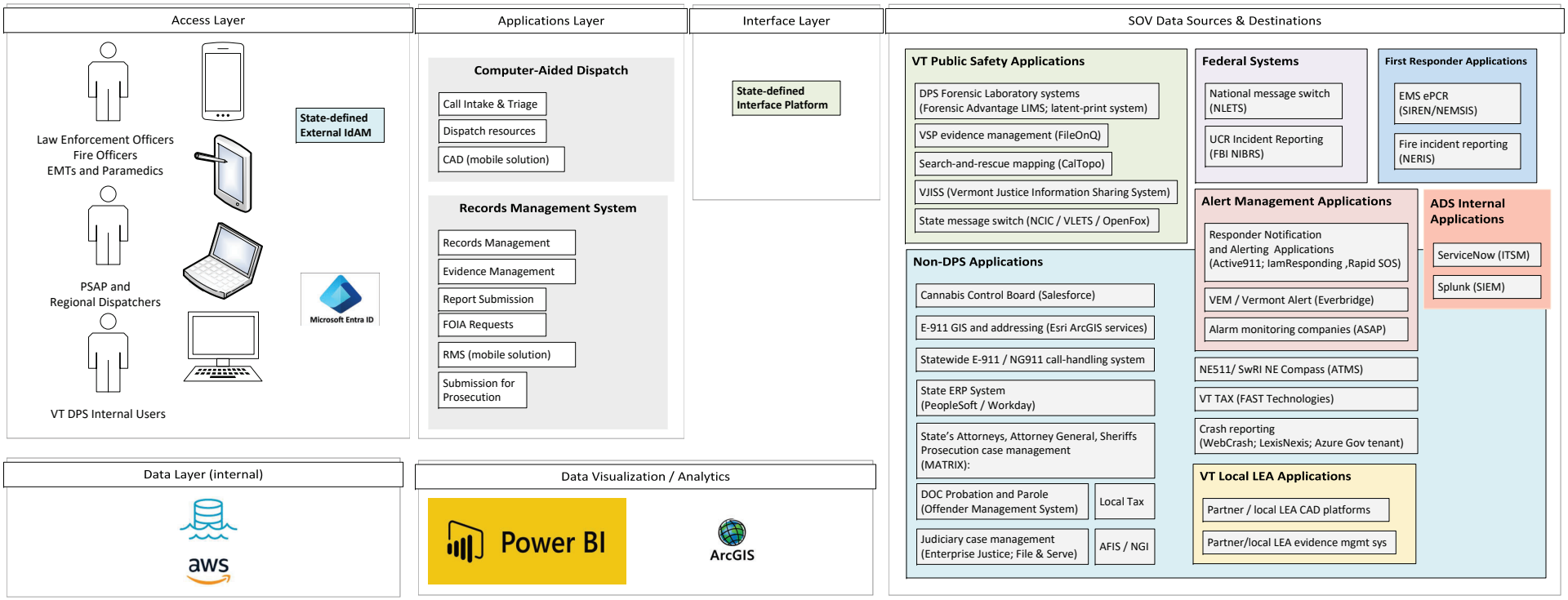
97	User Story	Describes a system need from the user's perspective and the business value it provides. "As a [Role/User], I need [capability/action], So that [business value/outcome]."
98	Valcour	Statewide Law-Enforcement RMS (Records Management System) in Vermont [Legacy System]
99	VCIC	Vermont Crime Information Center

PROJECT GLOSSARY		
#	**TERM**	**DEFINITION**
100	VIBRS	Vermont Incident Based Reporting System (Vermont system supporting incident-based crime reporting)
101	VISION	State of Vermont financial system
102	VJISS	Vermont Justice Information Sharing System (Integrates and queries data across criminal-justice agencies to give investigators and analysts a consolidated view of records held in separate systems)
103	VLETS	Vermont Law Enforcement Telecommunications System (Statewide message switch that connects Vermont agencies to one another and to state and national databases)
104	VOWS	Vermont Online Warrant System
105	VSOR	Vermont Sex Offender Registry
106	VSP	Vermont State Police
107	VT TRIPS	Vermont Title, Registration, Identification and Permitting System
108	VTrans	Vermont Agency of Transportation
109	WCAG	Web Content Accessibility Guidelines (Standards for making digital content accessible to people with disabilities)
110	WebCrash	Vermont statewide crash-report collection system
111	Workflow	Defined sequence of steps used to complete a business process

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ATTACHMENT I
Logical Architecture Diagram v1.0

Author: C. Scott
Date: 11/05/2026



Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

Exhibit C

VERMONT

State of Vermont Bidder Response Form

Request for Proposal Name: Department of Public Safety (DPS) Computer Aided Dispatch and Records Management System (CAD RMS) Replacement

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Vendor Instructions:

Provide the information requested in this form and submit it to the State of Vermont as part of your Request for Proposal (RFP) response. All answers must be provided within the form unless otherwise specified.

Important: This form must be completed and submitted in response to this RFP for your proposal to be considered valid. The submission must also include the eight (8) additional artifacts requested within this form (denoted by underlined green font).

See the RFP for full instructions for submitting a bid. **Bids must be received by the due date and at the location specified on the cover page of the RFP.**

Direct any questions you have concerning this form or the RFP to:

Kyle Emerson, State Purchasing Agent
State of Vermont
Office of Purchasing & Contracting
E-mail Address: **SOV.ThePathForward@vermont.gov**

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Part 1: VENDOR PROFILE

1. Complete the table below.

Item	Detail
Company Name:	[insert the name that you do business under]
Physical Address:	[if more than one office – put the address of your head office]
Postal Address:	[e.g. P.O Box address]
Business Website:	[url address]
Type of Entity (Legal Status):	[sole trader/partnership/limited liability company or specify other]
Primary Contact:	[name of the person responsible for communicating with the Buyer]
Title:	[job title or position]
Email Address:	[email]
Phone Number:	[landline]
Fax Number:	[fax]

2. Provide a brief overview of your company including number of years in business, number of employees, nature of business, and description of clients. Identify any parent corporation and/or subsidiaries.

3. Is your organization currently or has it previously provided solutions and/or services to any agency or entity of the Vermont State government within the past five years? If so, include a complete list of the State entities, the solutions and/or services provided, and the dates your organization provided the State with these services in the last five years.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

4. **Provide a Financial Statement* for your company and label it Attachment #1**. This requirement can be filled by:
   - A current Dun and Bradstreet Report that includes a financial analysis of the firm;
   - An Annual Report if it contains (at a minimum) a Compiled Income Statement and Balance Sheet verified by a Certified Public Accounting firm; or
   - Tax returns and financial statements including income statements and balance sheets for the most recent 3 years, and any available credit reports.

   A confidentiality statement may be included if this financial information is considered non-public information

   **Some types of procurements may require bidders to provide additional or specific financial information. Any such additional requirements will be clearly identified and explained within the RFP and may include supplemental forms in addition to this Bidder Response Form.*

5. Disclose any judgments, pending or expected litigation, or other real potential financial reversals, which might materially affect the viability or stability of your company or indicate below that no such condition is known to exist. A confidentiality statement may be included if this information is considered non-public information

6. Provide a list of three references similar in size and industry (preferably another governmental entity). References shall be clients, other than the State of Vermont, who have implemented your Solution within the past 48 months.

Reference 1	Detail
Reference Company Name:	[insert the name that you do business under]
Company Address:	[address]
Type of Industry:	[industry type: e.g., government, telecommunications, etc.]
Contact Name:	[if applicable]
Contact Phone Number:	[phone]
Contact Email Address:	[email]
Description of system(s) implemented:	[description]

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Date of Implementation:	[date]

Reference 2	**Detail**
Reference Company Name:	[insert the name that you do business under]
Company Address:	[address]
Type of Industry:	[industry type: e.g., government, telecommunications, etc.]
Contact Name:	[if applicable]
Contact Phone Number:	[phone]
Contact Email Address:	[email]
Description of system(s) implemented:	[description]
Date of Implementation:	[date]

Reference 3	**Detail**
Reference Company Name:	[insert the name that you do business under]
Company Address:	[address]
Type of Industry:	[industry type: e.g., government, telecommunications, etc.]
Contact Name:	[if applicable]
Contact Phone Number:	[phone]
Contact Email Address:	[email]
Description of system(s) implemented:	[description]

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Date of Implementation:	[date]

PART 2: VENDOR PROPOSAL/SOLUTION

1. Provide a description of the technology solution you are proposing.

2. Provide a description of the capabilities of the technology solution you are proposing.

3. If specific software is being proposed, provide a description of the:
   A. Standard features and functions of the software:

   B. The software licensing requirements for the solution:

      - Maximum number of concurrent users:

4. Give a brief description of the evolution of the system/software solution you are proposing. Include the date of the first installed site and major developments which have occurred (e.g. new versions, new modules, specific features).

5. List the total number of installations in the last 3 years by the year of installation.

6. Provide the total number of current users for the proposed system and indicate what version they are using.

7. Have you implemented the proposed solution for other government entities? If so, tell us who, when, and how that implementation went?

8. **Provide a Road Map that outlines the company's short term and long term goals for the proposed solution/software and label it Attachment #2. (**A confidentiality statement may be included if this information is considered non-public information)

9. **Provide a PowerPoint (minimum of 1 slide and maximum of 10 slides) that provides an Executive level summary of your proposal to the State. Label it Attachment #3.**

10. Describe any infrastructure, equipment, network or hardware *required* to implement and/or run the solution.

11. What is your recommended way to host this solution?

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

12. Describe how your solution can be integrated to other applications and if you offer a standard-based interface to enable integrations.

13. Respond to the following questions about the solution being proposed:

Question	Vendor Response/Explanation	
	Yes or No	
A. Does the solution use Service Oriented Architecture for integration?		
B. Does the solution use a Rules Engine for business rules?		
C. Does the solution use any Master Data Management?		
D. Does the solution use any Enterprise Content Management software?		
E. Does the solution use any Case Management software?		
F. Does the solution use any Business Intelligence software?		
G. Does the solution use any Database software?		
H. Does the solution use any Business Process Management software?		
I. Is this a browser based solution and if so what browsers do you support?		
J. Does the solution include an API for integration?		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 3: FUNCTIONAL REQUIREMENTS

The State's Functional Requirements are available in the accompanying file: "**DPS_CAD-RMS Modernization_RFP_Functional Requirements-User Stories_FINAL.pdf**". Indicate the "Availability" for each requirement for your proposed solution. Use the "Vendor Comments" column to provide any additional information or explanations.

A - Feature is available in the core ("out-of-the-box") solution.
D - Feature is currently under development (indicate anticipated date of availability in the Vendor comments column).
C - Feature is not available in the core solution, but can provided with customization.
N - Feature is not available.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 4: NON- FUNCTIONAL REQUIREMENTS

The accompanying file "**DPS_CAD-RMS Modernization_RFP_Nonfunctional Requirements-NFRs_FINAL.pdf**" lists the State's Non-Functional Requirements. Indicate if your proposed solution complies in the "Comply" column.

Yes = the solution complies with the stated requirement.
No = the solution does not comply with the stated requirement.
N/A = Not applicable to this offering.

Describe how the requirement is met in the "Vendor Description of Compliance" column.

4.4 Other Non-Functional Requirements

General Administrative Requirements can be found in the accompanying file: "**DPS_CAD-RMS Modernization_RFP_General Admin Requirements-GRQs_FINAL.pdf**".

For each requirement listed, indicate if and how you comply or type "N/A" if it is not applicable to your offering.

4.5 Data Compliance

Vendors and their solutions must adhere to applicable State and Federal standards, policies, and laws based on the type of data that will be stored, accessed, transmitted and/or controlled by the solution. If the "Type of Data" column is checked below, respond "Yes" or "No" in the "Comply" column and provide an explanation on how you comply in the "Vendor's Description of Compliance" column.

Type of Data	Applicable State & Federal Standards, Policies, and Laws	Comply	Vendor's Description of Compliance
☒ Publicly available information	▪ NIST 800-171		
☒ Confidential Personally Identifiable Information (PII)	▪ State law on Notification of Security Breaches ▪ State Law on Social Security Number Protection ▪ State law on the Protection of Personal Information ▪ National Institute of Standards & Technology: NIST SP 800-53 "Moderate" risk controls ▪ Privacy Act of 1974, 5 U.S.C. 552a.		
☐ Payment Card Information	▪ Payment Card Industry Data Security Standard (PCI DSS) v 3.2		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

☐ Federal Tax Information	▪ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: IRS Pub 1075		
☒ Personal Health Information (PHI)	▪ Health Insurance Portability and Accountability Act of 1996: HIPAA ▪ The Health Information Technology for Economic and Clinical Health Act HITECH ▪ Code of Federal Regulations 45 CFR 95.621		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Type of Data	Applicable State & Federal Standards, Policies, and Laws	Comply	Vendor's Description of Compliance
☐ Affordable Care Act Personally Identifiable Information (PII)	▪ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies IRS Pub 1075 ▪ Minimum Acceptable Risk Standards for Exchanges MARS-E 2.0 (Scroll down the page)		
☐ Medicaid Information	▪ Medicaid Information Technology Architecture MITA3.0 ▪ Code of Federal Regulations 45 CFR 95.621		
☒ Prescription Information	▪ State law on the Confidentiality of Prescription Information		
☐ Student Education Data	▪ Family Educational Rights and Privacy Act: FERPA		
☒ Personal Information from Motor Vehicle Records	▪ Driver's Privacy Protection Act (Title XXX) ("DPPA") 18 U.S.C. Chapter 123, §§ 2721 – 2725		
☒ Criminal Records	▪ Criminal Justice Information Security Policy: CJIS		
☒ Other sensitive data	▪ Data that does not fit into the above categories but is sensitive and requires additional protection.		

4.6 State of Vermont Cybersecurity Standard Update

Bidder shall certify by checking the box below the Solution shall not include, incorporate, rely on, utilize or be supported by any products or services subject to the limitations provided under State of Vermont Cybersecurity Standard Update, which Bidder acknowledges has been provided to it, and is available on-line at the following URL: https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives

☐ Bidder hereby certifies that in connection with the Request for Proposal, **none** of the applicable products or services will be included in or used to support State systems in a manner prohibited under the Standard.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 5: IMPLEMENTATION/PROJECT MANAGEMENT APPROACH

1. Describe the approach you would recommend for project managing this engagement.
2. Provide a list of the standard project management deliverables that you would normally produce for this type of engagement.
3. **Provide a proposed list of project phases, major milestones, and an implementation time-line. Label this Attachment #4.**
4. What types of difficulties have other clients experienced with implementation of the proposed solution?

4 Describe the experience and qualifications of the Project Manager you would offer as the resource for this engagement. **Provide a copy of their resume and label it Attachment #5.**

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 6: TECHNICAL SERVICES

1. Describe the technical services included in your proposal (e.g., business analysis, configuration, testing, implementation, etc.).

2. Provide a list of the standard deliverables for the technical services described above.

3. Provide a description of the roles/services/tasks the State will be expected to cover as part of this engagement. Describe any additional roles/services/tasks that are optional, but would be beneficial for the State to provide.

4. Describe your typical conversion plan to convert data from existing systems to your proposed solution (if applicable).

5. Describe **and attach your typical Implementation Plan (label it Attachment #6)**, which shall include planning for the transition to maintenance and operations.

6. Describe the experience and qualifications of the technical resources proposed for this engagement. **Provide their resume(s) and label them Attachment #7.**

7. Describe the training that is included in your proposal.

8. Describe the system, administrator, and/or user documentation that is included in your proposal.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 7: MAINTENANCE AND SUPPORT SERVICES

1. Provide answers to the questions below regarding your company's Maintenance and Support Services:

Questions	Vendor Response
Service: Customer Phone &/or Email Support	
What is the method for contacting technical support?	
What are the hours of operation for support?	
What is the turnaround time for responses?	
What is the escalation process for support issues?	
Who comprises the support team and what are their qualifications?	
Define your response resolution metrics and how you capture and report them.	
Service: Incident/Security Breach Notification and Process	
Describe your identification and notification process for security breaches.	
Service: Data Management	
Describe how data is stored, retained and backed-up (including frequency).	
Service: Hosting	
Describe the hosting service and associated service levels.	

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Questions	Vendor Response
Service: Scheduled Maintenance/Downtime	
What is the frequency of scheduled maintenance and downtime?	
What is the notification process for scheduled maintenance and downtime?	
Describe how "maintenance" updates are tested with customers prior to installing them in their live environments.	
Service: System Upgrades	
Are software upgrades provided as part of the software support contract?	
Describe your software upgrade process.	
How often are new versions released?	
Is documentation and training provided for system upgrades?	
Are there additional costs for upgrades and/or new releases?	
Describe how and when the State will have an opportunity to test system upgrades/releases prior to live installation.	
Describe how the State will validate post installation and how changes will be backed out in the event that a problem is encountered.	

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Questions	Vendor Response
Service: Bug Fixes and Minor Enhancements	
Describe the frequency and process for providing, testing, and installing bug fixes and minor enhancements.	
Service: Disaster Recovery	
Describe the disaster recovery services included in this proposal for any non-state hosted services.	
What is your standard RPO and RTO? State standard is 2-4 hours for RTO. State standard is 15 minutes – 1 hour.	
Describe the plan your company has in place for its own disaster recovery of any sites that may be involved in support of this proposal.	

2. Describe how adherence to your service levels is measured and what remedies you would provide the State when performance doesn't meet the standard?

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 8: PRICING

1. Submit pricing for your proposed solution in the table below. Fill in only the lines that are applicable to your proposal. **Insert lines for additional costs, but do not delete or rename any lines in the Table. Total each column and provide a total of all columns in the "Total Implementation, plus 5 Year Costs" box on the next page.**

Cost Type	One Time (Implementation)	Year 1	Year 2	Year 3	Year 4	Year 5
Software						
Enterprise Application: License Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Maintenance &/or License Fee Add-Ons	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Subscription cost	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Storage Limitations and/or Additional Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Database Software: License Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Middleware Tools: License Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Operating System Software: License Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Upgrade Costs for Later Years	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Support and Maintenance Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Implementation Services						
Project Management	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Requirements	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Design (Architect Solution)	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Development (Build, Configure or Aggregate)/Testing	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
System Testing	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Defect Removal	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Implement/Deploy or Integrate	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Quality Management	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

Cost Type	One Time (Implementation)	Year 1	Year 2	Year 3	Year 4	Year 5
Implementation Services Continued						
Training	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Telecom						$0.00
Bandwidth	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Hardware						$0.00
Computing Hardware	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Storage and Backup Hardware	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Network Hardware	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Facilities/Data Center	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Hosting						$0.00
Hosting Fees	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00
Total Base Costs	**$0.00**					

Total Implementation plus Five Year Costs	**$ 0.00**

2. Describe any assumptions you have made in relation to the above cost and pricing information.

3. Provide pricing information for any volume discounts that are available based on the number of software licenses purchased or support years purchased.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

4. Provide pricing for any Functional Requirements marked as “C” (feature is not available in the core solution, but can be provided with customization).

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 9: TERMS AND CONDITIONS

Exceptions to the States standard terms, conditions, and templates is strongly discouraged. Accordingly, exceptions may result in a determination that a bidders proposal is not in the best interest of the State. However, if a bidder does wish to take exception to the State's terms, conditions, or templates they must indicate those objections in the table below. Add lines to the table below as needed. The State considers contractor documents the bidder wishes to append to the contract as exceptions.

Clause Location	Exception	Proposed Verbiage
[indicate RFP, exhibit, attachment or addendum, section & page number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]
[indicate RFP, exhibit, attachment or addendum, section & page number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]
[indicate RFP, exhibit, attachment or addendum, section & page number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

PART 10: CERTIFICATE OF COMPLIANCE/AUTHORIZED COMPANY SIGNATURE

A. **NON COLLUSION:** Bidder hereby certifies that the prices quoted have been arrived at without collusion and that no prior information concerning these prices has been received from or given to a competitive company. If there is sufficient evidence to warrant investigation of the bid/contract process by the Office of the Attorney General, bidder understands that this paragraph might be used as a basis for litigation.

B. **CONTRACT TERMS:** Bidder hereby acknowledges that is has read, understands and agrees to the terms of this RFP, including Attachment C: Standard State Contract Provisions, and any other contract attachments included with this RFP.

C. **WORKER CLASSIFICATION COMPLIANCE REQUIREMENT:** In accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), the following provisions and requirements apply to Bidder when the amount of its bid exceeds $250,000.00.

Self-Reporting. Bidder hereby self-reports the following information relating to past violations, convictions, suspensions, and any other information related to past performance relative to coding and classification of workers, that occurred in the previous 12 months.

Summary of Detailed Information	Date of Notification	Outcome

Subcontractor Reporting. Bidder hereby acknowledges and agrees that if it is a successful bidder, prior to execution of any contract resulting from this RFP, Bidder will provide to the State a list of all proposed subcontractors and subcontractors' subcontractors, together with the identity of those subcontractors' workers compensation insurance providers, and additional required or requested information, as applicable, in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54), and Bidder will provide any update of such list to the State as additional subcontractors are hired. Bidder further acknowledges and agrees that the failure to submit subcontractor reporting in accordance with Section 32 of The Vermont Recovery and Reinvestment Act of 2009 (Act No. 54) will constitute non-compliance and may result in cancellation of contract and/or restriction from bidding on future state contracts.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

D. **Executive Order 05 – 16: Climate Change Considerations in State Procurements Certification**

Bidder certifies to the following (Bidder may attach any desired explanation or substantiation. Please also note that Bidder may be asked to provide documentation for any applicable claims):

1. Bidder owns, leases or utilizes, for business purposes, space that has received:
   - ❑ Energy Star® Certification
   - ❑ LEED®, Green Globes®, or Living Buildings Challenge℠ Certification
   - ❑ Other internationally recognized building certification:

_____

2. Bidder has received incentives or rebates from an Energy Efficiency Utility or Energy Efficiency Program in the last five years for energy efficient improvements made at bidder's place of business. Please explain:

_____

3. Please Check all that apply:
   - ❑ Bidder can claim on-site renewable power or anaerobic-digester power ("cow-power"). Or bidder consumes renewable electricity through voluntary purchase or offset, provided no such claimed power can be double-claimed by another party.
   - ❑ Bidder uses renewable biomass or bio-fuel for the purposes of thermal (heat) energy at its place of business.
   - ❑ Bidder's heating system has modern, high-efficiency units (boilers, furnaces, stoves, etc.), having reduced emissions of particulate matter and other air pollutants.
   - ❑ Bidder tracks its energy consumption and harmful greenhouse gas emissions. What tool is used to do this?
     _____
   - ❑ Bidder promotes the use of plug-in electric vehicles by providing electric vehicle charging, electric fleet vehicles, preferred parking, designated parking, purchase or lease incentives, etc..
   - ❑ Bidder offers employees an option for a fossil fuel divestment retirement account.
   - ❑ Bidder offers products or services that reduce waste, conserve water, or promote energy efficiency and conservation. Please explain:

_____

_____

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

4. Please list any additional practices that promote clean energy and take action to address climate change:

_____

_____

_____

E. **Executive Order 02 – 22: Solidarity with the Ukrainian People**

❑ By checking this box, Bidder certifies that none of the goods, products, or materials offered in response to this solicitation are Russian-sourced goods or produced by Russian entities. If Bidder is unable to check the box, it shall indicate in the table below which of the applicable offerings are Russian-sourced goods and/or which are produced by Russian entities. An additional column is provided for any note or comment that you may have.

Provided Equipment or Product	Note or Comment

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

F. **Certification Regarding Use of Contract Funds for Lobbying.** The following provision is applicable to the Contractor for contracts over $100,000.00, and Contractor shall include this clause in all its subcontracts over $100,000.00.

1. The prospective contractor certifies, to the best of his or her knowledge and belief, under the penalties of perjury under the laws of the State of Vermont and the United States that on behalf of the person, firm, association, or corporation he or she represents, that:

a. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any Federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

b. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any Federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

2. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31 U.S.C. 1352. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

3. The prospective contractor also agrees that they shall require that the language of this certification be included in all lower tier subcontracts, which exceed $100,000 and that all such recipients shall certify and disclose accordingly.

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

VERMONT

State of Vermont Bidder Response Form

For your bid to be considered valid, this Bidder Response Form must be signed by a duly authorized representative of the bidder, and submitted as part of the response to the proposal.

I am authorized to submit a proposal to the State of Vermont in response to this RFP on behalf of my organization. The information provided as part of my organization's response is a true and accurate representation of my organization's ability to meet the State of Vermont's business needs as expressed in this RFP.

Signature:	
Full name:	
Title:	
Company:	
Date:	

PART 3: FUNCTIONAL REQUIREMENTS

The table below lists the State's Functional Requirements. Indicate the "Availability" for each requirement for your proposed solution.	**A**	Feature is **available in the core** ("out-of-the-box") solution.
Use the "Vendor Comments" column to provide any additional information or explanations.	**D**	***Feature is currently **under development** ***(indicate date of availability in Vendor Comments).
	C	Feature is **not** available in the core solution, but can **provided with customization**.
This content was drafted and edited with the assistance of a generative artificial intelligence (ChatGPT). The content has been reviewed and verified to be accurate and complete and represents the intent of Amy B. Boulanger.	**N**	Feature is **not available**.

ADO ID	Title	User Story	Acceptance Criteria	Availability?	Vendor Comments
EPIC 01: Emergency Communications & CAD Call Management					
7794	911 Call Intake and CAD Call Creation	As a Dispatcher, I want the solution to receive available 911 call information and create or associate it with a CAD call record with available caller and location information, so that emergency calls are captured for call intake and response.	AC 1 Given an 911 call contains available caller or location information, When the solution receives the call, Then the solution shall create or associate the information with a CAD call record.; AC 2 Given a CAD call record is created from an 911 call, When available caller and location information is received, Then the solution shall retain the information with the call record for authorized users.; AC 3 Given an 911 call contains a unique call identifier, When the solution receives the call, Then the solution shall associate the identifier with the CAD call record.; AC 4 Given an 911 call contains incomplete information, When the solution receives the call, Then the solution shall create the call record with the available information.; AC 5 Given an 911 call contains incomplete information, When the solution receives the call, Then the solution shall identify missing information where configured.; AC 6 Given an 911 call is received, When the CAD call record is created, Then the solution shall record the call receipt date and time.; AC 7 Given an 911 call record already exists for the received call, When the solution processes the call information, Then the solution shall associate the received information with the existing call record rather than creating a duplicate record.;		
7795	Dispatcher Call Classification and Response Priority	As a Dispatcher, I need the solution to receive available caller identification and location information, including ANI/ALI information where provided, from the 911 system and provide configurable call types and response priorities for manual assignment, so that incoming calls and incidents can be accurately classified and prioritized to support appropriate response and dispatch.	AC 1 Given an incoming 911 call is received, When the call information is delivered to CAD, Then the solution shall receive and display the available caller identification and location information provided by the 911 system.; AC 2 Given an incoming call or incident is being created, When the Dispatcher selects a call type, Then the solution shall provide a configurable menu of available call types for classification.; AC 3 Given a call type has an associated response priority, When the Dispatcher selects the call type, Then the solution shall assign the configured response priority.; AC 4 Given a call or incident has been classified, When the Dispatcher changes the call type or response priority, Then the solution shall retain the updated classification and priority.; AC 5 Given an Authorized User administers call types and associated response priorities, When approved configuration changes are saved, Then the solution shall apply the updated configuration to subsequent calls and incidents.; AC 6 Given a call type or response priority is changed, When the change is saved, Then the solution shall maintain an audit record identifying the change, the user, and the date and time of the change.		
7796	CFS Routing and Transfer	As a Dispatcher, I want the solution to transfer or route a call for service (CFS) to the solution (CAD-to-CAD) or agency while retaining and transmitting associated caller and incident information, so that the receiving solution or agency can continue call handling with continuity of the CAD call record and without unnecessary re-entry of information.	AC 1 Given a CFS requires transfer to another solution or agency, When an authorized dispatcher initiates the transfer, Then the solution shall identify the configured receiving destination.; AC 2 Given a CFS is transferred, When the transfer is initiated, Then the solution shall transmit the configured caller and incident information to the receiving destination.; AC 3 Given the receiving solution or agency accepts the CFS, When the acceptance is received, Then the originating system shall record the transfer status.; AC 4 Given a CFS transfer fails, When the failure is detected, Then the solution shall notify the dispatcher.; AC 5 Given a CFS transfer fails, When the failure is detected, Then the solution shall retain the transfer status.; AC 6 Given a CFS has been transferred, When an Authorized User reviews the originating record, Then the user shall be able to identify the receiving destination and transfer history.; AC 7 Given a transferred CFS contains information already captured by the originating system, When the receiving system receives the information, Then the solution shall prefill the receiving record with the transmitted information for the receiving user.;		
7797	Caller-Provided Incident Information	As a Dispatcher, I want to capture and retain information provided by the caller about an incident, so that dispatch personnel have the information needed to evaluate, document and dispatch the incident.	AC 1. Given a 911 call taker has collected initial call information, When the call information is delivered to the appropriate dispatch agency, Then the solution shall receive and make the available caller-provided information accessible to authorized dispatch personnel for creating or updating the CAD incident record.; AC 2. Given the receiving dispatch agency has received the initial 911 call information, When an authorized dispatcher creates or updates a CAD incident record, Then the solution shall associate and retain the initial call information with the applicable CAD incident record.; AC 3. Given initial call information and additional incident details have been entered into a CAD incident record, When an authorized dispatcher accesses the record, Then the solution shall display the recorded information for review and continued processing.; AC 4. Given an authorized dispatcher updates incident information, When the changes are saved, Then the solution shall retain the updated information and associated change history.; AC 5. Given required incident information is missing, When an authorized dispatcher attempts to complete the applicable incident workflow, Then the solution shall identify missing information in accordance with configured business rules.		

7798	Caller Identification and Contact Information	As a Dispatcher, I want the solution to capture caller identification and contact information, associate it with calls and incidents, and provide access to caller history, so that authorized users can review prior interactions and contact callers.	AC 1 Given caller identification information is available, When the dispatcher records the information, Then the solution shall associate it with the call or incident.; AC 2 Given caller contact information is available, When the dispatcher records the information, Then the solution shall retain the contact information with the record.; AC 3 Given caller information is associated with an incident, When an Authorized User accesses the record, Then the authorized user shall be able to view the available caller information.; AC 4 Given caller information is updated, When the authorized user saves the change, Then the solution shall retain the updated information and history.; AC 5 Given caller information is restricted by role, When an unauthorized user accesses the incident, Then the solution shall prevent access to restricted caller information.;		
7799	Call-to-Incident Creation	As a Dispatcher, I want to create an incident from an eligible call and carry forward captured call information, so that the incident record can be initiated without re-entering information.	AC 1 Given a call meets the configured criteria for incident creation, When the dispatcher creates an incident, Then the solution shall create an incident record.; AC 2 Given a CAD call contains caller information, When an incident is created from the call, Then the solution shall carry the caller information into the incident.; AC 3 Given a CAD call contains location information, When an incident is created from the call, Then the solution shall carry the location information into the incident.; AC 4 Given a CAD call contains call type and priority information, When an incident is created, Then the solution shall carry forward the information according to configured rules.; AC 5 Given an incident is created from an existing call, When the incident record is saved, Then the solution shall maintain the relationship between the call and incident.; AC 6 Given an incident cannot be created because required information is missing, When the dispatcher attempts to create the incident, Then the solution shall identify the missing information according to configured validation rules.;		
7800	Duplicate and Related Incident Identification	As a Dispatcher, I want the solution to identify potential duplicate or related incidents using defined matching criteria, so that duplicate response activity can be avoided and related incidents can be linked.	AC 1 Given an existing incident matches configured duplicate criteria, When a dispatcher creates a new incident, Then the solution shall identify the potential duplicate.; AC 2 Given an existing incident is potentially related based on configured criteria, When the dispatcher reviews the new incident, Then the solution shall identify the related incident.; AC 3 Given potential duplicate incidents are identified, When the dispatcher reviews the results, Then the solution shall display the information required to support an authorized determination.; AC 4 Given the dispatcher determines that incidents are related, When the relationship is saved, Then the solution shall maintain the relationship between the records.; AC 5 Given the dispatcher determines that incidents are not duplicates, When the dispatcher dismisses the potential match, Then the solution shall allow the new incident to proceed according to configured rules.;		
7801	Call Classification Override	As a Dispatcher, I want to review and override an automated call or incident classification when authorized, so that an incorrect classification or priority can be corrected before or during response.	AC 1 Given a call or incident has an automated classification, When an Authorized User reviews the classification, Then the solution shall display the current classification.; AC 2 Given an Authorized User determines that the automated classification is incorrect, When the user changes the classification, Then the solution shall save the authorized override.; AC 3 Given an Authorized User overrides the response priority, When the override is saved, Then the solution shall apply the new priority to the incident.; AC 4 Given a classification or priority is overridden, When the record is reviewed, Then the solution shall identify the overridden value and current value according to configured audit rules.; AC 5 Given an unauthorized user attempts to override a classification, When the user initiates the action, Then the solution shall prevent the override.;		
7802	Active Incident Monitoring and Event Updates	As a Dispatcher, I want the solution to allow me to view and filter active incidents by responder type and to supplement or update event information with any field of a closed event without reopening the event, so that I can monitor incidents and maintain accurate and complete event records throughout and after incident operations.	AC 1 Given multiple active incidents exist, When a dispatcher filters incidents by responder type, Then the solution shall display incidents matching the selected responder type.; AC 2 Given a dispatcher selects a responder-type filter, When the filter is applied, Then the solution shall refresh the active incident display using the selected criteria.; AC 3 Given an Authorized User updates an active incident, When the update is saved, Then the active incident display shall reflect the updated information.; AC 4 Given a closed event requires supplemental information, When an Authorized User updates an allowed field, Then the solution shall save the change without reopening the event.; AC 5 Given a closed event is updated, When the update is completed, Then the solution shall preserve the closed status and history.; AC 6 Given no active incidents match the selected responder type, When the filter is applied, Then the solution shall indicate that no matching active incidents are available.;		
7803	Resource Assignment	As a Dispatcher, I want the solution to assign available and eligible responders and resources to an incident based on configured operational rules and availability, and record each assignment, so that resources are dispatched and authorized users can identify what was assigned, when it was assigned, and the associated incident.	AC 1 Given an incident requires resources and eligible resources are available, When the dispatcher assigns resources according to configured rules, Then the solution shall record each assignment.; AC 2 Given a resource is unavailable, When the dispatcher attempts to assign the resource, Then the solution shall flag the assignment according to configured rules.; AC 3 Given a resource is assigned to an incident, When the assignment is saved, Then the solution shall record the resource and incident relationship.; AC 4 Given a resource assignment has been recorded, When an Authorized User views the assignment, Then the solution shall display the resource, assignment time, and status.; AC 5 Given multiple resources are assigned to an incident, When the incident is viewed, Then the solution shall display each authorized assignment.; AC 6 Given resource eligibility changes after assignment, When the solution evaluates the resource, Then the solution shall reflect the current eligibility or status according to configured rules.;		
7804	Resource Dispatch	As a Dispatcher, I need to dispatch an assigned responder or resource and record the dispatch action against the incident, so that responders receive actionable deployment information.	AC 1 Given a responder or resource has been assigned to an incident, When the dispatcher initiates dispatch, Then the solution shall record the dispatch action.; AC 2 Given a dispatch action is recorded, When the solution sends the deployment information, Then the assigned responder or resource shall receive the information through the supported channel.; AC 3 Given a dispatch attempt fails, When the failure is detected, Then the solution shall record the failure.; AC 4 Given a dispatch attempt fails, When the failure is detected, Then the solution shall notify the dispatcher according to configured rules.; AC 5 Given a resource has been dispatched, When an Authorized User reviews the incident, Then the user shall be able to view the dispatch status.; AC 6 Given a dispatch is cancelled or changed, When the authorized user records the change, Then the solution shall update the dispatch status.; AC 7 Given a dispatch is cancelled or changed, When the authorized user records the change, Then the solution shall retain the history.;		

7806	Configurable Dispatch Workflows	As a Dispatcher, I want the solution to support configurable dispatch workflows with workflow steps, required information, user actions, and controls, so that DPS can adapt dispatch processes to different operational needs.	AC 1 Given an authorized administrator configures a dispatch workflow, When the workflow is saved, Then the solution shall retain the configured workflow steps.; AC 2 Given a workflow contains required information, When a dispatcher processes an incident using the workflow, Then the solution shall require the configured information.; AC 3 Given a workflow contains required user actions, When the dispatcher processes the incident, Then the solution shall present the actions.; AC 4 Given an incident meets the conditions for a configured workflow, When the incident is processed, Then the solution shall apply the configured workflow.; AC 5 Given an authorized administrator changes an active workflow, When the updated workflow is published, Then subsequent incidents shall use the approved workflow configuration.;		
7807	Incident Status and Automatic CFS Closure	As a Dispatcher, I need the solution to allow me to manage an incident's status from creation through closure using defined status options and transition rules and remove closed CFS events from the active CFS display, so that current incident status and history remain accurate while closed events no longer appear as active.	AC 1 Given an incident has been created, When an Authorized User selects a permitted status transition, Then the solution shall update the incident status.; AC 2 Given an incident status changes, When the change is saved, Then the solution shall retain the previous and new status according to configured history rules.; AC 3 Given an incident is not eligible for a selected status transition, When the user attempts the transition, Then the solution shall prevent the invalid transition.; AC 4 Given an incident reaches the configured closed status, When the closure is completed, Then the solution shall remove the CFS event from the active CFS display.; AC 5 Given a closed incident remains in historical records, When an Authorized User searches for it, Then the solution shall return the incident according to configured access rules.; AC 6 Given an incident status is reopened, When the authorized reopening is completed, Then the solution shall return the incident to the active status.;		
7808	Incident Merge and Split	As a Dispatcher, I want to merge related incidents or split an incident when operational circumstances require separate records, so that incident records reflect changing conditions while preserving history.	AC 1 Given two incidents are determined to represent the same operational event, When an Authorized User merges the incidents, Then the solution shall create the configured merged relationship.; AC 2 Given incidents are merged, When the resulting record is viewed, Then information and history from the source incidents shall remain traceable.; AC 3 Given an incident contains separate operational activities, When an Authorized User splits the incident, Then the solution shall create the configured separate records.; AC 4 Given an incident is split, When the resulting records are reviewed, Then the solution shall retain traceability to the original incident.; AC 5 Given an unauthorized user attempts to merge or split incidents, When the action is initiated, Then the solution shall prevent the action.;		
7809	Inter-Center Incident Transfer	As a Dispatcher, I want to transfer an incident between authorized dispatch centers while preserving required information and status, so that responsibility can move without loss of operational information.	AC 1 Given an incident requires transfer to another authorized dispatch center, When the dispatcher initiates the transfer, Then the solution shall identify the receiving center.; AC 2 Given an incident is transferred, When the transfer is initiated, Then the solution shall transmit the required incident information and current status.; AC 3 Given the receiving center accepts the incident, When acceptance is received, Then the originating system shall record the transfer status.; AC 4 Given the transfer fails, When the failure occurs, Then the solution shall notify the dispatcher.; AC 5 Given the transfer fails, When the failure occurs, Then the solution shall retain the failure information.; AC 6 Given an incident has been transferred, When an Authorized User reviews the incident history, Then the transfer destination and transfer history shall be available.;		
7812	Responder Status and AVL Availability	As a Dispatcher, I want the solution to display current responder and resource availability and status, indicate AVL availability for each unit, use AVL information for supported reporting, messaging, response, and alerting functions, and allow me to create and view unlimited vehicle groups, so that resources can be organized, monitored, and managed based on current operational information.	AC 1 Given responder and resource information is available, When a dispatcher views resource status, Then the solution shall display current availability and operational status.; AC 2 Given a unit has AVL capability available, When a dispatcher views the unit, Then the solution shall indicate the unit's AVL availability.; AC 3 Given AVL information is available, When a supported reporting, messaging, response, or alerting function uses AVL data, Then the solution shall use the current available AVL information.; AC 4 Given an Authorized User creates a vehicle group, When the group is saved, Then the solution shall make the vehicle group available for operational use.; AC 5 Given multiple vehicle groups exist, When an Authorized User views vehicle groups, Then the solution shall display the configured groups.; AC 6 Given a resource changes availability status, When the status update is saved, Then the resource display shall reflect the current status.;		
7815	Incident and Case Updates	As a Dispatcher, I want to update incident and case information while preserving history, so that operational records remain current and complete.	AC 1 Given an Authorized User needs to update incident information, When the user saves an authorized change, Then the solution shall update the record.; AC 2 Given an Authorized User updates case information, When the change is saved, Then the solution shall retain the updated information.; AC 3 Given an existing record contains historical information, When an Authorized User changes data, Then the solution shall preserve required history.; AC 4 Given an unauthorized user attempts to modify restricted information, When the user attempts to save the change, Then the solution shall prevent the modification.; AC 5 Given an Authorized User updates information, When the change is recorded, Then the solution shall retain user and date/time audit information.;		
7822	Call Transcription	As a Dispatcher, I want call transcription information to be captured or received and associated with the call or incident, so that authorized users can review a written representation of the call.	AC 1 Given call transcription information is available, When the transcription is received or captured, Then the solution shall associate it with the call or incident.; AC 2 Given transcription information is received in multiple supported segments, When the solution processes the segments, Then the solution shall associate the segments with the call or incident.; AC 3 Given a transcription is associated with a call, When an Authorized User views the call, Then the user shall be able to access the available transcription.; AC 4 Given transcription information is unavailable, When an Authorized User accesses the call, Then the solution shall indicate that no transcription is available according to configured rules.; AC 5 Given transcription access is restricted, When an unauthorized user attempts to access the transcription, Then the solution shall prevent access.;		
7824	Resource Clearing and Disposition Management	As a Dispatcher or Responder, I want the solution to allow an assigned unit to clear from a CAD event and enter one or more dispositions, and allow authorized users to update the unit assignment and resource status, so that event dispositions, unit status, and resource availability remain accurate and current.	AC 1 Given a unit is assigned to a CAD event, When the responder clears from the event, Then the solution shall remove the active assignment according to configured rules.; AC 2 Given a responder clears from an event, When the responder enters a disposition, Then the solution shall record the selected disposition.; AC 3 Given multiple dispositions are permitted, When the responder enters more than one authorized disposition, Then the solution shall retain each disposition.; AC 4 Given a unit clears an event, When the unit status is updated, Then the solution shall reflect the current resource status.; AC 5 Given an Authorized User changes the unit assignment, When the change is saved, Then the solution shall update the assignment and resource status.; AC 6 Given a unit is cleared from an incident, When the incident is reviewed, Then the unit disposition and status history shall be available.;		

7825	Incident Closure	As a Dispatcher, I want to close an incident when defined closure conditions are satisfied, so that completed incidents are finalized and required history is retained.	AC 1 Given all configured closure conditions are satisfied, When an authorized dispatcher closes the incident, Then the solution shall change the incident to the configured closed status.; AC 2 Given required closure information is missing, When the dispatcher attempts to close the incident, Then the solution shall identify the missing information.; AC 3 Given an incident is closed, When the incident is viewed by an Authorized User, Then the solution shall display the closed status.; AC 4 Given an incident is closed, When the incident history is reviewed, Then the solution shall retain the required incident and closure information.; AC 5 Given an incident is not eligible for closure, When the dispatcher attempts to close it, Then the solution shall prevent closure according to configured rules.;		
7832	Incident Notes	As a Dispatcher, I want to create, update, and retain authorized notes associated with an incident, so that operational details can be documented in context.	AC 1 Given an Authorized User needs to document operational information, When the user creates a note, Then the solution shall associate the note with the incident.; AC 2 Given an Authorized User updates an existing note, When the change is saved, Then the solution shall retain the updated note.; AC 3 Given multiple notes are associated with an incident, When an Authorized User views the incident, Then the solution shall display the authorized notes.; AC 4 Given a note contains restricted information, When an unauthorized user accesses the incident, Then the solution shall restrict access to the note.; AC 5 Given note history is required, When an Authorized User updates a note, Then the solution shall retain the history according to configured rules.;		
7833	Unique Incident Identification	As a Dispatcher, I want each incident to receive a unique identifier that remains associated with the incident throughout its lifecycle, so that the incident can be referenced and traced.	AC 1 Given a new incident is created, When the solution establishes the incident record, Then the solution shall assign a unique incident identifier.; AC 2 Given an incident identifier has been assigned, When the incident is updated, Then the identifier shall remain associated with the incident.; AC 3 Given an incident is transferred, When the transfer is completed, Then the incident identifier shall remain traceable according to configured rules.; AC 4 Given an incident is closed, When an Authorized User retrieves the historical record, Then the original incident identifier shall remain available.; AC 5 Given an incident identifier already exists, When additional activity is recorded against the incident, Then the solution shall associate the activity with the existing identifier rather than create an unnecessary new identifier.;		
7837	Incident Hold	As a Dispatcher, I want to place an incident on hold using defined status options and record the reason, so that deferred incidents remain identified.	AC 1 Given an incident requires a hold, When an Authorized User selects the hold function, Then the solution shall allow the user to select an approved hold status.; AC 2 Given an incident is placed on hold, When the hold is saved, Then the solution shall record the reason.; AC 3 Given an incident is on hold, When an Authorized User views the incident, Then the solution shall display the hold status and reason.; AC 4 Given an incident is released from hold, When an Authorized User changes the status, Then the solution shall update the incident according to configured transition rules.; AC 5 Given an unauthorized user attempts to place an incident on hold, When the action is initiated, Then the solution shall prevent the action.;		
7840	Resource Reassignment	As a Dispatcher, I want to reassign a resource between incidents and update both assignments and statuses, so that changing operational priorities are managed.	AC 1 Given a resource is assigned to an incident, When an authorized dispatcher reassigns the resource to another incident, Then the solution shall update the resource assignment.; AC 2 Given a resource is reassigned, When the change is saved, Then the original incident shall reflect the resource's removal.; AC 3 Given a resource is reassigned, When the change is saved, Then the receiving incident shall reflect the new assignment.; AC 4 Given the resource's operational status changes as a result of reassignment, When the reassignment is completed, Then the solution shall update the resource status.; AC 5 Given a resource reassignment is completed, When an Authorized User reviews the history, Then the reassignment shall be traceable.;		
7841	Resource Arrival Tracking	As a Dispatcher, I want to record when an assigned resource arrives at an incident, so that response milestones and resource status are tracked.	AC 1 Given a resource has been dispatched to an incident, When the dispatcher records the resource's arrival, Then the solution shall record the arrival event.; AC 2 Given a resource arrival is recorded, When the event is saved, Then the solution shall record the arrival date and time.; AC 3 Given a resource has arrived, When an Authorized User views the incident, Then the solution shall display the arrival status.; AC 4 Given a resource arrives at an incident, When the resource status is updated, Then the resource availability status shall reflect the current operational state.; AC 5 Given an arrival event is recorded incorrectly, When an Authorized User corrects it, Then the solution shall retain the corrected information and history.;		
7843	Incident Reopening and Duplicate Event Detection	As a Dispatcher, I need the solution to check for potential duplicate events based on the incident location or coordinates during CFS event creation and allow me to reopen an existing closed incident when authorized conditions require additional activity, so that related activity is associated with the incident and duplicate events are minimized.	AC 1 Given a CFS is being created, When the solution evaluates the incident location against existing events, Then the solution shall identify potential duplicate events based on configured location or coordinate criteria.; AC 2 Given a potential duplicate event is identified, When the dispatcher reviews the result, Then the solution shall display the information required to support an authorized decision.; AC 3 Given a closed incident requires additional authorized activity, When the dispatcher selects the incident for reopening, Then the solution shall verify the reopening conditions.; AC 4 Given reopening conditions are satisfied, When the dispatcher confirms the reopening, Then the solution shall change the incident to the configured reopened status.; AC 5 Given an incident is reopened, When the incident history is reviewed, Then the solution shall retain the reopening action and date/time information.;		
7844	Response Plans and Run-Card Workflows	As a Dispatcher, I want to apply configured response plans and run-card workflows using defined IF/THEN conditions, so that resources and response actions are selected for an incident.	AC 1 Given an incident meets a configured response-plan condition, When the solution evaluates the incident, Then the solution shall identify the response plan.; AC 2 Given an incident meets a configured run-card condition, When the solution evaluates the incident, Then the solution shall identify the run card.; AC 3 Given a response plan contains configured resource assignments, When the plan is applied, Then the solution shall identify or assign the configured resources according to availability rules.; AC 4 Given a response plan contains configured actions, When the plan is applied, Then the solution shall present or execute the actions according to configuration.; AC 5 Given multiple IF/THEN conditions apply, When the solution evaluates the incident, Then the solution shall apply the configured condition precedence.; AC 6 Given an authorized administrator changes a response plan, When the change is activated, Then subsequent incidents shall use the current approved configuration.;		

7853	Responder and Resource Status Management	As a Dispatcher, I want to update responder and resource status using defined status options, so that dispatchers have current operational information.	AC 1 Given a responder or resource has a current operational status, When an authorized dispatcher selects a new configured status, Then the solution shall update the status.; AC 2 Given a responder or resource status is updated, When another authorized dispatcher views the resource, Then the solution shall display the current status.; AC 3 Given a status transition is not permitted, When the dispatcher attempts the transition, Then the solution shall prevent the invalid transition.; AC 4 Given a status change affects availability, When the status is saved, Then the solution shall update the resource availability according to configured rules.; AC 5 Given status history is required, When a responder or resource status changes, Then the solution shall retain the status history.;		
7943	Incident Radio Log	As a Dispatcher, I want the solution to allow me to manually enter and associate radio log entries with a selected incident, event, unit, channel, or specified time period, so that radio communications are documented and linked to the operational records for reference and review.	AC 1 Given a dispatcher needs to document radio communications, When the dispatcher manually enters a radio log entry, Then the solution shall capture the entry.; AC 2 Given a radio log entry is entered, When the dispatcher associates it with a selected incident, event, unit, channel, or time period, Then the solution shall retain the association.; AC 3 Given radio log entries are associated with operational records, When an authorized user reviews the record, Then the solution shall make the associated entries available for review.; AC 4 Given a radio log entry is created or updated, When the change is saved, Then the solution shall retain the entry with user and date/time information.; AC 5 Given required information for a radio log entry is missing, When the dispatcher attempts to save the entry, Then the solution shall identify the missing information according to configured rules.;		
7944	CFS Routing and Queue Assignment	As a Dispatcher, I want the solution to route calls for service to the dispatch position, queue, or decision dispatcher based on configured location, event type, priority, and response-plan rules, so that calls are handled by the operational resource.	AC 1 Given resources are available for a potential assignment, When CAD evaluates resource eligibility, Then the solution shall evaluate configured staffing and crew qualification requirements.; AC 2 Given a resource includes shared crews, strike teams, task forces, or other configured resource conditions, When eligibility is evaluated, Then the solution shall consider the conditions.; AC 3 Given a resource does not meet an eligibility condition, When recommendations are generated, Then the solution shall recommend only resources permitted by the configured rules.; AC 4 Given a resource meets all eligibility conditions, When recommendations are generated, Then the resource may be included as an eligible recommendation.;		
7946	Special Dispatch and Triage Rules	As a Dispatcher, I want the solution to apply configured special dispatch-area, and incident-triage rules based on incident location and type, so that incidents receive the response to established operational protocols.	AC 1 Given an incident has a configured location and type, When CAD evaluates the incident, Then the solution shall apply configured special dispatch-area rules.; AC 2 Given configured rules identify a required response, When the evaluation is completed, Then the solution shall use the resulting response for dispatch processing.;		
7948	Resource Recommendation Override and Rotation Management	As a Dispatcher, I want the solution to allow me to pre-alert, bypass, cancel, and re-evaluate resource recommendations based on current resource availability, proximity, and incident conditions, and return bypassed resources to a configured position in the dispatch rotation, so that resource assignments reflect current operational conditions and agency dispatch procedures.	AC 1 Given a resource recommendation has been generated, When the Dispatcher pre-alerts an eligible resource, Then the solution shall record the pre-alert status.; AC 2 Given a Dispatcher bypasses a recommended resource, When the bypass action is performed, Then the solution shall exclude the resource from the current assignment according to configured rules.; AC 3 Given a bypassed resource is eligible to return to the dispatch rotation, When the return condition is met, Then the solution shall return the resource to the configured position.; AC 4 Given resource availability, proximity, or incident conditions change, When the Dispatcher re-evaluates recommendations, Then the solution shall recalculate recommendations.; AC 5 Given a Dispatcher cancels a resource recommendation, When the cancellation is processed, Then the solution shall update the operational status.;		
7949	Manual and Delayed Call Intake	As a Dispatcher, I want to manually enter and reconcile CAD events when automatic call intake is unavailable or delayed, so that incidents received during an outage or processing backlog can be recorded, identified, and incorporated into the CAD event history.	AC 1 Given automatic call intake is unavailable or delayed, When a Dispatcher manually enters a CAD event, Then the solution shall create the event using the information entered by the Dispatcher.; AC 2 Given an received event is later available, When the Dispatcher reconciles the event, Then the solution shall associate the information without creating an unintended duplicate event.; AC 3 Given a manually entered event is reconciled, When the reconciliation is completed, Then the solution shall retain the source and event history.; AC 4 Given a manual event contains incomplete or invalid required information, When the Dispatcher attempts to save it, Then the solution shall identify the required correction.;		
7951	CAD Internal Messaging	As a Dispatcher or Supervisor, I want to send short operational messages to another CAD workstation or defined group, so that authorized personnel can communicate within the CAD environment without leaving their operational workflow.	AC 1 Given a Dispatcher or Supervisor has authorization to send CAD messages, When the user selects another CAD workstation or defined group, Then the solution shall allow an operational message to be sent.; AC 2 Given a message is sent to a defined recipient or group, When the recipient receives the message, Then the message shall identify the sender and content.; AC 3 Given a user is not authorized to communicate with a designated recipient or group, When the user attempts to send the message, Then the solution shall prevent the unauthorized communication.;		
7952	Major Incident and EOC Coordination	As a Supervisor, I want a controlled view and operational capability for major incidents with EOC coordination, so that command personnel can monitor and manage designated emergency operations without disrupting core CAD operations.	AC 1 Given an incident is designated as a major incident, When an authorized Supervisor accesses the major-incident capability, Then the solution shall provide the configured major-incident view and functions.; AC 2 Given EOC coordination is required, When authorized command personnel access the major-incident capability, Then the solution shall provide the configured coordination information.; AC 3 Given a major incident is active, When command personnel perform authorized actions, Then core CAD operations shall remain available to authorized operational users.;		
7957	Aviation and Weather Information	As a Dispatcher, I want access to approved public-safety flight and weather information, so that aviation resources can be coordinated using current operational and environmental information.	AC 1 Given an authorized Dispatcher requests public-safety flight information, When the request is processed, Then the solution shall provide information from the approved source.; AC 2 Given weather information is available, When the Dispatcher requests weather information, Then the solution shall provide the current information from the approved source.; AC 3 Given the external information source is unavailable, When the Dispatcher attempts to retrieve the information, Then the solution shall indicate that current information could not be retrieved.;		

7959	Configurable Messaging and Automated Alerts	As a Dispatcher, I want the solution to support configurable messaging, paging, alerts, and emergency notifications through approved communication channels with automated alerts triggered by defined operational conditions, so that required information is delivered to responders, supervisors, agencies, and designated recipients.	AC 1 Given an operational condition meets a configured alert trigger, When the condition occurs, Then the solution shall generate the configured alert or notification.; AC 2 Given a message or alert has designated recipients, When the notification is generated, Then the solution shall deliver it through the configured approved communication channel.; AC 3 Given paging, messaging, or emergency notification is initiated manually, When the user submits the notification, Then the solution shall transmit the configured information to the selected recipients.; AC 4 Given delivery fails, When the solution detects the failure, Then the notification status shall identify the unsuccessful delivery where supported.;		
7961	Non-Dispatchable Request	As a Dispatcher, I need the solution to support the receipt, documentation, and tracking of non-emergency requests for service received through approved communication channels, with the ability to refer requests to designated personnel or agencies for follow-up based on configured procedures, so that non-emergency service requests are appropriately recorded, managed, and addressed without requiring immediate responder dispatch.	AC 1 Given a supported non-dispatchable incident is received through a configured communication channel, When the solution processes the communication, Then the solution shall create or update the record according to configured rules.; AC 2 Given an operational message has predefined recipients, When an Authorized User sends the message, Then the solution shall deliver the message to the configured recipients.; AC 3 Given a supported communication cannot be processed, When the failure occurs, Then the solution shall provide a processing indication.;		
7963	Call Source and Channel Tracking	As a Dispatcher, I want the solution to retain the originating source or channel and captured caller and location information with the call or incident record, so that authorized users can identify the source, review the information received, and maintain an auditable record.	AC 1 Given a call or incident originates from a source or channel, When the solution creates the call or incident record, Then the solution shall retain the originating source or channel with the record.; AC 2 Given caller and location information is captured during call handling, When the information is received, Then the solution shall retain the captured caller and location information with the call or incident record.; AC 3 Given a record retains the originating source or channel, When an Authorized User reviews the record, Then the solution shall display the originating source or channel.; AC 4 Given a record retains captured caller and location information, When an Authorized User reviews the record, Then the solution shall display the captured caller and location information.; AC 5 Given source, channel, and captured information is retained with a record, When the record is reviewed, Then the solution shall maintain the retained information as an auditable record.;		
7964	Assignment Cancellation and Notification	As a Dispatcher, I want the solution to update incident and resource statuses and generate configured notifications following an assignment cancellation, so that operational status remains accurate and affected users are notified when required.	AC 1 Given an assignment is canceled, When the cancellation is processed, Then the solution shall update the incident and resource statuses according to configured rules.; AC 2 Given a configured notification is required following assignment cancellation, When the cancellation occurs, Then the solution shall generate the notification.; AC 3 Given affected users or resources are identified, When the notification is generated, Then the solution shall route it to the configured recipients.;		
7965	Dispatch Notification and Status Update	As a Dispatcher, I want the solution to notify the assigned responder or resource and update operational statuses following dispatch, so that responders receive the assignment information and the incident reflects the current response state.	AC 1 Given an incident status changes, When the new status is saved, Then the solution shall retain the prior status and new status.; AC 2 Given an incident status change is performed by a user or solution source, When the change is recorded, Then the solution shall retain the actor or source.; AC 3 Given an incident status change is recorded, When the history is reviewed, Then the solution shall display the timestamp.; AC 4 Given an Authorized User reviews incident status history, When the history is retrieved, Then the user shall be able to reconstruct the sequence of recorded status changes.;		
7987	Resource Recommendation	As a Dispatcher, I want the solution to recommend resources using configured capability, availability, workload, proximity, mutual-aid, and rotation rules, so that resource recommendations reflect current operational conditions and established resource-selection criteria.	AC 1 Given configured capability, availability, workload, proximity, mutual-aid, and rotation rules, When a resource is required for an incident, Then the solution shall recommend resources per the configured rules.; AC 2 Given operational conditions change, When resource status or availability is updated, Then the solution shall update the recommendation to reflect current conditions.AC 3 Given an Authorized User reviews a recommendation, When it is presented, Then the solution shall allow the user to accept or override the recommended resources.; AC 4 Given no resource satisfies the configured rules, When a recommendation is requested, Then the solution shall indicate that no qualifying resource is available.; AC 5 Given a recommendation is overridden, When the override is saved, Then the solution shall retain the override and associated audit information.		
7988	Coverage Gap and Resource Reallocation	As a Dispatcher, I want the solution to identify coverage gaps and support move-up, supplementation, and resource reallocation, so that available resources can be repositioned to maintain operational coverage.	AC 1 Given configured coverage requirements for an area, When current resource positioning falls below the configured coverage threshold, Then the solution shall identify the coverage gap to the dispatcher; AC 2 Given a coverage gap is identified, When the dispatcher requests move-up options, Then the solution shall recommend eligible units for repositioning based on configured move-up rules; AC 3 Given a dispatcher selects a move-up recommendation, When the move-up is executed, Then the solution shall update the affected units' assignments; AC 4 Given a dispatcher selects a move-up recommendation, When the move-up is executed, Then the solution shall record the move-up action; AC 5 Given additional resources are needed to maintain coverage, When a dispatcher initiates supplementation, Then the solution shall allow assignment of supplemental resources; AC 6 Given additional resources are needed to maintain coverage, When a dispatcher initiates supplementation, Then the solution shall record the supplementation; AC 7 Given resources are reallocated, When the reallocation is completed, Then the solution shall update coverage status to reflect the new resource positioning; AC 8 Given a move-up or reallocation occurs, When an Authorized User reviews the coverage history, Then the solution shall provide a date/time-stamped record of the repositioning action and the user who performed it;		

7990	Scheduled CAD Event Management	As a Dispatcher, I want to create, activate, adjust, and monitor scheduled CAD events, so that planned events can be managed before and during their operational lifecycle.	AC 1 Given an Authorized User enters the required information for a scheduled CAD event, When the event is created, Then the solution shall persist the scheduled event with its scheduled date and time; AC 2 Given a scheduled CAD event exists, When its scheduled activation time is reached or a user activates it, Then the solution shall activate the event; AC 3 Given a scheduled CAD event exists, When its scheduled activation time is reached or a user activates it, Then the solution shall make it available for operational management; AC 4 Given a scheduled or active CAD event, When an Authorized User adjusts its details, Then the solution shall apply the adjustment; AC 5 Given a scheduled or active CAD event, When an Authorized User adjusts its details, Then the solution shall retain a record of the change; AC 6 Given an active scheduled event, When a dispatcher monitors the event, Then the solution shall display the event's current status throughout its operational lifecycle; AC 7 Given required information for a scheduled event is incomplete, When the user attempts to create the event, Then the solution shall identify the missing required information; AC 8 Given required information for a scheduled event is incomplete, When the user attempts to create the event, Then the solution shall prevent creation; AC 9 Given a scheduled CAD event reaches completion or cancellation, When its lifecycle ends, Then the solution shall record the final status; AC 10 Given a scheduled CAD event reaches completion or cancellation, When its lifecycle ends, Then the solution shall retain the event record;		
8002	Turnout and Response-Time Threshold Configuration	As a Supervisor, I want to configure turnout and response-time thresholds by program, unit type, geography, or other approved operational criteria, so that performance monitoring and alerts align with established operational policies.	AC 1 Given a supervisor is authorized to configure thresholds, When the supervisor defines turnout and response-time thresholds by program, unit type, geography, or approved criteria, Then the solution shall persist the configured thresholds; AC 2 Given a user without configuration permission attempts to modify thresholds, When the change is submitted, Then the solution shall prevent the modification; AC 3 Given thresholds are configured, When performance monitoring and alerting are applied, Then the solution shall evaluate performance against the configured thresholds; AC 4 Given a threshold value is invalid, When the supervisor attempts to save it, Then the solution shall identify the invalid value; AC 5 Given a threshold value is invalid, When the supervisor attempts to save it, Then the solution shall prevent saving; AC 6 Given thresholds are changed, When an Authorized User reviews threshold configuration history, Then the solution shall provide a record of the change and the user who made it;		
8003	Turnout-Time Alerts	As a Dispatcher, I want to receive real-time alerts when a dispatched unit exceeds a configured turnout-time threshold, so that I can identify delayed turnout and take operational action.	AC 1 Given a configured turnout-time threshold, When a dispatched unit exceeds the threshold before reaching the response status, Then the solution shall generate a real-time alert to the dispatcher; AC 2 Given a turnout alert is generated, When the dispatcher views the alert, Then the solution shall identify the affected unit and incident; AC 3 Given a unit reaches the response status before the threshold, When turnout is evaluated, Then the solution shall withhold the turnout alert for that unit.; AC 4 Given a turnout alert is active, When the dispatcher acknowledges or clears it, Then the solution shall record the action; AC 5 Given a turnout alert is active, When the dispatcher acknowledges or clears it, Then the solution shall retain the alert in history; AC 6 Given a turnout alert occurs, When the alert is generated, Then the solution shall retain an auditable record of the alert for performance review;		
8004	Live Turnout Timer	As a Dispatcher, I want to view a live HH:MM:SS turnout timer for each dispatched unit until the unit changes to the response status, so that turnout progress can be monitored at a glance.	AC 1 Given a unit is dispatched, When the dispatch occurs, Then the solution shall display a live HH:MM:SS turnout timer for the unit; AC 2 Given a turnout timer is running, When the unit changes to the response status, Then the solution shall stop the turnout timer for that unit; AC 3 Given multiple units are dispatched, When the dispatcher views the active units, Then the solution shall display a distinct turnout timer for each dispatched unit; AC 4 Given a turnout timer is displayed, When time elapses, Then the solution shall update the timer display in HH:MM:SS format in real time; AC 5 Given a unit has reached response status, When the dispatcher reviews the incident, Then the solution shall retain the elapsed turnout time for the unit;		
8005	First-Arrival and Unit Response-Time Dashboard	As an Incident Commander or Supervisor, I want a dashboard showing incident-level first-arrival response time and per-unit response times, so that response performance can be monitored during an active incident.	AC 1 Given an active incident with dispatched units, When an incident commander or supervisor views the response dashboard, Then the solution shall display the incident-level first-arrival response time; AC 2 Given multiple units are assigned to an incident, When the user views the dashboard, Then the solution shall display per-unit response times; AC 3 Given response times are displayed, When time progresses during the active incident, Then the solution shall update the displayed response-time values in real time; AC 4 Given a first unit arrives on scene, When arrival is recorded, Then the solution shall calculate and display the first-arrival response time for the incident; AC 5 Given response-time values are displayed, When shown on the dashboard, Then the solution shall present them in HH:MM:SS format; AC 6 Given a user lacks permission to view the response dashboard, When the user attempts access, Then the solution shall prevent access;		
8011	Mayday Event Management	As a Dispatcher, I want the solution to receive, prioritize, track, and manage Mayday events, so that responder distress situations receive immediate and traceable operational attention.	AC 1 Given a Mayday event is received, When the solution processes the event, Then the solution shall create and prioritize it above routine activity per configured rules.; AC 2 Given a Mayday event is active, When a dispatcher manages the event, Then the solution shall track and display the event status and associated unit information.; AC 3 Given a Mayday event is initiated, When the event is created, Then the solution shall notify the configured dispatcher or responders.; AC 4 Given a Mayday event is updated or cleared, When the change is saved, Then the solution shall retain the event status and history for traceability.		
8015	Specialized Resource Identification	As a Dispatcher, I want the solution to identify special teams and resources with configured specialized equipment, qualifications, or capabilities, so that incidents can be assigned resources that meet established operational requirements.	AC 1 Given special teams and resources are configured with specialized equipment, qualifications, or capabilities, When a dispatcher searches for resources meeting an incident requirement, Then the solution shall identify the resources that meet the configured requirement; AC 2 Given an incident requires a specialized capability, When the solution recommends resources, Then the solution shall include only resources possessing the required capability; AC 3 Given a resource lacks a required specialized capability, When resource identification occurs, Then the solution shall exclude that resource from the qualifying results; AC 4 Given specialized capabilities are configured, When an administrator updates a resource's capabilities, Then the solution shall reflect the updated capabilities in subsequent identification; AC 5 Given a specialized resource is identified for an incident, When the dispatcher assigns it, Then the solution shall associate the specialized resource with the incident;		

8016	Run-Card Resource Recommendations	As a Dispatcher, I want the solution to use run cards to recommend the closest eligible units based on AVL and estimated time of arrival (ETA), so that resource recommendations support response and coverage.	AC 1 Given run cards and AVL data are available, When a dispatcher requests a recommendation, Then the solution shall recommend the closest eligible units based on AVL and estimated time of arrival; AC 2 Given multiple eligible units are available, When the solution computes recommendations, Then the solution shall rank the units by estimated time of arrival; AC 3 Given AVL data is unavailable for a unit, When the solution computes the recommendation, Then the solution shall apply the configured fallback and indicate the limitation; AC 4 Given a run card defines eligible units for an incident type and location, When a recommendation is generated, Then the solution shall restrict recommendations to units eligible under the run card; AC 5 Given unit locations change, When the dispatcher refreshes the recommendation, Then the solution shall recalculate the closest eligible units using current AVL and ETA; AC 6 Given a dispatcher overrides the recommended closest units, When the override is applied, Then the solution shall record the override and the selected units;		
8017	Run-Card Partner Agency Support	As a System Administrator, I want to create run cards that include partner agencies under approved agreements, so that inter-agency responses follow policy.	AC 1 Given approved inter-agency agreements are configured, When an administrator defines a run card, Then the solution shall allow partner agencies covered by the agreements to be included on the run card; AC 2 Given a partner agency is included on a run card, When an inter-agency response is recommended, Then the solution shall recommend the partner agency's resources in accordance with policy; AC 3 Given a partner agency is not covered by an approved agreement, When an administrator attempts to add it to a run card, Then the solution shall prevent the addition; AC 4 Given run card changes involving partner agencies are made, When the changes are saved, Then the solution shall retain a record of the change and the user;		
8018	ETA and Distance-Based Resource Selection	As a Dispatcher, I want selection to use ETA or distance metrics, so that recommendations reflect real-world travel time and constraints.	AC 1 Given ETA and distance metrics are available, When the solution selects recommended units, Then the solution shall use the configured ETA or distance metric for selection; AC 2 Given travel constraints affect ETA, When the solution computes ETA, Then the solution shall reflect the travel constraints in the selection; AC 3 Given an administrator configures the selection metric, When the configuration is saved, Then the solution shall apply the selected ETA or distance metric to subsequent recommendations; AC 4 Given the required location or travel data is unavailable, When the solution computes selection, Then the solution shall apply the configured fallback and indicate the limitation;		
8019	Time- and Day-Based Run Cards	As a System Administrator, I want run cards to vary by time and day, so that staffing and risk patterns are reflected.	AC 1 Given run cards configured to vary by time and day, When a recommendation is generated at a given time and day, Then the solution shall apply the run card in effect for that time and day; AC 2 Given an administrator defines time- and day-based run card variations, When the configuration is saved, Then the solution shall persist the time- and day-specific run cards; AC 3 Given the time or day changes, When a recommendation is generated, Then the solution shall apply the time- and day-based run card without manual intervention; AC 4 Given overlapping or conflicting time or day run cards are configured, When the configuration is saved, Then the solution shall identify the conflict; AC 5 Given overlapping or conflicting time or day run cards are configured, When the configuration is saved, Then the solution shall prevent an ambiguous configuration;		
8020	Configurable Dispatch Levels	As a Supervisor, I want adjustable dispatch levels with custom names and no artificial limits, so that posture can be scaled and understood.	AC 1 Given a supervisor defines dispatch levels with custom names, When the levels are saved, Then the solution shall persist the dispatch levels with their custom names; AC 2 Given dispatch levels are being defined, When a supervisor adds levels, Then the solution shall support the number of dispatch levels the supervisor configures.; AC 3 Given a supervisor adjusts a dispatch level, When the change is saved, Then the solution shall apply the adjusted level to operations; AC 4 Given a dispatch level name is missing or duplicates an existing name, When the supervisor attempts to save it, Then the solution shall identify the condition; AC 5 Given a dispatch level name is missing or duplicates an existing name, When the supervisor attempts to save it, Then the solution shall prevent saving; AC 6 Given dispatch levels are configured, When a supervisor views the levels, Then the solution shall present each level with its custom name;		
8021	Discipline-Specific Dispatch Levels	As a Supervisor, I want to activate levels by plan/discipline, so that each domain can scale independently.	AC 1 Given dispatch levels are configured by plan or discipline, When a supervisor activates a level for a specific plan or discipline, Then the solution shall activate the level for that plan or discipline only; AC 2 Given a level is activated for one discipline, When another discipline operates concurrently, Then the solution shall allow each discipline to scale independently; AC 3 Given a level activation is applied, When the activation occurs, Then the solution shall record the activation with the user, plan or discipline, and time; AC 4 Given a user lacks permission to activate levels, When the user attempts activation, Then the solution shall prevent the action;		
8022	Resource Requirement Alerts	As a Dispatcher, I want to receive alerts when required unit counts or types are unmet, so that I can correct gaps.	AC 1 Given a dispatch level specifies required unit counts or types, When the assigned units do not meet the requirement, Then the solution shall alert the dispatcher to the unmet requirement; AC 2 Given an unmet-requirement alert is generated, When the dispatcher views it, Then the solution shall identify the specific shortfall in count or type; AC 3 Given the requirement is subsequently met, When units are assigned, Then the solution shall clear the unmet-requirement alert; AC 4 Given an unmet-requirement alert occurs, When the alert is generated, Then the solution shall retain a record of the alert for review;		
8023	Unit Attribute Management	As a System Administrator, I want the solution to define and assign multiple attributes to each unit with capabilities, equipment, certifications, and other approved characteristics, so that units can be identified and selected based on their configured capabilities.	AC 1 Given an administrator defines unit attributes, When the administrator assigns multiple attributes to a unit, Then the solution shall persist all assigned attributes for that unit; AC 2 Given a unit has multiple attributes, When selection logic is applied, Then the solution shall evaluate the unit using all of its assigned attributes; AC 3 Given an administrator removes or updates a unit attribute, When the change is saved, Then the solution shall reflect the updated attributes in subsequent selection; AC 4 Given a user lacks permission to modify unit attributes, When the user attempts the change, Then the solution shall prevent the modification;		
8024	Personnel Attribute Management	As a System Administrator, I want the solution to define and assign multiple attributes and qualifications to personnel, so that personnel can be identified and assigned based on their qualifications, certifications, and other approved characteristics.	AC 1 Given personnel attributes are configured, When personnel are assigned to a unit, Then the solution shall factor the personnel attributes into the unit's capability; AC 2 Given a unit's staffing changes, When personnel with qualifications are added or removed, Then the solution shall update the unit's capability accordingly; AC 3 Given a unit's capability depends on staffing qualifications, When eligibility is evaluated, Then the solution shall determine eligibility using the current personnel attributes; AC 4 Given required personnel qualifications are not met, When unit capability is evaluated, Then the solution shall reflect the reduced capability;		

8025	Unit and Personnel Attribute Search	As a Dispatcher, I want to search units/personnel by attributes, so that I can find suitable resources.	AC 1 Given units and personnel have configured attributes, When a dispatcher searches by one or more attributes, Then the solution shall return units and personnel matching the specified attributes; AC 2 Given no units or personnel match the search attributes, When the dispatcher performs the search, Then the solution shall indicate that no matching resources were found; AC 3 Given search results are returned, When the dispatcher views them, Then the solution shall present the matching resources with their attributes; AC 4 Given multiple attributes are specified, When the dispatcher searches, Then the solution shall return resources meeting the combined criteria;		
8026	Shared Crew Identification and Management	As a Scheduler, I want the solution to allow me to search for and identify shared crews and personnel assigned across multiple units, and view their associated unit assignments and availability, so that shared personnel can be managed when scheduling and assigning resources.	AC 1 Given crews are shared across multiple units, When a scheduler assigns a shared crew, Then the solution shall associate the crew with the units; AC 2 Given a shared crew is already committed to one unit, When the scheduler attempts to commit it to a conflicting unit, Then the solution shall identify the overcommitment; AC 3 Given a shared crew is already committed to one unit, When the scheduler attempts to commit it to a conflicting unit, Then the solution shall prevent it; AC 4 Given a shared crew's assignment changes, When the change is saved, Then the solution shall update the availability of all affected units; AC 5 Given a shared crew is assigned, When a dispatcher views unit availability, Then the solution shall reflect the crew's commitment across the affected units; AC 6 Given shared-crew assignments are made, When an Authorized User reviews the history, Then the solution shall provide a record of the assignments and changes;		
8032	Pending Queue Priority and Time Sorting	As a Dispatcher or Authorized User, I want the solution to present the pending event queue ordered first by call priority and then by elapsed wait time, so that the highest-priority events are addressed first and events of equal priority are processed in the order received.	AC 1 Given events are in the pending queue, When the queue is displayed, Then the solution shall sort the pending events first by priority and then by time; AC 2 Given a new event enters the pending queue, When the queue updates, Then the solution shall position the event according to its priority and time; AC 3 Given two events share the same priority, When the queue is sorted, Then the solution shall order them by time; AC 4 Given an event's priority changes, When the queue updates, Then the solution shall re-sort the pending queue accordingly; AC 5 Given the pending queue is displayed, When a dispatcher processes events, Then the solution shall present the events in the sorted order;		
8033	Resource Rotation Rules	As a Supervisor, I want rotation rules for equivalent units, so that workload is balanced and policy is met.	AC 1 Given rotation rules for equivalent units are configured, When the solution selects from a rotation pool, Then the solution shall select the next eligible unit in the configured rotation; AC 2 Given a unit is selected from rotation, When the selection occurs, Then the solution shall advance the rotation so workload is balanced per policy; AC 3 Given a unit in the rotation is unavailable, When the solution selects from rotation, Then the solution shall skip the unavailable unit and select the next eligible unit; AC 4 Given a supervisor configures rotation rules, When the configuration is saved, Then the solution shall persist the rotation rules; AC 5 Given rotation selections occur, When an Authorized User reviews rotation history, Then the solution shall provide a record of the selections for policy verification;		
8034	Conditional Resource Availability	As a Supervisor, I want to encode conditional availability, so that dispatch respects temporary constraints.	AC 1 Given a resource has a temporary constraint on its availability, When an Authorized User encodes the conditional availability, Then the solution shall persist the conditional availability for the resource; AC 2 Given a resource has encoded conditional availability, When the solution evaluates the resource for dispatch, Then the solution shall respect the temporary constraint; AC 3 Given a conditional availability constraint expires, When the constraint period ends, Then the solution shall restore the resource's normal availability; AC 4 Given a dispatcher attempts to assign a resource during a constrained period, When the assignment is submitted, Then the solution shall notify the dispatcher of the conditional availability; AC 5 Given conditional availability is encoded or changed, When an Authorized User reviews availability history, Then the solution shall provide a record of the change and the user;		
8038	Unit, Officer, and AVL Identification	As a Dispatcher, I want the solution to import and display radio IDs, officer IDs, and AVL IDs as configurable unit aliases, so that unit identity and location status can be identified and associated during incident operations.	AC 1 Given radio IDs, officer IDs, and AVL IDs are available, When the solution imports them, Then the solution shall associate the imported identifiers as configurable unit aliases; AC 2 Given unit aliases are configured, When a unit's identity or location status is displayed, Then the solution shall display the radio, officer, or AVL alias; AC 3 Given an administrator configures a unit alias, When the configuration is saved, Then the solution shall persist the alias for the unit; AC 4 Given an imported identifier cannot be associated with a known unit, When the import occurs, Then the solution shall identify the unmatched identifier for resolution; AC 5 Given a unit alias changes, When the change is applied, Then the solution shall reflect the updated alias in subsequent identification and association;		
8039	Public Non-Dispatchable Incident Submission	As a Member of the Public, I want to submit non-dispatchable incidents online, so that cases are captured and assigned a case number and history.	AC 1 Given a member of the public submits a non-dispatchable incident online, When the submission is received, Then the solution shall create a case record from the submission; AC 2 Given a non-dispatchable incident is created, When the case record is created, Then the solution shall assign a case number to the record; AC 3 Given an online submission is incomplete in required fields, When the member of the public submits it, Then the solution shall identify the missing required information; AC 4 Given an online submission is incomplete in required fields, When the member of the public submits it, Then the solution shall prevent submission; AC 5 Given a non-dispatchable case is created, When the case is processed, Then the solution shall maintain a history for the case; AC 6 Given a non-dispatchable submission is received, When the case is created, Then the solution shall record the submission as non-dispatchable.;		
8050	Direct Event Processing	As a Dispatcher, I want the solution to allow me to create an event, assign a unit, and close the event with a disposition without completing the standard dispatch workflow, so that events that do not require the full dispatch process can be documented and managed.	AC 1 Given an event does not require the full dispatch process, When a dispatcher creates the event, Then the solution shall allow creation without completing the standard dispatch workflow; AC 2 Given such an event is created, When the dispatcher assigns a unit, Then the solution shall allow the unit assignment; AC 3 Given such an event is open, When the dispatcher closes it with a disposition, Then the solution shall close the event; AC 4 Given such an event is open, When the dispatcher closes it with a disposition, Then the solution shall record the disposition; AC 5 Given a required disposition is not provided and policy requires one, When the dispatcher attempts to close the event, Then the solution shall prevent closure until a disposition is entered; AC 6 Given the event is created and closed outside the standard workflow, When the event is processed, Then the solution shall retain a complete history of the event actions; AC 7 Given such an event is closed, When an Authorized User views it, Then the solution shall display the assigned unit and disposition;		

8051	Advised Event and Disposition Management	As a Dispatcher, I want the solution to allow me to designate a CFS as an "Advised Event" independently of the incident type or nature code and append a disposition code and comments to events that are not assigned resources, so that events can be classified and documented regardless of whether a response is dispatched.	AC 1 Given a CFS does not have assigned resources, When a dispatcher designates it as an Advised Event, Then the solution shall apply the Advised Event designation independently of the incident type or nature code; AC 2 Given an Advised Event or other non-resourced event, When a dispatcher appends a disposition code and comments, Then the solution shall record the disposition code and comments on the event; AC 3 Given an event is designated as an Advised Event, When the designation is applied, Then the solution shall make resource assignment optional for the Advised Event.; AC 4 Given an Advised Event designation is applied, When the action occurs, Then the solution shall record the designation with the user and time; AC 5 Given an Advised Event is documented, When an Authorized User views it, Then the solution shall display the Advised Event designation, disposition, and comments; AC 6 Given a user lacks permission to designate Advised Events, When the user attempts the designation, Then the solution shall prevent the action;		
8052	Event Update and Change Entry	As a Dispatcher, I want the solution to support an event update/change data entry screen, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an existing CAD event, When a dispatcher initiates an event update, Then the solution shall provide an event update/change data entry screen; AC 2 Given the event update screen is displayed, When the dispatcher enters changes, Then the solution shall apply the updates to the event record; AC 3 Given required update information is incomplete, When the dispatcher submits the update, Then the solution shall identify the missing information; AC 4 Given required update information is incomplete, When the dispatcher submits the update, Then the solution shall prevent completion; AC 5 Given an event is updated, When the change is saved, Then the solution shall record the update in the event history with the user and time;		
8053	Confirm Before Updating a Closed Event	As a Dispatcher, I want the solution to require confirmation from the user when attempting to update any field in a closed event, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a closed event, When a user attempts to update any field, Then the solution shall require confirmation from the user before applying the change; AC 2 Given the user confirms the update to a closed event, When confirmation is provided, Then the solution shall apply the change; AC 3 Given the user declines the confirmation, When the prompt is dismissed, Then the solution shall retain the prior values and discard the declined change.; AC 4 Given a closed event is updated after confirmation, When the change is saved, Then the solution shall record the update in the event history with the user and time;		
8054	Acknowledge Successful Event Update	As a Dispatcher, I want the solution to provide the user with acknowledgment that an update to a CAD event record was successfully completed, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a user updates a CAD event record, When the update is successfully completed, Then the solution shall provide the user acknowledgment that the update was completed; AC 2 Given a user update fails to complete, When the failure occurs, Then the solution shall notify the user that the update was not completed; AC 3 Given an acknowledgment is provided, When the update completes, Then the solution shall ensure the acknowledgment reflects the actual persisted result;		
8055	Multi-Agency Event Creation	As a Dispatcher, I want the solution to support, in a multiple dispatch agency or jurisdiction environment, the ability to create multiple CFS events with a single CFS event entry, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a multiple dispatch agency or jurisdiction environment and an incident type, When a dispatcher creates a single CFS event entry, Then the solution shall create the multiple CFS events limited to law enforcement, EMS, and fire; AC 2 Given multiple CFS events are created from a single entry, When they are created, Then the solution shall carry forward the incident information to each event; AC 3 Given the configured incident type determines the events to create, When the single entry is submitted, Then the solution shall create only the events to that incident type; AC 4 Given multiple related CFS events are created, When an Authorized User views them, Then the solution shall identify the events as related to the originating entry; AC 5 Given one of the multiple events is updated, When the update occurs, Then the solution shall maintain each event independently;		
8056	Configurable Duplicate Event Search	As a Dispatcher, I want the solution to allow an Authorized User to change the duplicate event search parameters, so that the capability is available in accordance with approved operational requirements.	AC 1 Given duplicate event search parameters are configurable, When an Authorized User changes a parameter limited to distance, exact street address match, or block range, Then the solution shall apply the changed parameters to duplicate searches; AC 2 Given a user lacks authorization to change search parameters, When the user attempts the change, Then the solution shall prevent the modification; AC 3 Given a parameter value is invalid, When the user attempts to save it, Then the solution shall identify the invalid value; AC 4 Given a parameter value is invalid, When the user attempts to save it, Then the solution shall prevent saving; AC 5 Given duplicate search parameters are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8063	Response Plan Compliance Monitoring	As a Dispatcher, I want the solution to monitor, on a continuous basis, each plan in effect and alert the dispatcher when units are not in their proper positions, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a plan is in effect, When the solution monitors the plan, Then the solution shall continuously evaluate whether units are in their proper positions; AC 2 Given units are not in their proper positions, When the plan goes out of compliance, Then the solution shall alert the dispatcher that the plan is out of compliance; AC 3 Given a plan returns to compliance, When unit positions are corrected, Then the solution shall clear the out-of-compliance alert; AC 4 Given multiple plans are in effect, When the solution monitors compliance, Then the solution shall monitor each plan independently; AC 5 Given an out-of-compliance condition occurs, When the alert is generated, Then the solution shall retain a record of the condition for review;		
8064	Multiple Resource-Type Response Plans	As a Dispatcher, I want the solution to include the capability for multiple plans by unit resource type, so that the capability is available in accordance with approved operational requirements.	AC 1 Given multiple plans are defined by unit resource type, When plans are configured, Then the solution shall support multiple plans by unit resource type; AC 2 Given plans exist for different resource types, When a plan is applied, Then the solution shall apply the plan corresponding to the unit resource type; AC 3 Given an Authorized User configures a plan by resource type, When the configuration is saved, Then the solution shall persist the plan for that resource type; AC 4 Given conflicting plans for a resource type are configured, When the configuration is saved, Then the solution shall identify the conflict; AC 5 Given conflicting plans for a resource type are configured, When the configuration is saved, Then the solution shall prevent an ambiguous configuration;		
8067	Configurable Unit Dispositions	As a Dispatcher, I want the solution to enable the CAD administrator to define a list of available unit dispositions, so that the capability is available in accordance with approved operational requirements.	AC 1 Given the CAD administrator defines available unit dispositions, When the disposition list is saved, Then the solution shall persist the defined list of available unit dispositions; AC 2 Given a unit disposition list is defined, When a dispatcher records a disposition, Then the solution shall present the defined dispositions for selection; AC 3 Given a user lacks permission to define dispositions, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given the disposition list is updated, When the change is saved, Then the solution shall apply the updated list to subsequent disposition selection;		

8068	Dispatcher and Field Unit Dispositions	As a Dispatcher, I want the solution to facilitate the recording of dispositions by the dispatcher or the field unit if MDC-equipped, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a dispatcher records a disposition, When the disposition is entered, Then the solution shall record the disposition for the unit or event; AC 2 Given a field unit is MDC-equipped, When the field unit records a disposition, Then the solution shall accept and record the disposition entered from the field; AC 3 Given a disposition is recorded from the field or by the dispatcher, When it is saved, Then the solution shall associate the disposition with the unit and event; AC 4 Given a disposition entry is incomplete, When it is submitted, Then the solution shall identify the missing information; AC 5 Given a disposition entry is incomplete, When it is submitted, Then the solution shall prevent completion;		
8069	Disposition Multipliers	As a Dispatcher, I want the solution to include a multiplication factor for each disposition when multiple instances of the same disposition apply, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a disposition applies multiple times for an event, When a dispatcher enters a multiplication factor for that disposition, Then the solution shall record the disposition with the specified multiplication factor; AC 2 Given a disposition with a multiplication factor is recorded, When the event is viewed or reported, Then the solution shall reflect the total count represented by the factor; AC 3 Given an invalid multiplication factor is entered, When the disposition is submitted, Then the solution shall identify the invalid value; AC 4 Given an invalid multiplication factor is entered, When the disposition is submitted, Then the solution shall prevent acceptance; AC 5 Given a disposition does not require a multiplication factor, When the disposition is recorded, Then the solution shall record a single instance;		
8070	Optional Disposition Requirements	As a Dispatcher, I want the solution to NOT require a disposition if agency policy does not require the use of dispositions, so that the capability is available in accordance with approved operational requirements.	AC 1 Given agency policy does not require the use of dispositions, When an event is closed, Then the solution shall make the disposition optional at event closure.; AC 2 Given agency policy requires dispositions, When an event is closed, Then the solution shall require a disposition in accordance with policy; AC 3 Given disposition requirements are configured by agency, When an event is processed, Then the solution shall apply the agency's disposition requirement; AC 4 Given an Authorized User configures whether dispositions are required, When the configuration is saved, Then the solution shall apply the configured requirement to subsequent events;		
8073	Dynamic Unit Staffing	As a Dispatcher, I want the solution to allow the dynamic entry of personnel staffing specific units/apparatus, so that the capability is available in accordance with approved operational requirements.	AC 1 Given units or apparatus require staffing, When a dispatcher enters personnel staffing a specific unit or apparatus, Then the solution shall record the personnel assigned to that unit or apparatus; AC 2 Given personnel staffing changes during operations, When the dispatcher updates the staffing, Then the solution shall update the unit's staffing in real time; AC 3 Given staffing information is entered, When it is saved, Then the solution shall associate the personnel with the unit or apparatus; AC 4 Given required staffing information is incomplete, When it is submitted, Then the solution shall identify the missing information; AC 5 Given required staffing information is incomplete, When it is submitted, Then the solution shall prevent completion;		
8074	Unit and Vehicle Identification Management	As a Dispatcher, I want the solution to maintain both vehicle identification and radio call sign for each unit and allow me to access and update the unit's most recent event using the unit identification or a currently assigned unit, so that unit and vehicle information remains accurate and traceable throughout event operations.	AC 1 Given each unit has a vehicle identification and a radio call sign, When unit information is maintained, Then the solution shall maintain both the vehicle identification and the radio call sign for the unit; AC 2 Given a dispatcher references a unit by its unit identification or a currently assigned unit, When the dispatcher accesses the unit's most recent event, Then the solution shall provide access to; AC 3 Given a dispatcher references a unit by its unit identification or a currently assigned unit, When the dispatcher accesses the unit's most recent event, Then the solution shall allow updates to that event; AC 4 Given unit or vehicle information changes, When the change is saved, Then the solution shall update the information while preserving traceability; AC 5 Given a dispatcher updates a unit's most recent event, When the update is saved, Then the solution shall record the update in the event history; AC 6 Given a referenced unit has no current event, When the dispatcher attempts access, Then the solution shall indicate that no current event exists for the unit;		
8077	Event Update Notifications	As a Dispatcher, I need the solution to present an audible or visual indication to the dispatcher when a CFS event is updated by another source limited to a call taker, another dispatcher, or a field unit, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CFS event is updated by another source limited to a call taker, another dispatcher, or a field unit, When the update occurs, Then the solution shall present an audible or visual indication to the dispatcher.; AC 2 Given multiple updates occur, When they are received, Then the solution shall indicate each update to the dispatcher; AC 3 Given the dispatcher acknowledges the indicated update, When acknowledgment occurs, Then the solution shall clear the update indication; AC 4 Given an update indication is configured, When an Authorized User sets the indication behavior, Then the solution shall apply the configured audible or visual indication;		
8078	Held CFS Management	As a Dispatcher, I want the solution to hold a CFS event for a specific unit, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CFS event and a specific unit, When a dispatcher holds the event for that unit, Then the solution shall hold the CFS event for the specified unit; AC 2 Given an event is held for a specific unit, When the hold is applied, Then the solution shall associate the hold with that unit; AC 3 Given an event is held for a unit, When the hold is released, Then the solution shall remove the hold; AC 4 Given an event is held for a unit, When the hold is released, Then the solution shall make the event available for assignment; AC 5 Given an event is held for a unit, When the action occurs, Then the solution shall record the hold in the event history;		
8079	Assign Offline Units with Confirmation	As a Dispatcher, I want to assign any valid field unit to an incident even if it is not logged on to the solution, with notification and confirmation that the correct unit was assigned, so that offline units can be dispatched accurately.	AC 1 Given a valid field unit is not currently logged on to the solution, When a dispatcher assigns that unit to an incident, Then the solution shall allow the assignment.; AC 2 Given a unit that is not logged on is assigned, When the assignment is made, Then the solution shall associate the unit with the incident.; AC 3 Given a not-logged-on unit is assigned, When the unit subsequently logs on, Then the solution shall reflect the existing assignment for the unit.; AC 4 Given an invalid unit is entered for assignment, When the assignment is submitted, Then the solution shall identify the invalid unit.; AC 5 Given an invalid unit is entered for assignment, When the assignment is submitted, Then the solution shall prevent the assignment.; AC 6 Given a unit assigned to an incident is not logged on, When the assignment is made, Then the solution shall notify the dispatcher and require confirmation that the correct unit was assigned before finalizing.; AC 7 Given the assignment of a not-logged-on unit is confirmed, When the confirmation occurs, Then the solution shall record the assignment and confirmation in the event history.;		
8080	Offline Unit Assignment Confirmation	As a Dispatcher, I need the solution to support/notify the dispatcher and confirm that the correct unit has been assigned if a unit assigned to an incident is not logged on the system, so that the capability is available consistently, traceably, and in accordance with approved operational requirements.	AC 287.1 Given a unit assigned to an incident is not logged on the system, When the assignment is made, Then the system shall notify the dispatcher that the unit is not logged on; AC 287.2 Given the dispatcher is notified that a unit is not logged on, When the dispatcher proceeds, Then the system shall confirm that the correct unit has been assigned; AC 287.3 Given the dispatcher does not confirm the assignment, When confirmation is pending, Then the system shall not finalize the assignment; AC 287.4 Given the assignment of a not-logged-on unit is confirmed, When the confirmation occurs, Then the system shall record the assignment and confirmation in the event history;		

8081	Reverse Chronological Event Comments	As a Dispatcher, I want the solution to allow the user to display the added comments in reverse chronological order, so that the capability is available in accordance with approved operational requirements.	AC 1 Given comments have been added to an event, When the user displays the comments, Then the solution shall display the added comments in reverse chronological order; AC 2 Given new comments are added, When the display refreshes, Then the solution shall maintain the reverse chronological order; AC 3 Given comments are displayed, When the user reviews them, Then the solution shall associate the comments with the event;		
8083	Concurrent Event Updates	As a Dispatcher, I want the solution to permit multiple users with MDC-equipped field resources, the ability to simultaneously update information to the CFS event, so that the capability is available in accordance with approved operational requirements.	AC 1 Given multiple users with MDC-equipped field resources, are accessing a CFS event, When they update information simultaneously, Then the solution shall permit simultaneous updates to the CFS event; AC 2 Given concurrent updates are submitted, When they are processed, Then the solution shall apply the updates while preserving each contribution in the event history; AC 3 Given concurrent updates affect the same field, When the conflict occurs, Then the solution shall handle the conflict in accordance with configured rules; AC 4 Given simultaneous updates occur, When they are recorded, Then the solution shall record each update with its source, user, and time;		
8084	Closed Incident Supplemental Information	As a Dispatcher, I want the solution to add supplemental information to closed incidents based on assigned user rights, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a closed incident and a user with rights, When the user adds supplemental information, Then the solution shall allow the supplemental information to be added to the closed incident; AC 2 Given a user lacks the rights to add supplemental information to closed incidents, When the user attempts the action, Then the solution shall prevent it; AC 3 Given supplemental information is added to a closed incident, When it is saved, Then the solution shall record the addition in the incident history with the user and time; AC 4 Given supplemental information is added, When an Authorized User views the incident, Then the solution shall display the supplemental information while preserving the original record;		
8086	Event Entry Notifications	As a Dispatcher, I want the solution to provide separate notification for each entry made, so that the capability is available in accordance with approved operational requirements.	AC 1 Given multiple entries are made, When each entry is recorded, Then the solution shall provide a separate notification for each entry; AC 2 Given separate notifications are generated, When they are delivered, Then the solution shall associate each notification with its corresponding entry; AC 3 Given a notification fails to deliver, When the failure occurs, Then the solution shall identify the delivery failure for the affected entry;		
8087	View Supplemental Event Data	As a Dispatcher, I want to view additional CFS event data with the newest information first and all at one time, so that I can review the complete supplemental record for an event.	AC 1 Given additional CFS event data exists, When the data is displayed, Then the solution shall display the additional CFS event data with the newest information first.; AC 2 Given new CFS event data is added, When the display refreshes, Then the solution shall maintain the newest-first ordering.; AC 3 Given additional CFS event data is displayed, When the user reviews it, Then the solution shall associate the displayed data with the event.; AC 4 Given additional CFS event data exists, When the user requests to view all of it, Then the solution shall display all additional CFS event data at one time.; AC 5 Given no additional CFS event data exists, When the user requests to view it, Then the solution shall indicate that no additional data is available.;		
8088	Supplemental Event Data View	As a Dispatcher, I need the solution to support/view all additional CFS event data at one time, so that the capability is available consistently, traceably, and in accordance with approved operational requirements.	AC 295.1 Given additional CFS event data exists, When the user requests to view all of it, Then the system shall display all additional CFS event data at one time; AC 295.2 Given all additional CFS event data is displayed, When the user reviews it, Then the system shall present the complete set of additional data for the event; AC 295.3 Given no additional CFS event data exists, When the user requests to view it, Then the system shall indicate that no additional data is available;		
8089	CFS Multimedia Capture, Streaming, and Association	As a Dispatcher, I want the solution to capture, associate, and retain multimedia data with a CFS event or an approved external repository, support streaming video and audio, and allow authorized users to start, stop, pause, rewind, and resize multimedia feeds, so that multimedia information can be linked to the associated incident and accessed for operational and historical purposes.	AC 1 Given multimedia data is available for a CFS event, When the dispatcher captures or receives the multimedia, Then the solution shall associate the multimedia with the CFS event or approved external repository.; AC 2 Given multimedia is associated with a CFS event, When an authorized user accesses the event, Then the solution shall retain and make the multimedia available for operational and historical purposes.; AC 3 Given streaming video or audio is available, When an authorized user views the feed, Then the solution shall support streaming of the video and audio.; AC 4 Given a multimedia feed is displayed, When an authorized user controls playback, Then the solution shall allow the user to start, stop, pause, rewind, and resize the feed.; AC 5 Given multimedia access is restricted, When an unauthorized user attempts access, Then the solution shall prevent access according to configured rules.;		
8090	Multiple Held Events	As a Dispatcher, I want the solution to allow multiple events to be placed on hold for a single unit, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a single unit, When a dispatcher places multiple events on hold for that unit, Then the solution shall allow multiple events to be held for the single unit; AC 2 Given multiple events are held for a unit, When they are held, Then the solution shall maintain each held event's association with the unit; AC 3 Given multiple events are held for a unit, When a held event is released, Then the solution shall release only the selected event; AC 4 Given events are held for a unit, When an Authorized User reviews the unit, Then the solution shall display the events currently held for that unit;		
8091	Held Event for Offline Unit	As a Dispatcher, I want the solution to allow a CFS event to be held for a unit that is not yet logged on, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a unit is not yet logged on, When a dispatcher holds a CFS event for that unit, Then the solution shall allow the event to be held for the not-logged-on unit; AC 2 Given an event is held for a not-logged-on unit, When the unit logs on, Then the solution shall reflect the held event for the unit; AC 3 Given an event is held for a not-logged-on unit, When the hold is applied, Then the solution shall record the hold in the event history; AC 4 Given an invalid unit is entered for a hold, When the hold is submitted, Then the solution shall identify the invalid unit; AC 5 Given an invalid unit is entered for a hold, When the hold is submitted, Then the solution shall prevent the hold;		
8092	Held Event History	As a Dispatcher, I need the solution to support/record a date/time-stamped record of the change in the CFS event when an event is placed on hold, so that the capability is available consistently, traceably, and in accordance with approved operational requirements.	AC 299.1 Given an event is placed on hold, When the hold occurs, Then the system shall record in the history of the CFS event that the event was placed on hold; AC 299.2 Given a hold is recorded in the event history, When an authorized user reviews the history, Then the system shall display the hold action with a date/time stamp; AC 299.3 Given a hold is released, When the release occurs, Then the system shall record the release in the event history;		

8093	Held Event Resource Assignment	As a Dispatcher, I want the solution to support and not limit the ability of the dispatcher to assign another unit to the incident or for field units to self-dispatch (assign) themselves to an event that has been placed on hold, if permitted by agency policy, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an event has been placed on hold and agency policy permits, When a dispatcher assigns another unit to the incident, Then the solution shall allow the additional assignment; AC 2 Given an event has been placed on hold and agency policy permits, When a field unit self-dispatches to the event, Then the solution shall allow the self-dispatch; AC 3 Given agency policy does not permit self-dispatch or additional assignment to held events, When the action is attempted, Then the solution shall prevent it; AC 4 Given a unit is assigned to or self-dispatches to a held event, When the action occurs, Then the solution shall record the action in the event history;		
8094	Unit Secondary Location	As a Dispatcher, I want the solution to change a unit's location from the primary address to a secondary address without clearing the unit from the incident or CAD record, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a unit is assigned to an incident at a primary address, When the unit's location is changed to a secondary address, Then the solution shall change the unit's location without clearing the unit from the incident or CAD record; AC 2 Given a unit's location is changed to a secondary address, When the change occurs, Then the solution shall retain the unit's assignment to the incident; AC 3 Given a unit location change is made, When it is saved, Then the solution shall record the change in the event history; AC 4 Given a unit returns to its primary address, When the location is changed back, Then the solution shall update the unit's location while preserving the assignment;		
8095	Event Change History	As a Dispatcher, I want the solution to log a date/time stamped record of each change in the CFS event, including when an event is placed on hold or released, so that the change history is complete and auditable.	AC 1 Given a change occurs in the CFS event, When the change is made, Then the solution shall log a date/time stamped record of the change in the CFS event.; AC 2 Given a logged change exists, When an Authorized User reviews the event, Then the solution shall display the change with its date/time stamp.; AC 3 Given multiple changes occur, When they are logged, Then the solution shall record each change in sequence.; AC 4 Given an event is placed on hold, When the hold occurs, Then the solution shall log the hold as a change in the event history with a date/time stamp.; AC 5 Given an event hold is released, When the release occurs, Then the solution shall log the release as a change in the event history.;		
8096	Agency-Specific Event Number	As a Dispatcher, I want the solution to assign an agency specific incident/event number to the CFS event, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an agency-specific incident/event number is required, When a dispatcher assigns it to the CFS event, Then the solution shall associate the agency-specific incident/event number with the CFS event; AC 2 Given an agency-specific number format is configured, When the number is assigned, Then the solution shall apply the configured format; AC 3 Given an agency-specific number is assigned, When the event is viewed, Then the solution shall display the agency-specific number with the event; AC 4 Given a duplicate agency-specific number is entered, When it is submitted, Then the solution shall identify the duplicate; AC 5 Given a duplicate agency-specific number is entered, When it is submitted, Then the solution shall prevent its assignment;		
8097	Added Resource Tracking	As a Dispatcher, I want the solution to track the added resources for the duration of the incident, so that the capability is available in accordance with approved operational requirements.	AC 1 Given resources are added to an incident, When the resources are added, Then the solution shall track the added resources for the duration of the incident; AC 2 Given added resources are being tracked, When their status changes, Then the solution shall update the tracked status for the incident; AC 3 Given the incident is closed, When tracking ends, Then the solution shall retain the record of the added resources and their involvement; AC 4 Given added resources are tracked, When an Authorized User reviews the incident, Then the solution shall display the added resources and their activity;		
8098	Configurable CAD Event Timers	As a Dispatcher, I want the solution to have, and allow configuration of, timers for solution events, limited to a priority one call overdue to be dispatched, so that the capability is available in accordance with approved operational requirements.	AC 1 Given timers for solution events are configured, When a configured condition limited to a priority one call overdue to be dispatched occurs, Then the solution shall trigger the timer alert; AC 2 Given an Authorized User configures a solution event timer, When the configuration is saved, Then the solution shall persist the timer configuration; AC 3 Given a timer threshold is reached, When the timer expires, Then the solution shall alert the dispatcher; AC 4 Given a timer condition is resolved before expiration, When the condition clears, Then the solution shall clear the timer and withhold the alert.; AC 5 Given a timer alert occurs, When it is generated, Then the solution shall record the alert for review;		
8099	Manual Timer Alerts	As a Dispatcher, I want the solution to allow for operators to manually place a timer alert on a CFS or a unit, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CFS or a unit, When an operator manually places a timer alert on it, Then the solution shall apply the manual timer alert to the CFS or unit; AC 2 Given a manual timer alert reaches its threshold, When the timer expires, Then the solution shall alert the operator; AC 3 Given a manual timer alert is placed, When it is set, Then the solution shall associate the timer with the CFS or unit; AC 4 Given an operator cancels a manual timer alert, When the cancellation occurs, Then the solution shall remove the timer; AC 5 Given an operator cancels a manual timer alert, When the cancellation occurs, Then the solution shall record the action;		
8100	Supplemental Resource Recommendations	As a Dispatcher, I want the solution to allow for agency-configurable, non-agency units, to be recommended, limited to the closest towing company recommendation when a unit is dispatched to an accident event type. The recommendation will consider the rotation of towing companies, so that the capability is available in accordance with approved operational requirements.	AC 1 Given agency-configurable non-agency units limited to towing companies are defined, When a unit is dispatched to a qualifying event type limited to an accident, Then the solution shall recommend the non-agency unit; AC 2 Given towing company rotation is configured, When a towing recommendation is made, Then the solution shall consider the rotation of towing companies; AC 3 Given an Authorized User configures non-agency unit recommendations, When the configuration is saved, Then the solution shall persist the configuration; AC 4 Given a recommended non-agency unit is selected, When the selection is made, Then the solution shall associate the non-agency unit with the event; AC 5 Given no eligible non-agency unit is available, When a recommendation is requested, Then the solution shall indicate that none is available;		
8101	Supplemental Resource Selection	As a Dispatcher, I want the solution to accommodate selection from the provided list either at random, by geographic proximity to the site of need, or by rotation, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a provided list of eligible providers, When a selection is made, Then the solution shall accommodate selection at random, by geographic proximity to the site of need, or by rotation; AC 2 Given a selection method is configured, When a selection occurs, Then the solution shall apply the configured selection method; AC 3 Given proximity-based selection is used, When the selection occurs, Then the solution shall select based on geographic proximity to the site of need; AC 4 Given rotation-based selection is used, When the selection occurs, Then the solution shall select the next provider in the rotation;		
8102	Resource Rotation Trigger	As a Dispatcher, I want the solution to trigger the next provider in the rotation, when selected by rotation and upon creation of the record, so that the capability is available in accordance with approved operational requirements.	AC 1 Given rotation-based selection is used, When a provider is selected by rotation upon creation of the record, Then the solution shall trigger the next provider in the rotation; AC 2 Given the next provider in rotation is triggered, When the record is created, Then the solution shall advance the rotation sequence; AC 3 Given the next provider in rotation is unavailable, When rotation advances, Then the solution shall move to the next eligible provider; AC 4 Given a rotation selection occurs, When it is recorded, Then the solution shall retain a record of the selection for policy verification;		

8104	Dynamic Event Updates	As a Dispatcher, I want the solution to have the ability to update the CFS event with notations, updates, status changes, and notifications, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CFS event, When a user adds notations, updates, status changes, or notifications, Then the solution shall update the CFS event accordingly; AC 2 Given a status change is entered on a CFS event, When it is applied, Then the solution shall update the event status; AC 3 Given a status change is entered on a CFS event, When it is applied, Then the solution shall record the change; AC 4 Given a notification is generated from a CFS event update, When the update occurs, Then the solution shall issue the notification; AC 5 Given dynamic updates are applied, When they are saved, Then the solution shall record each update in the event history with the user and time; AC 6 Given required information for an update is incomplete, When it is submitted, Then the solution shall identify the missing information; AC 7 Given required information for an update is incomplete, When it is submitted, Then the solution shall prevent completion;		
8107	Event Disposition	As a Dispatcher, I want the solution to provide for the CFS event to contain the disposition of the incident, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CFS event, When a disposition is recorded for the incident, Then the solution shall provide for the CFS event to contain the disposition of the incident; AC 2 Given a disposition is contained in the CFS event, When the event is viewed, Then the solution shall display the incident disposition with the event; AC 3 Given a disposition is required for the event, When the event is closed, Then the solution shall ensure the disposition is recorded; AC 4 Given a disposition is updated, When the change is saved, Then the solution shall record the updated disposition in the event history;		
8111	Duplicate Incident Search Radius	As a Dispatcher, I want the solution to support all incidents located within the solution's duplicate incident search radius to be checked as potential duplicates, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a configured duplicate incident search radius, When a new incident is located, Then the solution shall check all incidents within the search radius as potential duplicates; AC 2 Given potential duplicates are identified, When the check completes, Then the solution shall present the potential duplicates to the dispatcher; AC 3 Given no incidents fall within the search radius, When the check is performed, Then the solution shall indicate that no potential duplicates were found; AC 4 Given a potential duplicate is confirmed or dismissed by the dispatcher, When the action occurs, Then the solution shall record the disposition of the potential duplicate;		
8120	Back-Entered Record Audit	As a Dispatcher, I want the solution to log the entering individual's information and time of entry, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a record is back entered, When the entry is made, Then the solution shall log the entering individual's information and the time of entry; AC 2 Given a back-entered record is logged, When an Authorized User reviews it, Then the solution shall display the entering individual and time of entry; AC 3 Given a back entry is made, When it is saved, Then the solution shall associate the entry information with the record;		
8121	Back-Entered Event Data	As a Dispatcher, I want the solution to include all the information in back entered records that a live incident/event sheet should require, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a record is back entered, When the entry is created, Then the solution shall include all the information that a live incident/event sheet requires; AC 2 Given a back-entered record is missing required information, When it is submitted, Then the solution shall identify the missing information; AC 3 Given a back-entered record is missing required information, When it is submitted, Then the solution shall prevent completion; AC 4 Given a complete back-entered record is created, When it is saved, Then the solution shall retain the record with the same required information as a live event sheet; AC 5 Given a back-entered record is viewed, When an Authorized User accesses it, Then the solution shall present the complete record information;		
8127	SOP Prompting and Guidance	As a Dispatcher, I want the solution to provide SOP tool to prompt the user to ask for additional information, perform certain tasks, or relay critical information to responding units or other responders, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an SOP tool is configured, When an condition occurs, Then the solution shall prompt the user to ask for additional information, perform certain tasks, or relay critical information to responding units or other responders; AC 2 Given an SOP prompt is presented, When the user responds, Then the solution shall record the user's response or action; AC 3 Given an SOP prompt requires acknowledgment, When the user acknowledges it, Then the solution shall record the acknowledgment; AC 4 Given an Authorized User configures SOP prompts, When the configuration is saved, Then the solution shall apply the configured prompts to conditions;		
8128	Contextual SOP Retrieval	As a Dispatcher, I need the solution to provide a method where the retrieval of the SOPs is accessible from the CFS event information window and is associated with the location, incident type, unit, or special skilled personnel responding, so that the capability is available in accordance with approved operational requirements.	AC 1 Given SOPs are associated with a location, incident type, unit, or specially skilled responding personnel, When the dispatcher accesses the CFS event information window, Then the solution shall make the SOPs accessible from that window; AC 2 Given SOPs are associated with an event's context, When the event is processed, Then the solution shall retrieve the SOPs based on that context; AC 3 Given no SOPs are associated with an event's context, When the dispatcher requests them, Then the solution shall indicate that no SOPs exist; AC 4 Given SOP associations are configured, When an Authorized User changes them, Then the solution shall apply the updated associations to subsequent retrieval;		
8129	Incident-Specific SOP Access	As a Dispatcher, I need the solution to make these SOPs available for viewing or transmitting when an associated incident type is encountered, the response is designated to a specific location with unique response or operational requirements, or specialized units are assigned to the incident, so that the capability is available in accordance with approved operational requirements.	AC 1 Given SOPs are associated with an incident type, a specific location with unique response requirements, or assigned specialized units, When the associated condition is encountered, Then the solution shall make the SOPs available for viewing or transmitting; AC 2 Given an SOP is available for an encountered condition, When the dispatcher transmits it, Then the solution shall transmit the SOP to the responders; AC 3 Given an SOP is viewed or transmitted, When the action occurs, Then the solution shall record the action; AC 4 Given the associated condition is not encountered, When an event is processed, Then the solution shall present the SOP only when its associated condition is encountered.;		
8131	Co-Dispatch	As a Dispatch Supervisor, I want the solution to enable a supervisor, or another dispatcher with configured solution permissions, to co-dispatch the units under the control of another dispatcher, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a supervisor or another dispatcher with configured permissions, When that user co-dispatches units under the control of another dispatcher, Then the solution shall allow the co-dispatch of those units; AC 2 Given a user lacks the permissions to co-dispatch another dispatcher's units, When the user attempts it, Then the solution shall prevent the action; AC 3 Given units are co-dispatched, When the co-dispatch occurs, Then the solution shall associate the actions with the co-dispatching user; AC 4 Given a co-dispatch action is taken, When it is saved, Then the solution shall record the action in the event history; AC 5 Given units are co-dispatched by another user, When the controlling dispatcher views the units, Then the solution shall reflect the co-dispatched assignments;		

8146	Configurable Incident Types and Nature Codes	As a System Administrator, I need the solution to allow me to define and maintain CAD incident types and nature codes, so that incident classification can be configured to support agency-specific operational requirements.	AC 353.1 Given a system administrator defines CAD incident types and nature codes, When the definition is saved, Then the system shall persist the incident types and nature codes; AC 353.2 Given incident types and nature codes are defined, When incidents are classified, Then the system shall apply the configured incident types and nature codes; AC 353.3 Given a user lacks permission to define incident types or nature codes, When the user attempts the change, Then the system shall prevent the modification; AC 353.4 Given incident types or nature codes are changed, When the change is saved, Then the system shall record the change with the user and time;		
8147	Configurable Incident, Nature, and Disposition Codes	As a System Administrator, I want the solution to allow me to define and maintain CAD incident types, nature codes, and disposition codes, so that event classification and disposition can be configured to support agency-specific operational requirements.	AC 1 Given a system administrator defines CAD incident types, nature codes, and disposition codes, When the definition is saved, Then the solution shall persist the incident types, nature codes, and disposition codes; AC 2 Given these codes are defined, When events are classified and dispositioned, Then the solution shall apply the configured codes; AC 3 Given a user lacks permission to define these codes, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given any of these codes are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8148	Supplemental Event Information and Updates	As a Dispatcher, I want the solution to support entry of supplemental information and updates to existing event information, so that event records can be maintained throughout the incident lifecycle.	AC 1 Given an existing event, When a dispatcher enters supplemental information and updates, Then the solution shall support entry of the supplemental information and updates; AC 2 Given supplemental information is entered, When it is saved, Then the solution shall apply the updates to the event record; AC 3 Given supplemental information is entered, When it is saved, Then the solution shall record them in the event history; AC 4 Given required information for an update is incomplete, When it is submitted, Then the solution shall identify the missing information; AC 5 Given required information for an update is incomplete, When it is submitted, Then the solution shall prevent completion; AC 6 Given updates are entered throughout the incident lifecycle, When they are saved, Then the solution shall maintain the event record;		
8155	CFS Event Creation	As a Dispatcher, I want the solution to allow authorized users to create new CFS events based on the source of event information, so that events can be entered regardless of whether the information is received by a call taker or dispatcher.	AC 1 Given event information is received from a call taker or a dispatcher, When an Authorized User creates a new CFS event based on the source of the information, Then the solution shall create the CFS event according to the source; AC 2 Given a CFS event is created from a given source, When it is created, Then the solution shall associate the event with the source; AC 3 Given required CFS information is incomplete, When the user submits it, Then the solution shall identify the missing information; AC 4 Given required CFS information is incomplete, When the user submits it, Then the solution shall prevent creation; AC 5 Given a CFS event is created, When it is saved, Then the solution shall make the event available for processing;		
8156	Multi-Agency CFS Event Linking	As a Dispatcher, I want the solution to create linked copies of a CFS event for additional agencies, services, or interfaced solutions, with a unique incident/event number for each copy, so that each agency can manage its event independently while CAD users can identify all related records as part of the same incident.	AC 1 Given a CFS event that applies to additional agencies, services, or interfaced solutions, When linked copies are created, Then the solution shall create linked copies of the CFS event with a unique incident/event number for each copy; AC 2 Given linked copies are created, When they exist, Then the solution shall allow each agency to manage its event independently; AC 3 Given linked copies exist, When a CAD user views them, Then the solution shall identify all related records as part of the same incident; AC 4 Given a linked copy is updated, When the update occurs, Then the solution shall maintain each linked copy independently; AC 5 Given a unique number cannot be assigned to a copy, When the copy is created, Then the solution shall identify the condition; AC 6 Given a unique number cannot be assigned to a copy, When the copy is created, Then the solution shall prevent an invalid duplicate number; AC 7 Given linked copies are created, When they are created, Then the solution shall record the relationship among the related records;		
8158	Dynamic Unit Staffing Status	As a Dispatcher, I want the solution to allow me to document whether a unit is staffed or unstaffed before or after assignment to an incident, so that current unit staffing status is available to support accurate resource assignment and dispatch decisions.	AC 1 Given a unit, When a dispatcher documents whether the unit is staffed or unstaffed before or after assignment to an incident, Then the solution shall record the unit's staffing status; AC 2 Given a unit's staffing status is documented, When it is saved, Then the solution shall make the current staffing status available to support resource assignment and dispatch decisions; AC 3 Given a unit's staffing status changes, When the dispatcher updates it, Then the solution shall update the status; AC 4 Given a unit is unstaffed, When a dispatcher attempts to dispatch it, Then the solution shall reflect the unstaffed status for the decision; AC 5 Given a staffing status change is made, When it is saved, Then the solution shall record the change with the user and time;		
8159	Minimum Resource Complement Alerts	As a Dispatcher, I want the solution to warn me when a resource complement falls below a configured minimum, so that staffing deficiencies can be identified and addressed during operations.	AC 1 Given a configured minimum resource complement, When a unit's complement falls below the configured minimum, Then the solution shall warn the dispatcher of the staffing deficiency; AC 2 Given a below-minimum warning is generated, When the dispatcher views it, Then the solution shall identify the affected unit and the deficiency; AC 3 Given the complement is restored to or above the minimum, When staffing is updated, Then the solution shall clear the warning; AC 4 Given an Authorized User configures the minimum complement, When the configuration is saved, Then the solution shall apply the configured minimum to subsequent evaluation;		
8160	Call Type and Jurisdiction Dispositions	As a Dispatcher, I want the solution to require a disposition based on configured call type and jurisdiction, so that incident outcomes are documented according to configured requirements.	AC 1 Given disposition requirements configured by call type and jurisdiction, When an incident of a matching call type and jurisdiction is closed, Then the solution shall require a disposition; AC 2 Given a required disposition is not provided, When the user attempts to close the incident, Then the solution shall prevent closure until a disposition is entered; AC 3 Given a call type and jurisdiction do not require a disposition, When the incident is closed, Then the solution shall make the disposition optional at closure.; AC 4 Given disposition requirements are changed, When an Authorized User saves the configuration, Then the solution shall apply the updated requirements to subsequent incidents;		
8161	Assisting Unit Dispositions	As a Responder, I want the solution to allow assisting and authorized units to enter one or more dispositions for a CFS when required by agency policy, so that the actions and outcomes of each assigned unit are documented.	AC 1 Given agency policy requires it, When an assisting unit enters one or more dispositions for a CFS, Then the solution shall record the dispositions for that assisting unit; AC 2 Given multiple assisting units are on a CFS, When each enters its dispositions, Then the solution shall maintain each unit's dispositions independently; AC 3 Given a disposition entry is incomplete, When an assisting unit submits it, Then the solution shall identify the missing information; AC 4 Given a disposition entry is incomplete, When an assisting unit submits it, Then the solution shall prevent completion; AC 5 Given assisting-unit dispositions are recorded, When an Authorized User views the CFS, Then the solution shall display each assisting unit's dispositions; AC 6 Given agency policy does not require assisting-unit dispositions, When the CFS is closed, Then the solution shall make assisting-unit dispositions optional.;		

8162	Resource Identification and Information	As a Dispatcher, I want the solution to display associated resource details with information that supports resource identification, location, and purpose, so that I can select and manage resources during incident operations.	AC 1 Given resources with identification, location, and purpose information, When a dispatcher views resources during incident operations, Then the solution shall display the associated resource details; AC 2 Given resource details are displayed, When the dispatcher selects and manages resources, Then the solution shall present the information needed to select and manage resources; AC 3 Given a resource's details change, When the change occurs, Then the solution shall update the displayed resource details; AC 4 Given resource detail information is unavailable, When the dispatcher views the resource, Then the solution shall indicate that the information is unavailable;		
8163	Dynamic Unit Staffing and Crew Capability Management	As a Dispatcher, I want the solution to account for the number of personnel currently staffed on each unit and allow authorized users to modify unit crew capabilities as staffing changes throughout the day, so that resource availability and capabilities reflect current operational conditions.	AC 1 Given units with assigned personnel, When the solution accounts for staffing, Then the solution shall account for the number of personnel currently staffed on each unit; AC 2 Given staffing changes throughout the day, When an Authorized User modifies a unit's crew capabilities, Then the solution shall apply the change and reflect current operational conditions; AC 3 Given crew capabilities are modified, When the change is saved, Then the solution shall update the unit's resource availability and capabilities; AC 4 Given a user lacks permission to modify crew capabilities, When the user attempts it, Then the solution shall prevent the change; AC 5 Given a crew capability change is made, When it is saved, Then the solution shall record the change with the user and time;		
8165	Dynamic Unit Recommendation Updates	As a Dispatcher, I want the solution to update unit recommendations when associated incident information changes with incident type, location, or alarm level, so that resource recommendations reflect current incident conditions without requiring manual intervention.	AC 1 Given associated incident information changes with incident type, location, or alarm level, When a recommendation exists for the incident, Then the solution shall update the unit recommendations; AC 2 Given unit recommendations are updated, When the change occurs, Then the solution shall reflect current incident conditions without requiring manual intervention; AC 3 Given a dispatcher has overridden a recommendation, When incident information changes, Then the solution shall handle the recommendation update in accordance with configured rules; AC 4 Given recommendation-affecting data is unavailable, When the solution attempts to update, Then the solution shall indicate the limitation; AC 5 Given recommendations are updated, When the update occurs, Then the solution shall make the current recommendations available to the dispatcher;		
8166	Concurrent CFS Update Conflict Management	As an Authorized User, I want the solution to identify when another user has modified a CFS field since I retrieved the event and prompt me before overwriting the change, so that concurrent updates do not unintentionally overwrite information entered by another user.	AC 1 Given a user retrieved a CFS event, When another user has modified a field since the retrieval, Then the solution shall identify that the field was modified; AC 2 Given a concurrent modification is identified, When the user attempts to overwrite the change, Then the solution shall prompt the user before overwriting; AC 3 Given the user confirms the overwrite, When confirmation is provided, Then the solution shall apply the change; AC 4 Given the user declines the overwrite, When the prompt is dismissed, Then the solution shall preserve the other user's change; AC 5 Given a concurrent modification is resolved, When the resolution occurs, Then the solution shall record the outcome in the event history;		
8178	Automatic CFS Event Notification Rules	As a System Administrator, I want the solution to allow authorized administrators to define rules for automatic CFS event notifications with events, notification conditions, recipients, and notification methods, so that event notifications are generated according to approved operational requirements.	AC 1 Given an authorized administrator defines rules for automatic CFS event notifications, When the administrator configures the events, notification conditions, recipients, and notification methods, Then the solution shall persist the notification rules; AC 2 Given automatic notification rules are configured, When a qualifying event and condition occur, Then the solution shall generate the notification to the configured recipients using the configured methods; AC 3 Given an event does not meet the notification conditions, When the event occurs, Then the solution shall withhold the notification.; AC 4 Given a user lacks permission to configure notification rules, When the user attempts the change, Then the solution shall prevent the modification; AC 5 Given notification rules are changed, When the change is saved, Then the solution shall apply the updated rules to subsequent events;		
8182	SOP Association and Management	As a System Administrator, I need the solution to store and associate SOPs with incident types, properties, or units, so that configured procedures can be accessed based on operational context.	AC 1 Given an authorized administrator stores and associates SOPs with incident types, properties, or units, When the association is saved, Then the solution shall persist the SOP associations; AC 2 Given SOPs are associated with an operational context, When that context applies, Then the solution shall make the SOPs accessible; AC 3 Given a user lacks permission to store or associate SOPs, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given SOP associations are changed, When the change is saved, Then the solution shall apply the updated associations to subsequent access;		
8194	Configurable Duplicate Event Search Radius	As a System Administrator, I want the solution to allow authorized administrators to configure the geographic search radius with the unit of measurement, used to identify potential duplicate events based on an incident's location or coordinates, so that duplicate event detection can be applied using agency-defined criteria.	AC 1 Given an authorized administrator configures the geographic search radius with the unit of measurement, used to identify potential duplicate events, When the configuration is saved, Then the solution shall persist the duplicate-event search radius; AC 2 Given the search radius is configured, When duplicate-event detection is performed, Then the solution shall apply the configured radius based on an incident's location or coordinates; AC 3 Given an invalid radius value is entered, When the administrator attempts to save it, Then the solution shall identify the invalid value; AC 4 Given an invalid radius value is entered, When the administrator attempts to save it, Then the solution shall prevent saving; AC 5 Given the search radius is changed, When the change is saved, Then the solution shall apply the updated criteria to subsequent duplicate detection;		
8198	Informational Incident Records	As a Dispatcher, I want the solution to create and manage informational incident records and radio-log records with durable identifiers that do not consume agency case numbers, so that non-case activities can be documented, searched, and tracked without creating unnecessary case records.	AC 1 Given informational incidents and radio-log records, When a dispatcher creates such a record, Then the solution shall create the record with a durable identifier that does not consume an agency case number; AC 2 Given informational and radio-log records exist, When an Authorized User searches for them, Then the solution shall allow the records to be searched and tracked; AC 3 Given a non-case activity is documented, When the record is created, Then the solution shall record the non-case activity as a non-case entry.; AC 4 Given a durable identifier is assigned, When the record is referenced, Then the solution shall maintain the identifier for the life of the record; AC 5 Given an informational or radio-log record is created or updated, When it is saved, Then the solution shall retain the record with its history;		

8199	Parent and Child Incident Management	As a Dispatcher, I want the solution to create a parent dispatch incident and associate related law enforcement, fire, EMS, or informational incidents as child records, so that related activities can be managed independently while maintaining their relationship to the originating event.	AC 1 Given a dispatch incident, When a dispatcher creates a parent dispatch incident and associates related law enforcement, fire, EMS, or informational incidents, Then the solution shall associate the related incidents as child records of the parent; AC 2 Given parent and child records exist, When a child record is managed, Then the solution shall allow the child record to be managed independently while maintaining its relationship to the parent; AC 3 Given related records are associated, When an Authorized User views any of them, Then the solution shall identify the parent-child relationship among the records; AC 4 Given a child record is updated, When the update occurs, Then the solution shall maintain each record independently; AC 5 Given a parent dispatch incident is created, When child records are associated, Then the solution shall preserve the relationship to the originating event; AC 6 Given a user lacks permission to associate or manage related records, When the user attempts it, Then the solution shall prevent the action;		
8217	Call-Taker to Dispatcher Handoff	As a Call-Taker or Dispatcher, I want the solution to support a configurable call-intake model in which a call-taker can capture and hand off a call to a dispatcher within the same communications center, so that DPS can operate either a combined call-taker/dispatcher role or separate roles according to each center's staffing model.	AC 1 Given an authorized administrator configures the call-intake model, When the configuration is saved, Then the solution shall apply either a combined call-taker/dispatcher role or separate call-taker and dispatcher roles as configured.; AC 2 Given a call-taker captures call information, When the call-taker hands the call off to a dispatcher, Then the solution shall transfer the call and its captured information without requiring re-entry.; AC 3 Given a call is handed off between positions within the center, When the handoff occurs, Then the solution shall record the originating and receiving users with date and time.; AC 4 Given the center operates a combined role, When a single user performs both call-taking and dispatching, Then the solution shall allow the user to proceed without a handoff step.; AC 5 Given a handoff is pending acceptance, When the receiving dispatcher is unavailable, Then the solution shall retain the call in the configured intake queue until accepted.;		
8218	Validation Override for Incomplete or Flagged Conditions	As a Dispatcher, I want the solution to allow me to override configured validation rules and create an incident or complete an assignment after being warned of missing or flagged information, so that time-critical incidents can be initiated and resources committed even when complete information is not yet available.	AC 1 Given required incident information is missing, When the dispatcher attempts to create the incident, Then the solution shall warn the dispatcher of the specific missing information.; AC 2 Given required incident information is missing, When the dispatcher attempts to create the incident, Then the solution shall allow an authorized override to create the incident.; AC 3 Given a dispatcher overrides validation to create an incomplete incident, When the override is applied, Then the solution shall create the incident.; AC 4 Given a dispatcher overrides validation to create an incomplete incident, When the override is applied, Then the solution shall flag it as containing incomplete information for follow-up.; AC 5 Given a resource is flagged as unavailable or ineligible, When the dispatcher elects to proceed, Then the solution shall allow an authorized override of the assignment or reassignment.; AC 6 Given an override is performed, When the action is saved, Then the solution shall record the override, the overriding user, the reason where configured, and the date and time.; AC 7 Given a user lacks override permission, When the user attempts to bypass validation, Then the solution shall prevent the override.; AC 8 Given an incident was created with incomplete information, When the missing information becomes available, Then the solution shall allow an Authorized User to complete the record and clear the incomplete flag.;		
8219	Second-Level Time Precision for Event Timestamps	As a Dispatcher, I want the solution to record and display event timestamps with second-level precision (HH:MM:SS), so that the timing of calls, dispatches, arrivals, and status changes can be documented and reviewed.	AC 1 Given a date/time is recorded for any call, incident, dispatch, arrival, or status event, When the event is saved, Then the solution shall record the time with second-level precision.; AC 2 Given a timestamp is displayed to an Authorized User, When the record is viewed, Then the solution shall present the time in HH:MM:SS format.; AC 3 Given event records are exported or reported, When the output is generated, Then the solution shall retain second-level precision in the output.; AC 4 Given timestamps are recorded across integrated components, When events are logged, Then the solution shall apply a consistent, synchronized time source.;		
8223	Dispatcher Escalation of Public Submission to CFS	As a Dispatcher, I want the solution to allow me to create a dispatchable CFS event from a public non-dispatchable submission when circumstances warrant, so that a public report can be escalated to an incident at dispatcher discretion.	AC 1 Given a public non-dispatchable submission exists, When an authorized dispatcher elects to escalate it, Then the solution shall create a dispatchable CFS event from the submission.; AC 2 Given a CFS event is created from a submission, When the event is created, Then the solution shall carry forward the submission information without re-entry.; AC 3 Given a submission is escalated to a CFS event, When the event is created, Then the solution shall maintain the relationship between the original case and the new event.; AC 4 Given a dispatcher reviews a submission, When escalation criteria are not met or not selected, Then the solution shall retain the submission as a non-dispatchable case.; AC 5 Given a submission is escalated, When the action occurs, Then the solution shall record the escalating user and date/time.;		
8224	Multi-Incident Comment Routing	As a Dispatcher, I want the solution to apply a comment entered on a linked multi-agency dispatch to all related incidents by default while allowing a comment to be directed to a single specified incident, so that shared information reaches all responders and incident-specific information is kept to the incident.	AC 1 Given multiple related incidents are linked to a single dispatch, When a dispatcher enters a standard comment, Then the solution shall apply the comment to all related incidents.; AC 2 Given a dispatcher intends a comment for a single incident, When the dispatcher designates the target incident, Then the solution shall apply the comment only to the designated incident.; AC 3 Given a comment is applied to one or more incidents, When an Authorized User views an incident, Then the solution shall display the comments to that incident.; AC 4 Given a comment is directed to a single incident, When the comment is saved, Then the solution shall apply the comment only to the specified incident.; AC 5 Given a comment is entered, When it is saved, Then the solution shall record the entering user and date/time for each incident to which it applies.;		
8225	Held-Event Readiness Notification	As a Dispatcher, I want the solution to notify me when a unit that has a CFS event held for it becomes available (clears its current incident), so that the pending held event can be dispatched without delay.	AC 1 Given a CFS event is held for a specific unit, When that unit clears its current incident and becomes available, Then the solution shall notify the dispatcher that a held event is pending for the unit.; AC 2 Given a held-event notification is generated, When the dispatcher views it, Then the solution shall identify the unit and the held event.; AC 3 Given a held event is dispatched or released, When the action occurs, Then the solution shall clear the pending notification.; AC 4 Given multiple events are held for a unit, When the unit becomes available, Then the solution shall identify each pending held event.; AC 5 Given a held-event notification occurs, When the action is recorded, Then the solution shall retain the notification in the event history.;		
8226	Independent Unit Activity Logging	As a Dispatcher, I want the solution to log a status or activity update for a unit that is not related to the incident the unit is currently assigned to, so that unit activity occurring outside an assigned call can be documented.	AC 1 Given a unit is assigned to an incident, When the dispatcher logs an unrelated unit update, Then the solution shall record the update against the unit without associating it with the assigned incident.; AC 2 Given an independent unit update is recorded, When an Authorized User reviews unit activity, Then the solution shall display the update with date/time.; AC 3 Given an independent unit update is recorded, When the unit's assigned incident is reviewed, Then the solution shall associate the unit update only with its related records.; AC 4 Given an independent unit update affects unit status, When the update is saved, Then the solution shall reflect the current unit status accordingly.;		

8241	UAV / Drone Deployment Tracking	As a Dispatcher, I want to track Unmanned Aerial Vehicle (UAV) resources and their deployment to incidents, so that drone assets are managed and documented like other dispatchable resources.	AC 1 Given UAV resources are configured, When a dispatcher assigns a UAV to an incident, Then the solution shall record the assignment and status like other resources.; AC 2 Given a UAV is deployed, When status updates occur, Then the solution shall track and retain the UAV status and times with the incident.; AC 3 Given a UAV deployment is recorded, When the incident is reviewed or reported, Then UAV activity shall be available in the incident history and reports.; AC 4 Given UAV-specific attributes exist, When resources are managed, Then the solution shall support configurable UAV resource attributes and capabilities.;		
8242	Incident Radio Log Printing	As a Dispatcher, I want the solution to print the radio log associated with a selected incident, event, unit, channel, or specified time period, so that radio communications can be produced in a readable format for reference, review, and records.	AC 1 Given radio log entries are associated with an incident, event, unit, channel, or time period, When an Authorized User selects that scope, Then the solution shall retrieve the associated radio log entries for printing.; AC 2 Given a radio log scope is selected, When the user requests a printout, Then the solution shall generate a printable radio log containing the entry details with timestamp, channel, unit, and entry text.; AC 3 Given a radio log is generated for printing, When the output is produced, Then the solution shall present the entries in chronological order with the incident, event, unit, and channel identifiers.; AC 4 Given a radio log printout is requested, When the user selects an output option, Then the solution shall support printing and export to a standard format limited to PDF.; AC 5 Given a radio log is printed or exported, When the output is produced, Then the solution shall record the action consistent with configured audit and retention rules.;		
8791	Send Automatic and Manual Notifications	As an authorized user, I want the solution to send automatic and manual notifications to predefined recipients through configured channels, so that personnel receive the notifications they need.	AC 1 Given predefined recipients or groups and configured channels are set up, When an automatic or manual notification is triggered, Then the solution shall send the notification to the designated recipients through the configured channels.; AC 2 Given a notification is configured for text messaging or email, When the notification is sent, Then the solution shall deliver it using the configured channel.; AC 3 Given an authorized user composes a manual notification, When the user sends it, Then the solution shall deliver the notification to the selected recipients or groups.;		
8792	Present Visual and Audible Alerts	As an authorized user, I want workstation alerts to be visual and audible, so that notifications are noticed.	AC 1 Given a notification is presented at a workstation, When the notification occurs, Then the solution shall provide informative visual and audible indication.; AC 2 Given workstation alerting is configured, When an alert is presented, Then the solution shall apply the configured visual and audible alert settings.; AC 3 Given a visual and audible alert is presented, When the user has not acknowledged it, Then the solution shall continue the indication until the alert is acknowledged.;		
8793	Handle Notification Delivery Failures	As an authorized user, I want notification failures identified and logged, so that delivery issues are visible and auditable.	AC 1 Given a notification fails to deliver, When the failure occurs, Then the solution shall identify the delivery failure.; AC 2 Given notifications are sent, When they are processed, Then the solution shall log the notifications for audit and review.;		
8794	Acknowledge and Manage Notifications	As an authorized user, I want to acknowledge and manage active notifications, so that alerting stays manageable.	AC 1 Given multiple notifications are active, When a user manages them, Then the solution shall allow the user to acknowledge and manage the notifications.; AC 2 Given a notification has been acknowledged, When the user views active notifications, Then the solution shall update the notification status to acknowledged.; AC 3 Given multiple notifications are active, When a user dismisses a notification, Then the solution shall remove the dismissed notification from the active list.;		
8795	Capture and Retain CFS Multimedia	As a Dispatcher, I want the solution to capture, associate, and retain multimedia with a CFS event, so that multimedia is preserved with the event.	AC 1 Given multimedia data is received for a CFS event, When the solution processes it, Then the solution shall capture, associate.; AC 2 Given multimedia data is received for a CFS event, When the solution processes it, Then the solution shall retain the multimedia with the CFS event or an approved external repository.; AC 3 Given multimedia is retained in an approved external repository, When the event references it, Then the solution shall maintain the association between the event and the stored multimedia.;		
8796	Stream CFS Multimedia	As a Dispatcher, I want to stream CFS multimedia and control playback, so that I can review video and audio for an event.	AC 1 Given streaming video or audio is available for an event, When an authorized user accesses it, Then the solution shall support streaming of the video and audio.; AC 2 Given a multimedia feed is playing, When an authorized user controls playback, Then the solution shall allow the user to start, stop, pause, rewind, and resize the feed.;		
8797	Access CFS Multimedia	As a Dispatcher, I want to access multimedia linked to an event, so that authorized users can use it operationally and historically.	AC 1 Given multimedia is associated with an event, When an authorized user views the event, Then the solution shall make the linked multimedia accessible for operational and historical purposes.; AC 2 Given a user lacks permission to access multimedia, When the user attempts access, Then the solution shall prevent the		
8798	Audit CFS Multimedia Actions	As an authorized user, I want multimedia actions recorded for audit, so that access and capture are traceable.	AC 1 Given multimedia is captured or accessed, When the action occurs, Then the solution shall record the action for audit purposes.; AC 2 Given a multimedia action is recorded, When the action occurs, Then the solution shall record the user, action type, and date and time.; AC 3 Given multimedia audit records exist, When an authorized user reviews them, Then the solution shall present the recorded multimedia actions for traceability.;		
8822	Reference Source Lookup	As a Dispatcher, I want the solution to provide access to reference sources such as statutes, NCIC code manuals, and DMV conviction codes, so that authorized users can look up and apply the correct codes during call handling and reporting.	AC 1 Given reference sources are configured, When an authorized user performs a lookup, Then the solution shall return the matching reference information.; AC 2 Given a user is entering coded information, When a reference code is required, Then the solution shall make the applicable code list available for selection.; AC 3 Given reference sources are updated by an authorized administrator, When a subsequent lookup is performed, Then the solution shall return the current approved reference data.; AC 4 Given a reference lookup returns no result, When the outcome occurs, Then the solution shall notify the user.; AC 5 Given reference data is applied to a record, When the record is saved, Then the solution shall retain the selected reference values.;		
8827	RapidSOS Device-Based Location Integration	As a Call-Taker, I want the solution to receive supplemental device-based location from RapidSOS during 9-1-1 call handling, so that I can more precisely locate callers from smartphones and connected devices.	AC 1 Given a 9-1-1 call is being handled, When RapidSOS provides supplemental device-based location, Then the solution shall receive and display the location to the call-taker.; AC 2 Given RapidSOS location is received, When it is displayed, Then the solution shall associate it with the active call record and show it on the map.; AC 3 Given both RapidSOS and other location sources are available, When they are presented, Then the solution shall identify the source of each location.; AC 4 Given RapidSOS location is unavailable or fails, When a call is handled, Then the solution shall continue with available location information.; AC 5 Given RapidSOS location is unavailable or fails, When a call is handled, Then the solution shall record the outcome.; AC 6 Given RapidSOS location data is received, When the call completes, Then the solution shall retain the location data with the call record for audit.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**

EPIC 02: CAD Response, GIS & Mapping					
7805	Caller Location Validation	As a Dispatcher, I want the solution to validate available caller location information against available GIS and address data, so that I can use validated location information when handling an emergency call or incident.	AC 1 Given caller location information is available, When the solution validates the location against available GIS and address data, Then the solution shall determine whether the location is valid according to configured validation rules.; AC 2 Given the location matches available GIS information, When validation is completed, Then the solution shall identify the location as validated.; AC 3 Given the location does not match available GIS information, When validation is completed, Then the solution shall identify the location as requiring attention.; AC 4 Given a location requires correction, When an authorized dispatcher updates the location, Then the solution shall retain the corrected location according to configured rules.; AC 5 Given a location has been validated, When the dispatcher views the incident, Then the validated location shall be available for response operations.;		
7818	Integrated GIS Imagery and Incident Attachments	As an Authorized User, I want the solution to associate supporting files with incidents or cases and integrate high-resolution aerial imagery, shape files, and vector data with the mapping system, so that operational records and geographic information can be accessed together to support incident response and analysis.	AC 1 Given an Authorized User selects a supporting file, When the file is associated with an incident or case, Then the solution shall retain the file relationship.; AC 2 Given an attached file is associated with an incident, When an Authorized User views the incident, Then the user shall be able to access the file according to permissions.; AC 3 Given approved aerial imagery is available, When an Authorized User opens the supported map, Then the mapping system shall display the imagery.; AC 4 Given approved shape or vector data is available, When an Authorized User opens the supported map, Then the mapping system shall display the geographic data.; AC 5 Given geographic data is associated with an incident, When the incident is viewed on the map, Then the geographic information shall be available in context.; AC 6 Given a user lacks authorization to access an attached file or geographic data, When the user attempts access, Then the solution shall restrict access.;		
7846	Time-Limited Premises Information Management	As a Dispatcher, I want the solution to maintain premises information with configurable effective and expiration dates and notify designated supervisors of upcoming expirations, so that time-sensitive premises information remains current and available for incident response.	AC 1 Given premises information is entered, When an Authorized User saves the premises record, Then the solution shall require or retain the configured effective date.; AC 2 Given premises information has an expiration date, When the information is saved, Then the solution shall retain the expiration date.; AC 3 Given premises information is currently effective, When a dispatcher views an incident, Then the current premises information shall be available according to configuration.; AC 4 Given a premises expiration date is approaching, When the configured notification threshold is reached, Then the solution shall notify the designated supervisor.; AC 5 Given premises information expires, When the expiration date is reached, Then the solution shall identify the information as expired according to configured rules.;		
7931	Enterprise GIS Mapping and Integration	As an Authorized User, I need the CAD solution to provide native GIS mapping capabilities that utilize approved State enterprise GIS services and authoritative geographic data, including statewide map layers published by VCGI through Esri ArcGIS services, with integration capabilities as needed, so that incident locations and mapping information remain accurate and consistent with State geographic standards and support dispatch, routing, situational awareness, and field operations.	AC 1 Given the CAD solution provides GIS mapping capabilities, When an authorized CAD user accesses the mapping interface, Then the system shall provide native GIS mapping functionality for viewing and interacting with geographic data.; AC 2 Given approved State enterprise GIS services are available, When the CAD solution retrieves geographic data, Then the system shall utilize approved State GIS services and authoritative geographic data, including statewide map layers published by VCGI through Esri ArcGIS services, through native functionality or approved integrations.; AC 3 Given authoritative geographic data and map layers are available, When a CAD user views a map, Then the CAD solution shall display the applicable geographic information using the approved State map layers and geographic data.; AC 4 Given an incident location is entered, received, or updated, When the CAD solution processes the location, Then the system shall support locating and displaying the incident on the GIS map using the applicable geographic data and coordinate information.; AC 5 Given GIS map information is available, When a CAD user performs dispatch or field operations, Then the system shall support map-based situational awareness, including the display of incident locations, responder locations, and relevant geographic features.; AC 6 Given routing or location-based operations are performed, When the CAD solution uses geographic data, Then the system shall support mapping and routing capabilities using approved geographic data and services.; AC 7 Given authoritative GIS data or map layers are updated by the State GIS source, When the CAD solution retrieves or synchronizes the updated data, Then the system shall make the updated geographic information available in accordance with the configured integration and refresh procedures.; AC 8 Given an approved GIS service or data source is unavailable or returns an error, When the CAD solution attempts to retrieve geographic information, Then the system shall indicate the applicable service or data availability status and provide available error information.; AC 9 Given GIS data and mapping services are accessed, When the CAD solution retrieves, displays, or uses geographic information, Then the system shall maintain applicable source attribution, data currency, and access controls in accordance with State GIS standards and approved security requirements.		
7945	Hydrant and Water Source Mapping	As a Dispatcher, I want to view authoritative hydrant and alternative water-source information on the CAD map, so that fire response planning can consider available water resources when determining a configured response.	AC 1 Given authoritative hydrant and alternative water-source information is available, When the Dispatcher views the CAD map, Then the solution shall display eligible water sources.; AC 2 Given a water source has geographic information, When it is displayed on the map, Then its location shall correspond to the authoritative geographic data.; AC 3 Given an incident is being evaluated for fire response, When the Dispatcher views water-source information, Then the information shall be available for response planning.;		
7981	Geographic Data Management	As a System Administrator, I need to import, update, validate, and maintain approved geographic data, so that CAD and related operational functions use accurate and current geographic information.	AC 188.1 Given approved geographic data is available for import, When the System Administrator initiates the import, Then the system shall import the supported geographic data.; AC 188.2 Given geographic data contains invalid or unsupported information, When validation is performed, Then the system shall identify the invalid information.; AC 188.3 Given geographic data has been successfully validated, When the data is applied, Then the applicable CAD functions shall use the updated geographic information.; AC 188.4 Given geographic data is updated, When an authorized administrator reviews the data, Then the current approved geographic information shall be available.		

7982	Geographic Zone and Geo-Fence Management	As a System Administrator, I want the solution to define and maintain geo-fences, response zones, street networks, and other geographic layers using GIS and mapping tools, with configurable boundaries, names, and entry and exit conditions, so that geographic areas can be defined and managed for law enforcement, fire, EMS, and other response operations.	AC 1 Given an authorized administrator creates a geo-fence, response zone, street network, or geographic layer, When the configuration is saved, Then the solution shall retain the defined geographic boundary and attributes.; AC 2 Given a geographic area has a configured name or identifier, When the area is displayed, Then the solution shall present the configured name or identifier.; AC 3 Given an area has configured entry or exit conditions, When a qualifying geographic event occurs, Then the solution shall evaluate the configured condition.; AC 4 Given an authorized administrator updates a geographic boundary, When the change is saved, Then the solution shall apply the updated boundary to CAD/RMS functions.;		
7984	Route Impediments and Alternatives	As a Dispatcher, I want the solution to identify route impediments and calculate or display available route alternatives, so that dispatchers can account for known routing conditions when supporting responder travel.	AC 1 Given approved routing and GIS data indicates an impediment on a route, When the solution evaluates the route to a destination, Then the solution shall identify the route impediment.; AC 2 Given a route impediment is identified, When the solution calculates routing, Then the solution shall calculate available route alternatives using approved routing and GIS data.; AC 3 Given available route alternatives are calculated, When a dispatcher reviews the routing, Then the solution shall display the available route alternatives.; AC 4 Given a route impediment affects responder travel, When a dispatcher reviews the route, Then the solution shall display the known routing condition.; AC 5 Given no route impediment is identified for a destination, When the solution evaluates the route, Then the solution shall display the primary route.;		
7985	Agency and Jurisdiction Assignment	As a Dispatcher, I want the solution to determine the responsible agency, jurisdiction, and service area using approved geographic and operational rules, so that incidents are directed to the operational authority.	AC 1 Given an incident has a valid location and operational information, When CAD evaluates the incident, Then the solution shall determine the responsible agency, jurisdiction, and service area using approved rules.; AC 2 Given geographic and operational rules identify a responsible agency, When the evaluation is completed, Then the solution shall assign the agency or jurisdiction.; AC 3 Given an incident crosses or falls within defined service-area boundaries, When the geographic rules are evaluated, Then the solution shall identify the service area.; AC 4 Given the solution cannot determine an assignment using the configured rules, When the evaluation is completed, Then the solution shall identify the condition for operational handling.;		
7986	Geographic Assignment Correction and Audit	As a Dispatcher or Supervisor, I want authorized users to correct an automated geographic assignment and record the reason, user, and time of the change, so that incorrect assignments can be corrected while maintaining an auditable history.	AC 1 Given an automated geographic assignment has been made, When an authorized Dispatcher or Supervisor determines that the assignment is incorrect, Then the solution shall allow the authorized user to correct the assignment.; AC 2 Given an automated geographic assignment is corrected, When the correction is saved, Then the solution shall require or retain the reason for the change.; AC 3 Given a geographic assignment is corrected, When the change is recorded, Then the solution shall retain the identity of the user who made the change and the date and time of the change.; AC 4 Given an Authorized User reviews the assignment history, When the history is retrieved, Then the original automated assignment and subsequent correction shall be available according to configured audit requirements.;		
8035	Independent Geofile Address Validation	As an Authorized User, I want the solution to perform geofile-based address validation and location lookups independently of CFS event creation, so that incident locations can be validated, confirmed, and reused before or during event creation.	AC 1 Given a geofile is available, When an Authorized User performs an address validation or location lookup independently of event creation, Then the solution shall validate the location against the geofile; AC 2 Given a geofile is available, When an Authorized User performs an address validation or location lookup independently of event creation, Then the solution shall return the result; AC 3 Given a location is validated outside of event creation, When the user subsequently creates a CFS event, Then the solution shall allow the validated location to be reused; AC 4 Given an entered location does not match the geofile, When the user performs the lookup, Then the solution shall indicate that the location could not be validated; AC 5 Given multiple candidate matches exist for a location, When the lookup is performed, Then the solution shall present the candidate matches for selection; AC 6 Given a location is validated, When the validation completes, Then the solution shall make the confirmed location available for confirmation and reuse; AC 7 Given a user performs a standalone location lookup, When the lookup occurs, Then the solution shall allow the standalone location lookup independently of any CFS event.;		
8036	Cross-Street and Jurisdiction Display	As a Dispatcher, I want the two nearest cross-streets and jurisdictional boundaries displayed, so that I can verify location.	AC 1 Given a validated incident location, When the location is displayed, Then the solution shall display the two nearest cross-streets for the location; AC 2 Given a validated incident location, When the location is displayed, Then the solution shall display the jurisdictional boundaries for the location; AC 3 Given cross-street or boundary information is unavailable for a location, When the location is displayed, Then the solution shall indicate that the information is unavailable; AC 4 Given the incident location changes, When the new location is validated, Then the solution shall update the displayed cross-streets and jurisdictional boundaries;		
8037	Caller Identification, Location Information, and Address Notification Preservation	As a Dispatcher, I want the solution to preserve originally received caller identification and location information, including ANI/ALI information where provided, display special address notifications, and allow authorized users to correct inaccurate location information in the event record, so that critical caller and location information is retained, identified, and maintained.	AC 1 Given ANI/ALI information is received from the 911 system or associated service, When the event record is created, Then the solution shall preserve the original ANI/ALI information in the event record; AC 2 Given a location has a configured special address notification, When the location is received or displayed, Then the solution shall display the special address notification; AC 3 Given an Authorized User identifies incorrect caller location information, When the user edits the ALI information in the event record, Then the solution shall apply the correction while retaining the original ANI/ALI; AC 4 Given a user is not authorized to edit caller location information, When the user attempts the edit, Then the solution shall prevent the change; AC 5 Given caller location information is edited, When the change is saved, Then the solution shall record the edit with the user and time while preserving the original received values; AC 6 Given original and edited caller location information exist, When an Authorized User views the event record, Then the solution shall distinguish the original received information from edited information;		
8057	Address Alias Management	As a Dispatcher, I want the solution to allow each address or commonplace name to have an unlimited number of alias names, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an address or commonplace name, When an Authorized User adds alias names, Then the solution shall allow an unlimited number of alias names for that address or commonplace; AC 2 Given aliases exist for an address, When a user searches by an alias, Then the solution shall resolve the alias to the correct address; AC 3 Given an alias is added or removed, When the change is saved, Then the solution shall persist the updated alias list; AC 4 Given a duplicate alias is entered for the same address, When the user attempts to save it, Then the solution shall identify the duplicate; AC 5 Given a duplicate alias is entered for the same address, When the user attempts to save it, Then the solution shall prevent its creation;		

8058	Business and Tenant Address Names	As a Dispatcher, I want the solution to allow authorized users to store multiple names for businesses and tenants for a given street address, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a street address, When an Authorized User stores multiple business and tenant names for the address, Then the solution shall persist all stored names for that address; AC 2 Given multiple business or tenant names exist for an address, When a user searches by one of the names, Then the solution shall return the associated address; AC 3 Given a user lacks permission to maintain business or tenant names, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given business or tenant names are updated, When the change is saved, Then the solution shall persist the updated names for the address;		
8059	Address Match Display	As a Dispatcher, I want the solution to display address matches in a structured list that shows each candidate's distinguishing attributes such as full address, jurisdiction, and match type, so that I can identify the valid incident location.	AC 1 Given multiple address matches result from a location search, When the matches are displayed, Then the solution shall display the address matches in a structured list; AC 2 Given address matches are displayed, When a dispatcher reviews them, Then the solution shall display each match's distinguishing attributes such as full address, jurisdiction, and match type; AC 3 Given a dispatcher selects a match from the displayed list, When the selection is made, Then the solution shall apply the selected location to the event; AC 4 Given no address matches are found, When the search is performed, Then the solution shall indicate that no matching locations were found;		
8060	Tactical Map and NENA Address Data	As a Dispatcher, I want the solution to display the incident location in relation to other active incidents on the solution's tactical map display during the CAD event entry process, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a CAD event is being entered, When the incident location is established, Then the solution shall display the incident location in relation to other active incidents on the tactical map display; AC 2 Given a data entry field contains an address, When the address is processed, Then the solution shall follow the NENA Standard for NG9-1-1 GIS Data Model 71-003, Section 3.5 with at a minimum the Site/Structure Address data elements; AC 3 Given other active incidents exist near the entered location, When the location is displayed, Then the solution shall visually distinguish the current incident location from other active incidents; AC 4 Given the entered location changes during event entry, When the new location is established, Then the solution shall update the tactical map display accordingly; AC 5 Given a required address data element is missing, When the address is entered, Then the solution shall identify the missing element in accordance with the GIS data model;		
8071	Geo-Fence and Resource Alerts	As a Dispatcher, I want the solution to provide configurable alerts with distinct visual and audible identification, resource identification, geo-fence identification, current resource position, and timestamps for geo-fence entry and exit, and allow me to clear alerts and alert history from the active display while retaining historical records, so that I can identify and manage resource activity while preserving an auditable history.	AC 1 Given configurable alerts are defined, When an alert condition occurs, Then the solution shall present the alert with distinct visual and audible identification; AC 2 Given a resource triggers a geo-fence event, When the alert is generated, Then the solution shall include resource identification, geo-fence identification, current resource position, and timestamps for geo-fence entry and exit; AC 3 Given an alert is displayed on the active display, When a dispatcher clears the alert, Then the solution shall remove it from the active display while retaining the historical record; AC 4 Given alert history exists, When a dispatcher clears alert history from the active display, Then the solution shall retain the historical records; AC 5 Given alerts and alert history have been cleared from the active display, When an Authorized User reviews history, Then the solution shall provide the retained alert history; AC 6 Given an authorized administrator configures alerts, When the configuration is saved, Then the solution shall apply the configured alert behavior;		
8108	Coordinate-Based Geographic Search	As a Dispatcher, I want the solution to support X, Y coordinate-based geographic searches for such things as nearby hazardous materials, duplicate incidents, and premises information at or near an incident's location, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an incident location with X, Y coordinates, When a coordinate-based geographic search is performed, Then the solution shall support X, Y coordinate-based searches for items limited to nearby hazardous materials, duplicate incidents, and premises information; AC 2 Given a geographic search identifies matching information at or near a location, When the search completes, Then the solution shall return the matching information; AC 3 Given no matching information exists within the search area, When the search is performed, Then the solution shall indicate that no matches were found; AC 4 Given a geographic search is performed, When results are returned, Then the solution shall associate the results with the incident location; AC 5 Given the search area is configurable, When an Authorized User adjusts it, Then the solution shall apply the adjusted search area to subsequent searches;		
8109	Configurable Location Information Databases	As a System Administrator, I want the solution to allow authorized administrators to define and maintain location-based information databases with hazards, premises information, street closures, and other user-defined geographic data, so that associated location information is available to support incident response and dispatch operations.	AC 1 Given an authorized administrator defines location-based information databases with hazards, premises information, street closures, and other user-defined geographic data, When the definition is saved, Then the solution shall persist the location-based information; AC 2 Given location-based information is maintained, When an incident occurs at or near an location, Then the solution shall make the associated location information available to support response and dispatch; AC 3 Given an administrator defines user-defined geographic data elements, When the configuration is saved, Then the solution shall support the user-defined geographic data; AC 4 Given a user lacks permission to maintain location-based databases, When the user attempts the change, Then the solution shall prevent the modification; AC 5 Given location-based information is changed, When the change is saved, Then the solution shall record the change with the user and time;		
8110	Real-Time Boundary and Response Zone Assignment	As a Dispatcher, I need the solution to determine the response zone and jurisdiction in real time by processing the incident's X, Y coordinates against the RCL or address point file and the boundary files, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an incident's X, Y coordinates and the RCL or address point file and the boundary files, When boundary assignment is performed, Then the solution shall determine the response zone and jurisdiction for the incident in real time; AC 2 Given a boundary assignment is determined, When the incident is processed, Then the solution shall associate the response zone and jurisdiction with the incident; AC 3 Given the incident's coordinates fall outside defined boundaries, When boundary assignment is performed, Then the solution shall identify the condition for resolution; AC 4 Given the incident location changes, When new coordinates are established, Then the solution shall recompute the boundary assignment in real time; AC 5 Given boundary files are updated, When a subsequent incident is processed, Then the solution shall use the current boundary files for assignment;		

8122	Premises Safety Information	As a Dispatcher, I need the solution to capture, maintain, or interface with premises information with hazardous materials and conditions, lock codes, dangerous animals, accessibility information, emergency contacts, unit safety information, warrants, alarms, protective orders, sexual offender information, fire pre-plans, user-defined premises fields, and electronic attachments limited to images and files, so that associated premises information is available to support safe and informed response operations.	AC 1 Given premises information is available, When an authorized user captures or interfaces the information, Then the solution shall retain or make available the premises information.; AC 2 Given premises information is maintained, When it is recorded, Then the solution shall support hazardous materials and conditions, lock codes, dangerous animals, accessibility information, emergency contacts, unit safety information, warrants, alarms, protective orders, sexual offender information, fire pre-plans, user-defined premises fields, and electronic attachments limited to images and files.; AC 3 Given premises information is associated with a location, When an incident occurs at or near the premises, Then the solution shall make the associated premises information available to support response.; AC 4 Given premises information is updated, When the change is saved, Then the solution shall retain the updated information and history.; AC 5 Given premises information is restricted, When an unauthorized user attempts access, Then the solution shall prevent access according to configured rules.;		
8123	Automatic Premises History	As a Dispatcher, I want the solution to create premises history upon closing of an incident based on pre-determined criteria, so that the capability is available in accordance with approved operational requirements.	AC 1 Given pre-determined criteria for premises history, When an incident is closed, Then the solution shall create premises history based on the pre-determined criteria; AC 2 Given premises history is created, When it is generated, Then the solution shall associate the history with the premises; AC 3 Given the pre-determined criteria are not met, When an incident is closed, Then the solution shall create premises history only for incidents that meet the pre-determined criteria.; AC 4 Given an Authorized User configures the premises history criteria, When the configuration is saved, Then the solution shall apply the criteria to subsequent incident closures;		
8124	Event Premises Information	As a Dispatcher, I want the solution to embed premises information into the event history at the time the event is created as a permanent record, so that each event retains the premises information as it existed when the event occurred.	AC 1 Given an event is created, When premises information exists for the location, Then the solution shall embed the premises information into the event history at the time the event is created; AC 2 Given premises information is embedded into the event history, When the event is viewed, Then the solution shall display the embedded premises information; AC 3 Given no premises information exists for the location, When the event is created, Then the solution shall create the event without embedded premises information; AC 4 Given premises information is embedded at event creation, When the premises information later changes, Then the solution shall retain the permanent record as embedded at creation time;		
8125	Permanent Premises History	As a Dispatcher, I need the solution to support/create a permanent record of the premises information in the event history, so that the capability is available consistently, traceably, and in accordance with approved operational requirements.	AC 332.1 Given premises information is associated with an event, When the event history is created, Then the system shall create a permanent record of the premises information in the event history; AC 332.2 Given a permanent premises record exists in the event history, When an authorized user reviews the event, Then the system shall present the permanent premises record; AC 332.3 Given the source premises information is subsequently changed, When the event history is viewed, Then the system shall retain the permanent record as it existed for that event;		
8136	Geographic Data Management	As a System Administrator, I want the solution to manage and use geographic and GIS data with street centerlines, system and agency boundaries, response zones, parcel-level information with approximate front-door locations, address validation, incident location determination, and validated incident X,Y coordinates, and to support bulk data uploads, scheduled data updates, metadata, and FGDC-standard data feeds with XML and KML, so that accurate and current geographic information supports incident location, mapping, response-zone assignment, and response operations.	AC 1 Given geographic and GIS data is provided, When an authorized administrator manages the data, Then the solution shall maintain street centerlines, system and agency boundaries, response zones, and parcel-level information with approximate front-door locations.; AC 2 Given an incident location is entered, When address validation and incident location determination are performed, Then the solution shall validate the location and determine the validated incident X,Y coordinates.; AC 3 Given geographic data updates are provided, When the data is ingested, Then the solution shall support bulk data uploads and scheduled data updates.; AC 4 Given FGDC-standard data feeds including XML and KML are provided, When the data is ingested, Then the solution shall support the standard data feeds and associated metadata.; AC 5 Given ingested geographic data contains invalid or unsupported information, When the data is validated, Then the solution shall identify the invalid or unsupported information.; AC 6 Given current geographic data is maintained, When response operations use the data, Then the solution shall make the geographic information available for incident location, mapping, and response-zone assignment.;		
8137	Distance-Based Location Search	As a Dispatcher, I want the solution to perform a distance search to identify the existence of location information during the event creation process, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an event is being created, When a distance search for location information limited to hazards is performed, Then the solution shall identify the existence of location information within the search distance; AC 2 Given location information exists within the search distance, When the search completes, Then the solution shall return the location information; AC 3 Given no location information exists within the search distance, When the search is performed, Then the solution shall indicate that none was found; AC 4 Given a distance search is performed during event creation, When results are returned, Then the solution shall associate the results with the event being created;		
8138	Configurable Location Search Distances	As a Dispatcher, I want the solution to support different search distance criteria for different types of locations, so that the capability is available in accordance with approved operational requirements.	AC 1 Given different types of locations, When search distance criteria are configured, Then the solution shall support different search distance criteria for different types of locations; AC 2 Given type-specific search distances are configured, When a search is performed for a given location type, Then the solution shall apply the search distance configured for that type; AC 3 Given an Authorized User changes a type-specific search distance, When the configuration is saved, Then the solution shall apply the updated distance to subsequent searches; AC 4 Given an invalid search distance is entered, When the user attempts to save it, Then the solution shall identify the invalid value; AC 5 Given an invalid search distance is entered, When the user attempts to save it, Then the solution shall prevent saving;		

8171	Incident Location Coordinate and Map Display	As a Dispatcher, I want the solution to verify an incident location, determine and record the X and Y coordinates for the validated location, and display the incident location on the Tactical Map Display (TMD) as the CFS event is created, so that accurate geographic coordinates and a visual incident location are available for mapping, routing, and incident response operations.	AC 1 Given a CFS event is being created, When the incident location is verified, Then the solution shall verify the incident location; AC 2 Given a CFS event is being created, When the incident location is verified, Then the solution shall determine and record the X and Y coordinates for the validated location; AC 3 Given a validated location with coordinates, When the CFS event is created, Then the solution shall display the incident location on the Tactical Map Display; AC 4 Given the incident location cannot be validated, When creation is attempted, Then the solution shall indicate that the location could not be validated; AC 5 Given the incident location changes during creation, When the new location is validated, Then the solution shall update the recorded coordinates and the Tactical Map Display; AC 6 Given coordinates are recorded, When they are saved, Then the solution shall make the coordinates available for mapping, routing, and response operations; AC 7 Given the location is displayed on the Tactical Map Display, When the dispatcher views it, Then the solution shall present a visual incident location;		
8172	Layered GIS and Location Imagery	As a System Administrator, I want the solution to support multiple layers of geographic information with building footprints, aerial imagery, and images associated with specific geographic areas and addresses, so that dispatchers and responders have access to associated location information during incident operations.	AC 1 Given multiple layers of geographic information with building footprints, aerial imagery, and images associated with specific geographic areas and addresses, When a user accesses mapping, Then the solution shall support the multiple geographic information layers; AC 2 Given geographic layers are available, When a dispatcher or responder views a location, Then the solution shall make the associated location information available during incident operations; AC 3 Given a layer is configured by an administrator, When the configuration is saved, Then the solution shall persist the layer configuration; AC 4 Given a geographic layer is unavailable, When a user requests it, Then the solution shall indicate that the layer is unavailable; AC 5 Given multiple layers are displayed, When the user manages them, Then the solution shall allow the user to select the layers;		
8173	Configurable Search Distance Criteria	As a System Administrator, I want the solution to support configurable search distance criteria by incident situation or hazard, allow authorized users to modify the search distance parameters, and allow CAD users to select the unit of measurement with feet or meters, so that geographic searches can be performed using criteria to the operational need.	AC 1 Given configurable search distance criteria by incident situation or hazard, When an Authorized User modifies the search distance parameters, Then the solution shall apply the modified search distance criteria; AC 2 Given a search distance is specified, When a CAD user selects the unit of measurement, Then the solution shall support the selected unit of measurement with feet or meters; AC 3 Given search distance criteria are configured by situation or hazard, When a geographic search is performed, Then the solution shall apply the criteria to the operational need; AC 4 Given an invalid search distance parameter is entered, When the user attempts to save it, Then the solution shall identify the invalid value; AC 5 Given an invalid search distance parameter is entered, When the user attempts to save it, Then the solution shall prevent saving; AC 6 Given search distance criteria are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8177	Configurable Tactical Maps and Automated Pin Mapping	As a System Administrator, I want the solution to allow authorized administrators to configure tactical map displays with map content by zoom level, predefined zoom levels by incident type, and map icons, and to support the creation of automatic pin maps or through an integrated third-party mapping tool, so that users can configure and generate maps that display incident locations based on defined operational criteria.	AC 1 Given an authorized administrator configures tactical map displays, When the administrator sets map content by zoom level, predefined zoom levels by incident type, and map icons, Then the solution shall persist the tactical map configuration; AC 2 Given automatic pin maps are supported or through an integrated third-party mapping tool, When a pin map is generated, Then the solution shall create the automatic pin map; AC 3 Given a tactical map configuration is applied, When a user generates a map, Then the solution shall display incident locations based on the defined operational criteria; AC 4 Given a user lacks permission to configure tactical map displays, When the user attempts the change, Then the solution shall prevent the modification; AC 5 Given a tactical map configuration is changed, When it is saved, Then the solution shall record the change with the user and time; AC 6 Given a predefined zoom level is configured by incident type, When an incident of that type is displayed, Then the solution shall apply the predefined zoom level;		
8181	Premises Information by Unit or Building	As a Dispatcher, I want the solution to allow me to view premises information for a specific suite, apartment, or unit, or view premises information for an entire building, so that I can access the configured level of location-specific information during incident response.	AC 1 Given premises information at a building with suites, apartments, or units, When a dispatcher requests premises information for a specific suite, apartment, or unit, Then the solution shall display the premises information for that specific location; AC 2 Given a dispatcher requests premises information for an entire building, When the request is made, Then the solution shall display the premises information for the entire building; AC 3 Given premises information exists at multiple levels, When the dispatcher selects a level, Then the solution shall present the information for the selected level; AC 4 Given no premises information exists for the requested level, When the dispatcher requests it, Then the solution shall indicate that none is available;		
8188	Integrated Tactical Map Display	As a Dispatcher, I want the solution to provide an integrated GIS-based tactical map display, so that geographic information can be viewed within the CAD workflow to support incident management and response operations.	AC 1 Given an integrated GIS-based tactical map display, When a dispatcher views mapping, Then the solution shall provide the integrated GIS-based tactical map display within the CAD workflow; AC 2 Given geographic information is available, When the tactical map is displayed, Then the solution shall present the information to support incident management and response; AC 3 Given geographic data updates, When the tactical map refreshes, Then the solution shall reflect the current geographic information; AC 4 Given the GIS map data is unavailable, When the dispatcher views mapping, Then the solution shall indicate that current map data is unavailable;		
8189	Integrated Map-Centric Tactical Display	As a Dispatcher, I want the solution to provide a map-centric tactical map display fully integrated with CAD with automatic display of unit locations from AVL when a separate tactical map application is used, so that incident and resource locations are available in a unified operational view.	AC 1 Given a map-centric tactical map display fully integrated with CAD, When a dispatcher views the display, Then the solution shall present incident and resource locations in a unified operational view; AC 2 Given a separate tactical map application is used, When unit locations are available from AVL, Then the solution shall display the unit locations from AVL; AC 3 Given unit or incident locations change, When the display refreshes, Then the solution shall update the map-centric display accordingly; AC 4 Given AVL unit location data is unavailable, When the display is shown, Then the solution shall indicate that current unit locations are unavailable; AC 5 Given the map-centric display is in use, When a dispatcher interacts with it, Then the solution shall present the integrated incident and resource information;		

8192	3D GIS Measurement and Data Overlay	As an Authorized User, I want the solution to measure distance, height, elevation, and area from supported 3D imagery and overlay GIS content and other associated data, so that geographic information can be analyzed and visualized within the mapping environment.	AC 1 Given supported 3D imagery and GIS content, When an Authorized User measures distance, height, elevation, or area, Then the solution shall perform the measurement from the 3D imagery; AC 2 Given GIS content and other associated data, When the user overlays it on the imagery, Then the solution shall display the overlaid content within the mapping environment; AC 3 Given a measurement is performed, When the result is produced, Then the solution shall present the measurement result; AC 4 Given the 3D imagery is unavailable, When the user attempts a measurement, Then the solution shall indicate that the imagery is unavailable; AC 5 Given overlay data is applied, When the user manages the overlays, Then the solution shall allow the user to select the overlays;		
8193	Address and Location Alias Management	As a System Administrator, I want the solution to support valid MSAG names and configurable aliases for street names, intersections, common place names, landmarks, and street or highway route numbers, so that locations can be identified and searched using recognized names and alternate references.	AC 1 Given valid MSAG names and configurable aliases for street names, intersections, common place names, landmarks, and street or highway route numbers, When location identification is performed, Then the solution shall support the MSAG names and configurable aliases; AC 2 Given aliases are configured, When a user searches by an alias, Then the solution shall resolve the alias to the correct location; AC 3 Given an Authorized User configures an alias, When the configuration is saved, Then the solution shall persist the alias; AC 4 Given an alias conflicts with an existing entry, When the user attempts to save it, Then the solution shall identify the conflict; AC 5 Given an alias conflicts with an existing entry, When the user attempts to save it, Then the solution shall prevent an ambiguous configuration; AC 6 Given aliases are changed, When the change is saved, Then the solution shall apply the updated aliases to subsequent identification and search;		
8197	Manual Incident Location Validation	As a Dispatcher, I want the solution to allow authorized users to manually validate and process an incident location when the location cannot be validated against the geofile, so that a CFS event can be created when the location is confirmed or otherwise known to exist within the local jurisdiction.	AC 1 Given an incident location cannot be validated against the geofile, When an Authorized User manually validates and processes the location, Then the solution shall allow the location to be manually validated and processed; AC 2 Given a location is manually confirmed or otherwise known to exist within the local jurisdiction, When the user proceeds, Then the solution shall allow a CFS event to be created for the location; AC 3 Given a user lacks permission to manually validate a location, When the user attempts it, Then the solution shall prevent the action; AC 4 Given a location is manually validated, When the event is created, Then the solution shall record that the location was manually validated and the user who did so; AC 5 Given a manually validated location is used, When the event is processed, Then the solution shall associate the manually validated location with the event;		
8200	On-Scene Timers and Check-In Alerts	As a Dispatcher or Supervisor, I want the solution to provide configurable on-scene timers and check-in alerts based on incident type, unit status, and responder type, so that personnel who remain on scene or in a status beyond an established threshold can be identified and followed up.	AC 1 Given configurable on-scene timers and check-in alerts based on incident type, unit status, and responder type, When the configured threshold is reached, Then the solution shall generate the on-scene timer or check-in alert; AC 2 Given a responder remains on scene or in a status beyond the established threshold, When the threshold is exceeded, Then the solution shall identify the personnel for follow-up; AC 3 Given an Authorized User configures on-scene timers and check-in alerts, When the configuration is saved, Then the solution shall persist the timer; AC 4 Given an Authorized User configures on-scene timers and check-in alerts, When the configuration is saved, Then the solution shall alert configuration; AC 5 Given a check-in is completed before the threshold, When the check-in occurs, Then the solution shall withhold the check-in alert.; AC 6 Given an on-scene timer or check-in alert occurs, When it is generated, Then the solution shall retain a record of the alert for review;		
8220	Address Type-Ahead Search and Autocomplete	As a Dispatcher, I want the solution to provide type-ahead search, autocomplete, and suggested-address matches wherever an address is entered in the solution, validated against available GIS/address data, so that I can select a valid location from matching results without entering the complete address.	AC 1 Given a dispatcher begins entering a partial address, When the entered characters match available GIS/address data, Then the solution shall display matching address candidates.; AC 2 Given matching candidates are displayed, When the dispatcher selects a candidate, Then the solution shall populate the location using the selected address.; AC 3 Given a partial entry returns no matches, When the search is performed, Then the solution shall indicate that no matching addresses were found.; AC 4 Given matching candidates are displayed, When the number of matches exceeds the configured limit, Then the solution shall narrow results as additional characters are entered.; AC 5 Given a location is selected through type-ahead, When the selection is applied, Then the solution shall validate the location according to configured GIS and address validation rules.;		
8227	Alert Source and Accountability	As a Dispatcher, I want the solution to document the origin of a safety or caution alert with who established it, the reason, and a contact, so that the basis and accountability for each alert can be reviewed.	AC 1 Given a safety or caution alert is established, When the alert is created, Then the solution shall record the user who established it, the reason, and a contact where provided.; AC 2 Given an alert has provenance information, When an Authorized User reviews the alert, Then the solution shall display the originating user, reason, and contact.; AC 3 Given an alert is modified, When the change is saved, Then the solution shall retain the change with the user, reason, and date/time.; AC 4 Given required provenance information is missing, When a user attempts to establish an alert, Then the solution shall identify the missing information according to configured rules.; AC 5 Given an alert is retired or expires, When the action occurs, Then the solution shall retain the provenance information in the alert history.;		
8238	Premises Radio-Coverage Quality Indicator	As a Dispatcher, I want premises records to carry a radio-coverage-quality indicator, so that responders are alerted when entering a building with known poor radio coverage.	AC 1 Given a premises record, When an Authorized User maintains premises information, Then the solution shall provide a configurable field to record radio-coverage quality for the location.; AC 2 Given radio-coverage quality is recorded for a premises, When an incident is created at that location, Then the solution shall display the coverage indicator to the dispatcher and assigned responders.; AC 3 Given a premises has poor radio-coverage recorded, When units are dispatched, Then the solution shall present the coverage caution consistent with other premises safety alerts.; AC 4 Given radio-coverage information changes, When an Authorized User updates the premises record, Then the solution shall retain the update and history.;		
8775	Enter and Associate Radio Log Entries	As a Dispatcher, I want to enter radio log entries and associate them with an operational reference, so that radio communications are documented and linked.	AC 1 Given a dispatcher needs to document radio communications, When the dispatcher manually enters a radio log entry, Then the solution shall record the entry with the communication details.; AC 2 Given a radio log entry has been entered, When the dispatcher associates the entry with an incident, event, unit, channel, or specified time period, Then the solution shall link the entry to the selected operational reference.; AC 3 Given a radio log entry contains required information that is missing or invalid, When the dispatcher attempts to save the entry, Then the solution shall identify the information requiring correction.;		

8776	Search and View Radio Log Entries	As a Dispatcher, I want to search and view radio log entries, so that I can review communications tied to an operational record.	AC 1 Given a dispatcher searches for radio log entries, When the dispatcher specifies an incident, event, unit, channel, or time period, Then the solution shall display the entries matching the specified criteria.; AC 2 Given multiple radio log entries are associated with an operational record, When an authorized user views the radio log, Then the solution shall display the entries in chronological order.; AC 3 Given a radio log entry has been saved, When an authorized user retrieves the associated operational record, Then the solution shall make the radio log entry available for reference and review.;		
8777	Update Radio Log Entries with History	As a Dispatcher, I want radio log corrections retained with history, so that changes remain auditable.	AC 1 Given a radio log entry has been saved, When an authorized user updates or corrects the entry, Then the solution shall retain the updated information.; AC 2 Given a radio log entry has been saved, When an authorized user updates or corrects the entry, Then the solution shall record history in accordance with configured audit requirements.; AC 3 Given a radio log entry exists, When a user without update permission attempts to change the entry, Then the solution shall prevent the change.; AC 4 Given a radio log entry has been corrected, When an authorized user reviews the entry, Then the solution shall display the current values and the change history.;		
8778	Recommend Resources Using Configured Rules	As a Dispatcher, I want the solution to recommend resources using configured capability, proximity, and workload rules, so that recommendations reflect established selection criteria.	AC 1 Given configured resource-selection rules for capability, availability, workload, proximity, mutual aid, and rotation are in effect, When a dispatcher requests a resource recommendation for an incident, Then the solution shall return a recommended resource set that reflects those configured rules.; AC 2 Given a unit lacks a capability that the configured rules require for the incident type, When the solution generates a resource recommendation, Then the solution shall exclude that unit from the recommended resources.; AC 3 Given multiple eligible units are available, When the solution recommends resources, Then the solution shall rank recommendations using the configured proximity and workload criteria.;		
8779	Reflect Current Conditions in Resource Recommendations	As a Dispatcher, I want resource recommendations to reflect current operational conditions, so that they stay accurate as conditions change.	AC 1 Given a unit's availability status changes, When a dispatcher requests a recommendation after the change, Then the solution shall reflect the unit's current availability in the recommendation.; AC 2 Given operational conditions change in availability, workload, or location, When the dispatcher refreshes the recommendation, Then the solution shall recalculate the recommendation using current conditions.;		
8780	Apply Mutual-Aid and Rotation Rules to Resource Recommendations	As a Dispatcher, I want mutual-aid and rotation rules applied to resource recommendations, so that resource selection follows established agreements.	AC 1 Given an incident qualifies for mutual-aid resources under configured agreements, When no eligible local resource is available, Then the solution shall include eligible mutual-aid resources in the recommendation.; AC 2 Given rotation rules apply to equivalent resources, When the solution recommends from a rotation pool, Then the solution shall select the next eligible resource in the configured rotation sequence.;		
8781	Override Resource Recommendation	As a Dispatcher, I want to override a resource recommendation with a recorded reason, so that overrides remain traceable.	AC 1 Given a dispatcher has the required permissions, When the dispatcher overrides a resource recommendation, Then the solution shall allow the override.; AC 2 Given a dispatcher has the required permissions, When the dispatcher overrides a resource recommendation, Then the solution shall record the overriding user, the original recommendation, and the selected resource.; AC 3 Given a dispatcher overrides a resource recommendation, When the override is submitted, Then the solution shall require a recorded reason before applying the override.; AC 4 Given a user lacks override permission, When the user attempts to override a resource recommendation, Then the solution shall prevent the override.;		
8782	Notify When No Eligible Resource	As a Dispatcher, I want to be notified when no resource meets the configured selection criteria, so that I can take alternative action.	AC 1 Given no resource satisfies the configured selection criteria, When a dispatcher requests a recommendation, Then the solution shall notify the dispatcher that no eligible resource is available.; AC 2 Given no resource satisfies the configured selection criteria, When the dispatcher is notified, Then the solution shall display the criteria that were not met.; AC 3 Given no eligible resource is available, When the notification occurs, Then the solution shall record the no-eligible-resource event with the incident.;		
8783	Correct Timestamps with Audit Retention	As a System Administrator, I want a controlled process to correct dispatch, enroute, or arrival timestamps while retaining the original values, so that corrections remain auditable.	AC 1 Given an authorized supervisor or administrator initiates a timestamp correction, When the user corrects a dispatch, enroute, or arrival timestamp, Then the solution shall apply the corrected value.; AC 2 Given an authorized supervisor or administrator initiates a timestamp correction, When the user corrects a dispatch, enroute, or arrival timestamp, Then the solution shall retain the original value, the reason, the user, and the time of correction.; AC 3 Given a required correction reason is not provided, When the user submits the correction, Then the solution shall prevent the correction until a reason is entered.;		
8784	Restrict and Validate Timestamp Corrections	As a System Administrator, I want corrections restricted to authorized users and valid sequences, so that timestamp integrity is preserved.	AC 1 Given a user without correction authorization attempts to change a timestamp, When the change is submitted, Then the solution shall prevent the correction.; AC 2 Given a corrected timestamp produces an invalid sequence such as arrival before dispatch, When the correction is submitted, Then the solution shall identify the invalid sequence.; AC 3 Given a corrected timestamp produces an invalid sequence such as arrival before dispatch, When the correction is submitted, Then the solution shall prevent acceptance.;		
8785	Recalculate Durations After Timestamp Correction	As a System Administrator, I want incident durations recalculated after a timestamp correction, so that calculated durations remain accurate.	AC 1 Given a timestamp is corrected, When the correction is saved, Then the solution shall recalculate affected durations using the corrected timestamp.; AC 2 Given durations are recalculated after a correction, When the record is viewed, Then the solution shall display the updated durations.;		
8786	Review Timestamp Correction History	As a System Administrator, I want to review the original and corrected timestamp values, so that the change history can be audited.	AC 1 Given a timestamp correction has been made, When an authorized user reviews the record, Then the solution shall present the original and corrected values and the correction details.; AC 2 Given a timestamp correction has been made, When an authorized user reviews the record, Then the solution shall display the user who made the correction and the date and time of the correction.; AC 3 Given timestamp correction history exists, When a user without audit permission attempts to view it, Then the solution shall prevent access.;		
8787	Create and Prioritize Mayday Events	As a Dispatcher, I want the solution to create and prioritize Mayday events, so that responder distress receives immediate attention.	AC 1 Given a Mayday event is received, When the solution processes it, Then the solution shall create and prioritize the Mayday event for immediate operational attention.; AC 2 Given a Mayday event is received, When the event is created, Then the solution shall identify the affected responder or resource.; AC 3 Given a Mayday event is received, When the solution prioritizes active events, Then the solution shall order the Mayday event ahead of lower-priority events.;		

8788	Display Active Mayday Events	As a Dispatcher, I want active Mayday events displayed distinctly, so that I can recognize them immediately.	AC 1 Given a Mayday event is active, When a dispatcher views active events, Then the solution shall display the Mayday event with distinguishable high-priority indication.; AC 2 Given a Mayday event is active, When the event is displayed, Then the solution shall present a persistent indication until the event is acknowledged or cleared.; AC 3 Given an active Mayday event is displayed, When a dispatcher selects the event, Then the solution shall present the associated unit, location, and event details.;		
8789	Track and Resolve Mayday Events	As a Dispatcher, I want to track and resolve Mayday events, so that distress situations are managed to closure.	AC 1 Given a Mayday event is being handled, When a dispatcher tracks the event, Then the solution shall allow the dispatcher to monitor.; AC 2 Given a Mayday event is being handled, When a dispatcher tracks the event, Then the solution shall update its status.; AC 3 Given a Mayday event is resolved, When its status is updated to cleared, Then the solution shall record the resolution.; AC 4 Given a Mayday event is resolved, When its status is updated to cleared, Then the solution shall retain the event history.;		
8790	Retain Traceable Mayday Record	As a Dispatcher, I want a traceable record of each Mayday event, so that distress handling is auditable.	AC 1 Given a Mayday event occurs, When the event is processed, Then the solution shall retain a traceable, date and time-stamped record of the Mayday event and the actions taken.; AC 2 Given a Mayday record has been retained, When an authorized user reviews the record, Then the solution shall present the record and its actions in read-only form for audit.; AC 3 Given a Mayday record is retained, When the configured retention period applies, Then the solution shall retain the record for the configured retention period.;		
8805	Capture and Maintain Premises Safety Information	As a Records user, I want to capture and maintain premises safety information, so that premises hazards and safety details are documented.	AC 1 Given premises information including hazardous materials and conditions, lock codes, dangerous animals, accessibility information, emergency contacts, unit safety information, warrants, alarms, protective orders, sexual offender information, fire pre-plans, user-defined premises fields, and electronic attachments, When the information is captured or maintained, Then the solution shall retain the premises information.; AC 2 Given a user lacks permission to maintain premises information, When the user attempts the change, Then the solution shall prevent the modification.; AC 3 Given premises information is changed, When the change is saved, Then the solution shall record the change with the user and time.; AC 4 Given user-defined premises fields are configured, When premises records are maintained, Then the solution shall support the user-defined fields.;		
8806	Interface Premises Information Updates	As a Records user, I want premises information maintained through an interface to stay current, so that source changes are reflected.	AC 1 Given premises information is maintained through an interface, When source information changes, Then the solution shall reflect the updated premises information.; AC 2 Given premises information is updated through the interface, When the update is received, Then the solution shall record the source and date and time of the update.; AC 3 Given a premises information update is received through the interface, When the update cannot be applied, Then the solution shall identify the failed update for review.;		
8807	Surface Premises Information on Incident	As a Dispatcher, I want associated premises information surfaced when an incident occurs at a location, so that responders have safety context.	AC 1 Given premises information exists for a location, When an incident occurs at that location, Then the solution shall make the relevant premises information available to support safe and informed response.; AC 2 Given electronic attachments such as images and files are associated with a premises, When an authorized user accesses the premises, Then the solution shall provide the attachments.;		
8808	Maintain and Use Geographic/GIS Data	As a System Administrator, I want the solution to maintain and use geographic and GIS data, so that current geographic information supports response operations.	AC 1 Given geographic and GIS data including street centerlines, system and agency boundaries, response zones, parcel-level information with approximate front-door locations, and validated incident coordinates, When the solution manages the data, Then the solution shall maintain and use the geographic and GIS data.; AC 2 Given GIS metadata is available, When data is managed, Then the solution shall maintain the associated metadata.; AC 3 Given GIS data is updated, When the update is applied, Then the solution shall use the current geographic information for incident location, mapping, and response-zone assignment.;		
8809	Validate Incident Location and Coordinates	As a Dispatcher, I want incident locations validated to X,Y coordinates, so that mapping and routing use accurate positions.	AC 1 Given an incident location is entered, When address validation and incident location determination are performed, Then the solution shall validate the location.; AC 2 Given an incident location is entered, When address validation and incident location determination are performed, Then the solution shall determine the validated incident X,Y coordinates.; AC 3 Given an entered incident location cannot be validated, When address validation is performed, Then the solution shall identify the location as unresolved and prompt for correction.; AC 4 Given address validation returns multiple candidate locations, When the validation is performed, Then the solution shall present the candidate locations for selection.;		
8810	Ingest Bulk, Scheduled, and Standard GIS Feeds	As a System Administrator, I want to ingest GIS data through bulk, scheduled, and standard feeds, so that geographic data stays current.	AC 1 Given bulk GIS data is provided, When a bulk data upload is performed, Then the solution shall support the bulk data upload.; AC 2 Given scheduled GIS data updates are configured, When a scheduled update occurs, Then the solution shall apply the scheduled data update.; AC 3 Given FGDC-standard data feeds including XML and KML are provided, When the data is ingested, Then the solution shall support the FGDC-standard data feeds.; AC 4 Given ingested geographic data contains invalid or unsupported information, When the data is validated during ingest, Then the solution shall identify the invalid or unsupported information.;		
8811	Handle GIS Data Load Failures	As a System Administrator, I want GIS load failures identified and handled, so that bad data does not disrupt operations.	AC 1 Given a GIS data upload or update fails, When the failure occurs, Then the solution shall identify the failure.; AC 2 Given a GIS data upload or update fails, When the failure occurs, Then the solution shall apply the configured handling.; AC 3 Given a GIS data load failure occurs, When the failure is identified, Then the solution shall notify the designated administrator of the failure.; AC 4 Given a GIS data load fails, When the failure is handled, Then the solution shall retain the last successfully loaded GIS data for continued operation.;		
8812	Real-Time Vehicle Location Integration	As a Dispatcher, I want the solution to integrate with vehicle tracking systems for real-time locations, so that current vehicle positions are available.	AC 1 Given integration with vehicle tracking systems, When real-time vehicle location data is received, Then the solution shall provide real-time vehicle locations.; AC 2 Given vehicle tracking data is unavailable, When real-time locations are requested, Then the solution shall indicate that current vehicle location data is unavailable.; AC 3 Given AVL data is recorded, When current and historical data is used, Then the solution shall support monitoring and evaluation of vehicle location, availability, activity, and operational status.;		
8813	Out-of-Service Vehicle Alert	As a Dispatcher, I want to be alerted when a vehicle is placed out of service, so that I can react to availability changes.	AC 1 Given a vehicle is placed out of service, When the status change occurs, Then the solution shall alert the designated users.; AC 2 Given a vehicle is placed out of service, When the status change occurs, Then the solution shall update the vehicle's availability so it is not recommended for dispatch.; AC 3 Given a vehicle is returned to service, When the status change occurs, Then the solution shall alert the designated users.; AC 4 Given a vehicle is returned to service, When the status change occurs, Then the solution shall restore the vehicle's availability.;		

8814	Configurable AVL Reports	As a Supervisor, I want to generate configurable AVL reports for a specified date range, so that I can review vehicle activity.	AC 1 Given a specified date range, When a user generates an AVL report, Then the solution shall generate a configurable AVL report for the specified date range.; AC 2 Given an AVL report is generated, When it is produced, Then the solution shall include vehicle activity, start and stop times, alert-triggering events, mileage, stops, and per-vehicle summaries.; AC 3 Given a user lacks permission to view AVL reports or vehicle locations, When the user attempts access, Then the solution shall prevent access.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 03: Mobile Communications & Field Operations					
7813	Responder Incident Access	As a Responder, I want access to incidents assigned to me and the information authorized for my role, so that I have the information needed to perform my assigned duties.	AC 1 Given a responder has an assigned incident, When the responder accesses the solution, Then the responder shall be able to view authorized information for the assigned incident.; AC 2 Given a responder does not have an assigned incident, When the responder searches for incidents, Then the solution shall limit results according to configured role and access rules.; AC 3 Given incident information is restricted by role, When a responder accesses the incident, Then the solution shall prevent access to unauthorized information.; AC 4 Given assigned incident information changes, When the responder refreshes or receives an update, Then the responder shall be able to view the current authorized information.; AC 5 Given an incident assignment is removed, When the assignment status changes, Then the solution shall revoke the access that the removed assignment had granted to the responder.;		
7814	Responder Capability and Status Management	As a System Administrator or Dispatcher, I want to maintain responder roles, skills, qualifications, specialized capabilities, operational attributes, equipment attributes, and activation status, so that responder eligibility, availability, and resource selection reflect current responder capabilities and operational needs.	AC 1 Given an authorized administrator or dispatcher maintains responder information, When a responder role is updated, Then the solution shall retain the updated role.; AC 2 Given responder skills or qualifications are updated, When the changes are saved, Then the current skills and qualifications shall be available for eligibility evaluation.; AC 3 Given specialized capabilities are updated, When the responder record is saved, Then the solution shall associate the current capabilities with the responder.; AC 4 Given responder equipment attributes are updated, When the changes are saved, Then the current equipment information shall be available for resource selection.; AC 5 Given responder activation status changes, When the status is saved, Then the responder's operational availability shall reflect the updated status.; AC 6 Given responder attributes affect resource eligibility, When the solution evaluates available resources, Then the solution shall use the current approved attributes.;		
7817	Mobile Assignment Notifications	As a Dispatcher, I want the solution to send incident assignment notifications to assigned responders through supported mobile channels, so that responders receive current information about their assignments.	AC 1 Given a responder has been assigned to an incident, When the assignment is saved, Then the solution shall generate the configured mobile notification.; AC 2 Given a mobile notification is generated, When the supported mobile channel is available, Then the solution shall transmit the notification to the assigned responder.; AC 3 Given the responder's assignment changes, When the change is saved, Then the solution shall transmit the updated assignment information through the supported channel.; AC 4 Given a mobile notification fails, When the failure is detected, Then the solution shall record the notification failure according to configured rules.; AC 5 Given a responder has no supported mobile channel, When the assignment is created, Then the solution shall process the assignment according to the configured alternate notification workflow.;		
7839	Mobile Incident Information Access	As a Responder, I want to view current incident information related to my assignments from a supported mobile device, so that I can access current operational information in the field.	AC 1 Given a responder has an assigned incident, When the responder accesses the solution from a supported mobile device, Then the solution shall display the current authorized incident information.; AC 2 Given incident information changes, When the mobile device receives the supported update, Then the responder shall be able to view the updated information.; AC 3 Given a responder is no longer assigned to an incident, When the assignment is removed, Then the solution shall send assignment-based updates only to responders with an active assignment.; AC 4 Given mobile access is unavailable, When the responder attempts to access current information, Then the solution shall respond according to configured connectivity behavior.; AC 5 Given incident information is restricted, When the responder accesses the mobile view, Then the solution shall display only information authorized for the responder's role.;		
7933	Secure Mobile CAD Operations	As an Officer, I want CAD/RMS mobile functions to operate securely on supported mobile data terminals, so that protected information can be used in the field consistent with CJIS and State security requirements.	AC 1 Given an Officer uses a supported mobile data terminal, When the Officer accesses CAD/RMS, Then the solution shall authenticate and authorize the user before providing protected information.; AC 2 Given protected CAD/RMS information is transmitted over a supported mobile connection, When the information is exchanged, Then the solution shall apply the required security controls.; AC 3 Given the Officer does not have authorization for a requested function or record, When access is attempted, Then the solution shall deny the unauthorized access.;		
7936	Constrained Technology and Connectivity Support	As a Responder, I want essential CAD/RMS workflows to remain usable on constrained technology and connectivity, so that volunteer agencies can participate without requiring enterprise-grade infrastructure at every location.	AC 1 Given a responder operates using constrained technology or connectivity, When the responder performs an essential supported CAD/RMS workflow, Then the required workflow shall remain usable within the supported constraints.; AC 2 Given connectivity is limited, When an essential workflow is performed, Then the solution shall provide the supported functionality to the available connectivity.; AC 3 Given an essential function cannot be completed because of connectivity limitations, When the limitation is detected, Then the solution shall provide an indication to the responder.;		
7954	Mobile Network and Connectivity Support	As an Officer or Responder, I want secure mobile CAD functions to operate over supported broadband, LTE, and constrained networks, so that I can access and update authorized CAD information while operating in the field.	AC 1 Given an Officer or Field Personnel is connected through supported broadband or LTE, When the user accesses mobile CAD, Then the solution shall provide the supported mobile CAD functions.; AC 2 Given connectivity is constrained, When the user performs a configured mobile CAD workflow, Then the solution shall operate according to the supported constrained-network behavior.; AC 3 Given a mobile user updates authorized CAD information, When the update is successfully transmitted, Then the CAD record shall reflect the update.;		

7983	Turn-by-Turn Driving Directions	As a Responder, I want the solution to provide turn-by-turn driving directions from my current location to a dispatched incident or selected destination using approved routing and GIS data, with the ability to accept or decline the recommended route, so that I can navigate while retaining control over the route used.	AC 1 Given a Responder has an authorized mobile CAD session and a dispatched incident or selected destination, When the Responder requests directions, Then the solution shall calculate a route using approved routing and GIS data.; AC 2 Given a recommended route is available, When the route is displayed, Then the solution shall present the route from the Responder's current location to the destination.; AC 3 Given the Responder accepts the recommended route, When the route is accepted, Then the solution shall retain the selected route for navigation.; AC 4 Given the Responder declines the recommended route, When the route is declined, Then the solution shall allow the Responder to proceed without accepting the recommended route.;		
8103	MDC Event Updates	As a Dispatcher, I want the solution to support the MDC interface so a field user can update the CFS event in CAD, so that field updates are captured in CAD.	AC 1 Given the MDC interface is available, When a field user updates the CFS event from the MDC, Then the solution shall apply the update to the CFS event in CAD; AC 2 Given an MDC update fails to transmit, When the failure occurs, Then the solution shall identify the failure; AC 3 Given an MDC update fails to transmit, When the failure occurs, Then the solution shall apply the configured handling; AC 4 Given a field update is applied, When it is saved, Then the solution shall record the update in the event history with its source; AC 5 Given a field user lacks permission to update the CFS event, When the update is attempted, Then the solution shall prevent it;		
8133	Mobile Day/Night Mode	As a Responder, I want the solution to provide day/night mode for mobile users, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a mobile user, When the user selects day or night mode, Then the solution shall provide the selected day/night display mode for the mobile user; AC 2 Given a display mode is selected, When the mobile client is used, Then the solution shall apply the selected mode; AC 3 Given display conditions change, When the mobile user switches modes, Then the solution shall update the display accordingly;		
8134	Mobile Mapping	As a Responder, I want the solution to provide an integrated mobile mapping client, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a mobile user, When the user accesses mapping, Then the solution shall provide an integrated mobile mapping client; AC 2 Given the mobile mapping client is in use, When incident or resource locations are available, Then the solution shall display them within the mobile mapping client; AC 3 Given map data updates, When the mobile client refreshes, Then the solution shall reflect the current mapping information; AC 4 Given mapping data is unavailable to the mobile client, When the user accesses mapping, Then the solution shall indicate that current mapping data is unavailable;		
8135	Mobile Resource and Personnel Search	As a Responder, I want the solution to provide mobile search capability for resources and personnel by type of vehicle, status, and location, so that the capability is available in accordance with approved operational requirements.	AC 1 Given resources and personnel have type, status, and location attributes, When a mobile user searches by type of vehicle, status, and location, Then the solution shall return the matching resources and personnel; AC 2 Given no resources or personnel match the mobile search, When the search is performed, Then the solution shall indicate that no matches were found; AC 3 Given mobile search results are returned, When the user views them, Then the solution shall present the matching resources and personnel with their attributes; AC 4 Given multiple search criteria are specified, When the mobile user searches, Then the solution shall return resources meeting the combined criteria;		
8139	Vehicle Tracking, Status Alerts, and AVL Reporting	As a Dispatcher, I want the solution to integrate with vehicle tracking systems to provide real-time vehicle locations, alert designated users when a vehicle is placed out of service, and generate configurable AVL reports for specified date ranges with vehicle activity, start and stop times, alert-triggering events, mileage, stops, and per-vehicle summaries, so that vehicle location, availability, activity, and operational status can be monitored and evaluated using current and historical AVL data.	AC 1 Given integration with vehicle tracking systems, When real-time vehicle location data is received, Then the solution shall provide real-time vehicle locations.; AC 2 Given a vehicle is placed out of service, When the status change occurs, Then the solution shall alert the designated users.; AC 3 Given a specified date range, When an authorized user generates an AVL report, Then the solution shall generate a configurable AVL report for the specified date range.; AC 4 Given an AVL report is generated, When it is produced, Then the solution shall include vehicle activity, start and stop times, alert-triggering events, mileage, stops, and per-vehicle summaries.; AC 5 Given current and historical AVL data is available, When it is used, Then the solution shall support monitoring and evaluation of vehicle location, availability, activity, and operational status.; AC 6 Given vehicle tracking data is unavailable, When real-time locations are requested, Then the solution shall indicate that current vehicle location data is unavailable.;		
8140	AVL Travel History Playback	As a Dispatcher, I want the solution to be able to play back a unit's AVL travel history and see the unit icon move from location to location on a map window, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a unit's AVL travel history exists, When a dispatcher plays back the travel history, Then the solution shall play back the unit's AVL travel history on a map window; AC 2 Given AVL travel history is played back, When the playback runs, Then the solution shall move the unit icon from location to location on the map; AC 3 Given no AVL travel history exists for a unit, When playback is requested, Then the solution shall indicate that no travel history is available; AC 4 Given a playback is in progress, When the dispatcher controls it, Then the solution shall allow the dispatcher to control the playback;		
8145	MDC-Initiated Call for Service	As a Responder, I want the solution to allow me to initiate and submit a CFS from an MDC/MDT to a dispatch center, either to request additional support for an existing emergency response or to report a newly observed emergency incident, so that dispatchers can receive and process the CFS for configured response.	AC 1 Given a responder on an MDC/MDT, When the responder initiates and submits a Call for Service to a dispatch center, Then the solution shall transmit the CFS to the dispatch center for processing; AC 2 Given a CFS is submitted to request additional support for an existing emergency response, When it is received, Then the solution shall associate the CFS with the existing response; AC 3 Given a CFS is submitted to report a newly observed emergency incident, When it is received, Then the solution shall create a new CFS for the reported incident; AC 4 Given required CFS information is incomplete, When the responder submits it, Then the solution shall identify the missing information; AC 5 Given required CFS information is incomplete, When the responder submits it, Then the solution shall prevent submission; AC 6 Given a CFS submission fails to transmit, When the failure occurs, Then the solution shall notify the responder that the CFS was not submitted; AC 7 Given a CFS is received from an MDC/MDT, When it is processed, Then the solution shall make it available to dispatchers for configured response;		
8168	MDC Event Disposition Entry	As a Field User, I want the MDC interface to the CAD to allow me to enter one or more dispositions for an event, so that the outcome and actions associated with the event are documented from the field.	AC 1 Given the MDC interface, When a field user enters one or more dispositions for an event, Then the solution shall record the dispositions from the field; AC 2 Given multiple dispositions are entered from the field, When they are submitted, Then the solution shall associate each disposition with the event; AC 3 Given a field disposition entry is incomplete, When it is submitted, Then the solution shall identify the missing information; AC 4 Given a field disposition entry is incomplete, When it is submitted, Then the solution shall prevent completion; AC 5 Given dispositions are entered from the field, When they are saved, Then the solution shall record them with the entering field user and time; AC 6 Given a field user lacks permission to enter dispositions, When the user attempts it, Then the solution shall prevent the action;		

8196	GPS Signal Loss and Last Known Unit Position	As a Dispatcher, I need the solution to identify units experiencing a loss of GPS signal or location data and display the unit's last known position, time of signal loss, and elapsed time since the signal was lost, so that I can assess the currency of unit location information and manage resources.	AC 1 Given units reporting GPS location data, When a unit experiences a loss of GPS signal or location data, Then the solution shall identify the unit experiencing the loss; AC 2 Given a unit has lost its GPS signal, When the condition is identified, Then the solution shall display the unit's last known position, the time of signal loss, and the elapsed time since the signal was lost; AC 3 Given a unit's GPS signal is restored, When location data resumes, Then the solution shall update the unit's current location; AC 4 Given a GPS signal loss is displayed, When the dispatcher reviews it, Then the solution shall allow the dispatcher to assess the currency of the unit's location information; AC 5 Given a GPS signal loss occurs, When it is identified, Then the solution shall retain a record of the signal-loss condition;		
8201	Mobile RMS Access and Case Updates	As a Responder, I want the solution to provide secure mobile access to authorized RMS searches, narratives, linked records, and case updates, so that I can retrieve and update case information from a smartphone, tablet, or other supported mobile device while in the field.	AC 1 Given a field investigator or responder on a supported mobile device, When the user accesses authorized RMS searches, narratives, linked records, and case updates, Then the solution shall provide secure mobile access to that information; AC 2 Given a user is authorized, When the user retrieves or updates case information from the field, Then the solution shall allow the retrieval; AC 3 Given a user is authorized, When the user retrieves or updates case information from the field, Then the solution shall update from the mobile device; AC 4 Given a user lacks permission for a requested RMS search or record, When the user attempts access, Then the solution shall prevent it; AC 5 Given a case update is made from the field, When it is saved, Then the solution shall record the update with the user and time; AC 6 Given mobile access occurs, When the connection is established, Then the solution shall secure the access to protect the information;		
8234	Hands-Free Voice-Activated Mobile Dispatch	As a Responder, I want hands-free, voice-activated access to common mobile dispatch actions (limited to updating unit status, initiating an incident, or running a query), so that I can perform essential tasks safely while operating a vehicle.	AC 1 Given the mobile solution supports voice activation, When a responder issues a configured voice command, Then the solution shall execute the corresponding action.; AC 2 Given the mobile solution supports voice activation, When a responder issues a configured voice command, Then the solution shall provide audible confirmation.; AC 3 Given a responder initiates a status change by voice, When the command is recognized, Then the solution shall update the unit status.; AC 4 Given a responder initiates a status change by voice, When the command is recognized, Then the solution shall log the action.; AC 5 Given a responder requests a query by voice, When the command is recognized and permitted, Then the solution shall initiate the query.; AC 6 Given a responder requests a query by voice, When the command is recognized and permitted, Then the solution shall return results via audible or visual response.; AC 7 Given a voice command is not recognized or is not permitted, When the command is issued, Then the solution shall notify the responder and take no unintended action.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 04: Law Enforcement Operations, RMS & Information Sharing					
7820	Vehicle and Plate Lookup	As an Authorized User, I want to submit vehicle or plate information to an approved lookup source and receive authorized results, so that associated vehicle information is available during public-safety activities.	AC 1 Given an officer enters an authorized vehicle or plate identifier, When the officer initiates an approved lookup, Then the solution shall transmit the inquiry to the configured lookup source.; AC 2 Given DMV is configured as an approved source, When the officer selects DMV for an eligible lookup, Then the solution shall transmit the inquiry through the approved DMV interface.; AC 3 Given the lookup source returns an authorized response, When the response is received, Then the solution shall display the vehicle information.; AC 4 Given the lookup source returns no matching information, When the response is received, Then the solution shall indicate that no matching result was returned.; AC 5 Given the lookup fails, When the failure is detected, Then the solution shall notify the officer according to configured rules.; AC 6 Given an officer is not authorized to perform the lookup, When the officer initiates the inquiry, Then the solution shall prevent the transaction.;		
7823	Case Status and Disposition	As an Investigator, I want to maintain case status and disposition throughout the case lifecycle, so that users can determine current and final case outcomes.	AC 1 Given a case exists, When an authorized investigator updates the case status, Then the solution shall save the selected status.; AC 2 Given case statuses have configured transition rules, When an investigator attempts a status change, Then the solution shall allow only permitted transitions.; AC 3 Given a case reaches a final disposition, When the investigator records the disposition, Then the solution shall retain the final outcome.; AC 4 Given a case status changes, When the change is saved, Then the solution shall retain status history.; AC 5 Given an Authorized User views a case, When the case is active, Then the solution shall display the current case status.; AC 6 Given a case has a final disposition, When an Authorized User views the case, Then the solution shall display the final disposition according to access rules.;		
7827	Investigative Case File Management	As an Investigator, I want a case file that links related incidents, persons, vehicles, property, evidence, documents, narratives, and investigative activities, so that investigators can manage an investigation from one connected case record.	AC 1 Given an investigation requires a case file, When an authorized investigator creates the case, Then the solution shall create the case file.; AC 2 Given related incidents exist, When an investigator associates them with the case, Then the solution shall retain the incident relationships.; AC 3 Given persons, vehicles, property, evidence, documents, narratives, or investigative activities are associated with the case, When the associations are saved, Then the solution shall retain the relationships.; AC 4 Given a case contains related records, When an investigator views the case file, Then the investigator shall be able to navigate to authorized related records.; AC 5 Given a related record is removed from the case, When the removal is saved, Then the solution shall update the case relationship while retaining required history.;		
7828	RMS Record Creation	As a Dispatcher, I want to create an RMS record using the required record type and data elements, so that records are established.	AC 1 Given an authorized dispatcher creates an RMS record, When the dispatcher selects an approved record type, Then the solution shall present the required data elements.; AC 2 Given required RMS data elements have been entered, When the dispatcher saves the record, Then the solution shall create the RMS record.; AC 3 Given required RMS data elements are missing, When the dispatcher attempts to save the record, Then the solution shall identify the missing information.; AC 4 Given an RMS record is created, When an Authorized User views the record, Then the solution shall display the configured record type.; AC 5 Given an RMS record requires a unique identifier, When the record is created, Then the solution shall assign the configured identifier.;		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

7830	Evidence Custody Tracking	As an Investigator, I want to record evidence transfers, custody events, and status changes, so that evidence accountability can be demonstrated.	AC 1 Given evidence is transferred between authorized custodians, When the transfer is recorded, Then the solution shall capture the transferring and receiving parties.; AC 2 Given an evidence transfer occurs, When the transfer is saved, Then the solution shall record the date and time.; AC 3 Given evidence changes custody, When the transfer is completed, Then the solution shall update the evidence custody status.; AC 4 Given multiple custody events exist, When an Authorized User views the evidence, Then the solution shall display the custody history.; AC 5 Given an unauthorized user attempts to modify a custody event, When the change is submitted, Then the solution shall prevent the modification.;		
7831	Evidence Intake and Tracking	As an Investigator, I want to record evidence intake, storage location, identifying information, and status, so that evidence remains documented and traceable.	AC 1 Given evidence is received, When an authorized investigator records the evidence intake, Then the solution shall capture the required evidence identifying information.; AC 2 Given evidence is received, When the intake is saved, Then the solution shall record the intake date and time.; AC 3 Given evidence is stored, When the storage location is entered, Then the solution shall associate the storage location with the evidence.; AC 4 Given evidence status changes, When an Authorized User records the change, Then the solution shall update the evidence status.; AC 5 Given evidence has a current storage location and status, When an Authorized User views the evidence record, Then the solution shall display the current information.; AC 6 Given evidence information is updated, When the update is saved, Then the solution shall retain the history.;		
7834	Investigative Record Relationships	As an Investigator, I want to establish and view authorized relationships among investigative records, so that investigators can identify connections across records.	AC 1 Given an investigator is authorized to establish relationships among investigative records, When the investigator creates a relationship, Then the solution shall associate the selected records.; AC 2 Given an authorized relationship exists, When an investigator views a related record, Then the solution shall display the relationship.; AC 3 Given multiple relationships exist, When the investigator views the record, Then the solution shall display the authorized relationships.; AC 4 Given an investigator removes an authorized relationship, When the removal is saved, Then the solution shall update the relationship while retaining required history.; AC 5 Given a user is not authorized to establish investigative relationships, When the user attempts to create one, Then the solution shall prevent the action.;		
7835	Investigative Record Search	As an Investigator, I want to search investigative records across all RMS databases using multiple criteria and navigate to related records, so that investigators can locate associated information and connections.	AC 1 Given an investigator has authorized search access, When the investigator enters one or more supported search criteria, Then the solution shall return matching investigative records.; AC 2 Given an investigator searches using multiple criteria, When the search is executed, Then the solution shall apply the criteria according to configured search rules.; AC 3 Given no records match the search criteria, When the search is executed, Then the solution shall indicate that no matching records were found.; AC 4 Given search results contain authorized related records, When the investigator selects a related record, Then the solution shall navigate to the selected record.; AC 5 Given a search result contains restricted information, When an unauthorized investigator views the results, Then the solution shall exclude the restricted information.;		
7836	Person, Vehicle and Property Associations	As a Dispatcher, I want to associate person, vehicle, and property records with authorized incidents and cases, so that related information can be linked and accessed across RMS records.	AC 1 Given an authorized person record exists, When a dispatcher associates the person with an incident or case, Then the solution shall create the authorized relationship.; AC 2 Given an authorized vehicle record exists, When a dispatcher associates the vehicle with an incident or case, Then the solution shall create the authorized relationship.; AC 3 Given an authorized property record exists, When a dispatcher associates the property with an incident or case, Then the solution shall create the authorized relationship.; AC 4 Given a person, vehicle, or property is associated with an incident, When an Authorized User views the incident, Then the related information shall be available.; AC 5 Given a related record is updated, When an Authorized User views the associated incident or case, Then the solution shall display the current authorized relationship information.;		
7847	RMS Narrative Management	As a Dispatcher, I need the CAD solution to create, edit, view, and retain required RMS narrative information associated with the record, so that record details are documented and maintained for authorized access and review.	AC 1 Given an Authorized User needs to document an RMS narrative, When the user creates the narrative, Then the solution shall associate it with the RMS record.; AC 2 Given a required narrative field exists, When the user attempts to save the record without the required narrative, Then the solution shall identify the missing information.; AC 3 Given an Authorized User edits a narrative, When the change is saved, Then the solution shall retain the updated narrative.; AC 4 Given narrative history is required, When an Authorized User modifies a narrative, Then the solution shall preserve prior history.; AC 5 Given an Authorized User views an RMS record, When the record contains narrative information, Then the authorized user shall be able to view the narrative.;		
7848	Record Sealing and Access Control	As a Dispatcher, I need the CAD solution to seal a record and apply all associated access restrictions in a single action or transaction, so that protected records are not available to unauthorized users.	AC 1 Given a record meets the configured criteria for sealing, When an Authorized User initiates the seal action, Then the solution shall require authorization.; AC 2 Given the sealing action is authorized, When the user completes the action, Then the solution shall change the record to the configured sealed status.; AC 3 Given a record is sealed, When an unauthorized user attempts to access it, Then the solution shall restrict access.; AC 4 Given a record is sealed, When an Authorized User accesses it, Then the solution shall apply the configured authorized access rules.; AC 5 Given a record is sealed, When the seal status is reviewed, Then the solution shall retain the seal date, user, and status history according to configuration.;		
7849	Prior Contact Search	As an Investigator, I want to retrieve authorized prior-contact information using approved criteria, so that associated history can be reviewed without exposing restricted information.	AC 1 Given an investigator has authorized access to prior-contact information, When the investigator enters approved search criteria, Then the solution shall return matching authorized prior-contact records.; AC 2 Given prior-contact records contain restricted information, When the investigator performs a search, Then the solution shall exclude restricted information from the results.; AC 3 Given matching prior-contact records are found, When the investigator selects a result, Then the solution shall display the authorized record information.; AC 4 Given no authorized records match the criteria, When the search is executed, Then the solution shall indicate that no matching authorized records were found.; AC 5 Given prior-contact information is subject to access restrictions, When an unauthorized user attempts to retrieve it, Then the solution shall prevent access.;		

7851	Traffic Stop Records	As an Officer, I want to create and maintain traffic-stop records containing required incident, vehicle, person, race, and disposition information, so that traffic-stop activity is documented.	AC 1 Given an officer initiates a traffic-stop record, When the officer enters the required incident information, Then the solution shall retain the information with the traffic-stop record.; AC 2 Given a vehicle is involved in the traffic stop, When the officer records the vehicle information, Then the solution shall associate the vehicle with the traffic-stop record.; AC 3 Given a person is involved in the traffic stop, When the officer records the person information, Then the solution shall associate the person with the traffic-stop record.; AC 4 Given a disposition is required, When the officer records the disposition, Then the solution shall retain the disposition with the traffic-stop record.; AC 5 Given required traffic-stop information is missing, When the officer attempts to complete the record, Then the solution shall identify the missing information.; AC 6 Given all required information is valid, When the officer saves the record, Then the solution shall retain the completed traffic-stop record.;		
7852	Record Unsealing and Access Restoration	As a Dispatcher, I want to unseal a record when authorized and restore access according to configured rules, so that authorized users can resume access.	AC 1 Given a record is sealed, When an Authorized User initiates the unseal process, Then the solution shall verify the user's authorization.; AC 2 Given the user is authorized to unseal the record, When the unseal action is completed, Then the solution shall restore access according to configured rules.; AC 3 Given a record is unsealed, When an Authorized User accesses the record, Then the user shall have the access permitted by the current record status.; AC 4 Given the unseal action is completed, When the record history is reviewed, Then the solution shall retain the unseal user, date/time, and status information.; AC 5 Given an unauthorized user attempts to unseal a record, When the action is initiated, Then the solution shall prevent the action.;		
7855	Vehicle History Search	As an Investigator, I want to search and view authorized vehicle information from external or historical sources, so that users can obtain associated prior vehicle information for investigative purposes.	AC 1 Given an investigator has authorization to search vehicle information, When the investigator enters supported vehicle criteria, Then the solution shall search authorized sources.; AC 2 Given an external source is available, When the investigator initiates the search, Then the solution shall submit the authorized inquiry.; AC 3 Given historical vehicle information exists, When the search returns the information, Then the solution shall display the authorized historical information.; AC 4 Given no matching vehicle information is found, When the search completes, Then the solution shall indicate that no matching result was found.; AC 5 Given an external lookup fails, When the failure is returned, Then the solution shall display the error or unavailable status.;		
7923	Person Type and Role Assignment	As an Officer or Investigator, I want to assign a configured person type or role to individuals associated with an incident or case, so that each person's involvement is documented and maintained in RMS.	AC 1 Given a person is associated with an incident or case, When an authorized Officer or Investigator assigns a person type or role, Then the solution shall store the selected person type or role with the association.; AC 2 Given an approved person type or role is available, When the user selects the type or role, Then the solution shall validate the selection against the configured values.; AC 3 Given a person's role or type changes, When an Authorized User updates the association, Then the solution shall retain the updated value according to configured record-history requirements.;		
7924	RMS Search and Crime Analysis Mapping	As an Authorized User, I want the solution to provide standardized and customized search capabilities across authorized RMS informational files using defined data formats, search criteria, and validation rules, and to support displaying search results using pin mapping, so that authorized information can be located, analyzed, and visualized geographically for crime analysis.	AC 1 Given an Authorized User has access to RMS informational files, When the user performs a search using approved criteria, Then the solution shall return records matching the defined search criteria.; AC 2 Given search criteria require defined data formats or validation rules, When the user enters search criteria, Then the solution shall validate the entered values before executing the search.; AC 3 Given search results contain geographic information, When the user selects pin mapping, Then the solution shall display eligible results using map pins.; AC 4 Given the user applies additional search criteria, When the search is executed, Then the results shall reflect the selected criteria.;		
7937	Prosecutor and State's Attorney Case Referral	As an Officer or Investigator, I want the solution to support authorized case referral and notification to the prosecutor or State's Attorney office, so that qualifying cases can be referred without unnecessary duplicate data entry.	AC 1 Given a case meets the configured criteria for prosecutor or State's Attorney referral, When an Authorized User initiates the referral, Then the solution shall identify the configured recipient according to configured rules.; AC 2 Given required case information is available, When the referral is submitted, Then the solution shall transmit the authorized information to the configured recipient.; AC 3 Given a referral is successfully submitted, When the transaction is completed, Then the solution shall retain the referral status or reference.; AC 4 Given a referral cannot be transmitted, When the failure occurs, Then the solution shall identify the unsuccessful referral.;		
7947	BOLO and Attempt-to-Locate Management	As an Officer or Investigator, I want to create, distribute, search, update, and track BOLO and Attempt-to-Locate information, so that authorized personnel can receive and act on information about persons, vehicles, or other subjects of interest.	AC 1 Given an authorized Officer or Investigator has information requiring a BOLO or Attempt-to-Locate record, When the user creates the record, Then the solution shall store the subject and activity information.; AC 2 Given an active BOLO or Attempt-to-Locate record exists, When an Authorized User searches for the information, Then the solution shall return matching active records.; AC 3 Given a BOLO or Attempt-to-Locate record requires an update, When an Authorized User updates it, Then the solution shall retain the updated information.; AC 4 Given a BOLO or Attempt-to-Locate record is distributed, When authorized recipients are configured, Then the solution shall distribute the information to those recipients.; AC 5 Given a BOLO or Attempt-to-Locate record changes status, When the change is saved, Then the solution shall track the status.;		
7958	Suspicious Activity Reporting	As an Officer, I want to flag and route suspicious activity reports associated with the National Suspicious Activity Report (SAR) Initiative, so that designated intelligence personnel can receive and process information.	AC 1 Given an Officer identifies activity that meets the configured criteria for a National SAR Initiative suspicious activity report, When the Officer flags the activity, Then the solution shall identify the record as a suspicious activity report.; AC 2 Given a suspicious activity report requires routing, When the Officer submits the report, Then the solution shall route the authorized information to the designated intelligence personnel.; AC 3 Given the report has been routed, When an Authorized User reviews the record, Then the solution shall provide the routing or processing status.;		
7971	Person Information Management	As a Dispatcher or Authorized User, I want to create, update, validate, and maintain identifying and demographic person information, so that authorized person records contain accurate and validated information for operational and case-related use.	AC 1 Given an Authorized User creates or updates a person record, When identifying or demographic information is entered, Then the solution shall validate the information against configured data rules.; AC 2 Given required person information is missing, When the user attempts to save the record, Then the solution shall identify the missing required information.; AC 3 Given valid person information is entered, When the record is saved, Then the solution shall retain the information in the person record.; AC 4 Given an Authorized User updates existing person information, When the update is saved, Then the solution shall retain the updated information according to configured history requirements.;		

7972	Person Record Search and Association	As a Dispatcher or Authorized User, I want to search for and associate authorized person records with incidents, cases, and related records, so that associated person information can be connected to the RMS records.	AC 1 Given an Authorized User searches for a person record, When valid search criteria are entered, Then the solution shall return matching authorized person records.; AC 2 Given a person record is selected for association, When the user associates the person with an incident or case, Then the solution shall create the relationship.; AC 3 Given a person is already associated with a related record, When the association is reviewed, Then the solution shall display the relationship.;		
7973	Vehicle Information Management	As a Dispatcher or Authorized User, I want to create, update, validate, and maintain vehicle identifying information, so that authorized vehicle records contain accurate and validated information for operational and case-related use.	AC 1 Given an Authorized User creates or updates a vehicle record, When vehicle identifying information is entered, Then the solution shall validate the information against configured data rules.; AC 2 Given required vehicle information is missing, When the user attempts to save the record, Then the solution shall identify the missing required information.; AC 3 Given valid vehicle information is entered, When the record is saved, Then the solution shall retain the information in the vehicle record.; AC 4 Given an Authorized User updates existing vehicle information, When the update is saved, Then the solution shall retain the updated information according to configured history requirements.;		
7974	Vehicle Record Search and Association	As a Dispatcher or Authorized User, I want to search for and associate authorized vehicle records with incidents, cases, and related records, so that associated vehicle information is connected to the RMS records.	AC 1 Given an Authorized User searches for a vehicle record, When valid search criteria are entered, Then the solution shall return matching authorized vehicle records.; AC 2 Given a vehicle record is selected for association, When the user associates the vehicle with an incident or case, Then the solution shall create the relationship.; AC 3 Given a vehicle is already associated with a related record, When the association is reviewed, Then the solution shall display the relationship.;		
7975	Property Information Management	As an Authorized User, I want to create, update, validate, and maintain property identifiers and location information, so that authorized property records contain accurate and validated information for operational and case-related use.	AC 1 Given an Authorized User creates or updates a property record, When property identifiers and location information are entered, Then the solution shall validate the information against configured data rules.; AC 2 Given required property information is missing, When the user attempts to save the record, Then the solution shall identify the missing required information.; AC 3 Given valid property information is entered, When the record is saved, Then the solution shall retain the information in the property record.; AC 4 Given an Authorized User updates existing property information, When the update is saved, Then the solution shall retain the updated information according to configured history requirements.;		
7976	Property Record Search and Association	As an Authorized User, I want to search for and associate authorized property records with incidents, cases, and related records, so that associated property information can be connected to the RMS records.	AC 1 Given an Authorized User searches for a property record, When valid search criteria are entered, Then the solution shall return matching authorized property records.; AC 2 Given a property record is selected for association, When the user associates the property with an incident or case, Then the solution shall create the relationship.; AC 3 Given a property is already associated with a related record, When the association is reviewed, Then the solution shall display the relationship.;		
8042	Suspicious CFS Identification	As a Dispatcher or Officer, I want to flag a CFS as suspicious, so that potential suspicious activity reports (SARs) are identified and tracked.	AC 1 Given a CFS exists, When a dispatcher or officer flags it as suspicious, Then the solution shall record the suspicious flag on the CFS; AC 2 Given a CFS is flagged as suspicious, When the flag is applied, Then the solution shall identify the CFS as a potential suspicious activity report for tracking; AC 3 Given a suspicious flag is applied, When the action occurs, Then the solution shall record the flagging user and time; AC 4 Given suspicious CFS records exist, When an Authorized User searches for them, Then the solution shall return the flagged records for review and tracking; AC 5 Given a user lacks permission to flag a CFS as suspicious, When the user attempts it, Then the solution shall prevent the action;		
8043	Suspicious CFS Distribution and Intelligence Notification	As a Supervisor, I want suspicious CFS distributed and the intelligence unit notified, so that suspicious activity reports (SARs) are reviewed.	AC 1 Given a CFS is flagged as suspicious, When the flag is applied, Then the solution shall distribute the suspicious CFS to the configured recipients; AC 2 Given a suspicious CFS is distributed, When the distribution occurs, Then the solution shall notify the intelligence unit; AC 3 Given the intelligence unit is notified, When the notification is sent, Then the solution shall record the notification for tracking; AC 4 Given a notification to the intelligence unit fails, When the failure occurs, Then the solution shall identify the failure for follow-up; AC 5 Given a suspicious CFS requires prompt review, When it is distributed, Then the solution shall make the record available to the intelligence unit for review;		
8062	Location-Based Responder Safety and Dispatch Information	As a Dispatcher, I want the solution to associate responder safety information, premises information, geographically sensitive hazards, and configured dispatch policies with validated locations, so that the solution can provide associated safety information and apply location-specific operational rules during incident response.	AC 1 Given responder safety information, premises information, geographically sensitive hazards, and dispatch policies are associated with validated locations, When an event occurs at a validated location, Then the solution shall provide the safety and premises information to the user; AC 2 Given a validated location has location-specific operational rules, When an incident is processed at that location, Then the solution shall apply the configured dispatch policies; AC 3 Given a geographically sensitive hazard is associated with a location, When an event is created at or near that location, Then the solution shall present the hazard information; AC 4 Given safety information is associated with a location, When the information is displayed, Then the solution shall present it in a manner that is recognizable to the user; AC 5 Given location-associated information changes, When an Authorized User updates it, Then the solution shall reflect the updated information for subsequent incidents at that location;		
8075	Supplemental Incident History Access	As a Dispatcher, I want the solution to enable Windows tabs to be used to allow the dispatcher to select supplemental history about the incident, so that the capability is available in accordance with approved operational requirements.	AC 1 Given supplemental incident history is available, When a dispatcher selects a tab limited to premises history, past event history, hazards, or persons of interest, Then the solution shall display the selected supplemental history for the incident; AC 2 Given multiple categories of supplemental history exist, When the dispatcher navigates the tabs, Then the solution shall allow selection among the available categories; AC 3 Given a supplemental history category has no information, When the dispatcher selects it, Then the solution shall indicate that no information is available; AC 4 Given supplemental history is displayed, When the dispatcher views it, Then the solution shall associate the displayed history with the current incident;		
8126	Location Cautions Management	As a Dispatcher, I want the solution to maintain or interface with a searchable location-based cautions file containing caution categories and narrative details about individuals or circumstances that may affect responder safety at or near a location, so that associated safety information can be identified and considered during incident response.	AC 1 Given a cautions file is provided or interfaced, When caution information pertaining to dangerous or exceptional persons at or near a location is maintained, Then the solution shall retain the caution information with a caution type category and free-form narrative; AC 2 Given caution information exists for a location, When an incident occurs at that location, Then the solution shall make the caution information available; AC 3 Given caution types are recorded, When a user searches by caution type, Then the solution shall return the matching caution records; AC 4 Given a user lacks permission to maintain caution information, When the user attempts the change, Then the solution shall prevent the modification; AC 5 Given caution information is changed, When the change is saved, Then the solution shall record the change with the user and time;		

8202	Person Safety and Warning Indicators	As an Authorized User, I want the solution to display configured safety and warning indicators associated with a person record with officer-safety information, so that authorized personnel can recognize safety considerations when interacting with or responding to a person.	AC 1 Given configured safety and warning indicators associated with a person record with officer-safety information, When an Authorized User interacts with or responds to the person, Then the solution shall display the configured safety and warning indicators; AC 2 Given officer-safety information exists for a person, When the person record is accessed, Then the solution shall present the information so authorized personnel can recognize safety considerations; AC 3 Given a user lacks permission to view a person's safety indicators, When the user attempts access, Then the solution shall enforce the access controls; AC 4 Given safety indicators are configured, When an Authorized User changes them, Then the solution shall apply the updated indicators to subsequent access; AC 5 Given a safety indicator is displayed, When the user views the person record, Then the solution shall present the indicator in a recognizable manner;		
8203	Agency-Managed Incident Tags and Flags	As a System Administrator, I want the solution to allow my agency to define and manage controlled incident tags or flags separate from offense codes, apply multiple tags to an incident, and use those tags for search and reporting, so that agency-specific classifications and operational information can be captured and analyzed.	AC 1 Given controlled incident tags or flags defined separately from offense codes, When a System Administrator defines and manages them, Then the solution shall allow the agency to define and manage the controlled tags; AC 2 Given multiple tags apply to an incident, When a user applies them, Then the solution shall allow multiple tags to be applied to the incident; AC 3 Given tagged incidents exist, When a user searches or reports by tag, Then the solution shall use the tags for search and reporting; AC 4 Given a user lacks permission to manage or apply controlled tags, When the user attempts it, Then the solution shall prevent the action; AC 5 Given tags are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8204	Investigative Case Task Management	As a Case Supervisor, I want the solution to create, assign, track, and complete investigative tasks within a case and notify responsible personnel of task status changes, so that investigative work can be coordinated and monitored without relying on separate spreadsheets or manual tracking.	AC 1 Given a case, When a case supervisor creates and assigns an investigative task, Then the solution shall create the task; AC 2 Given a case, When a case supervisor creates and assigns an investigative task, Then the solution shall associate it with the case and responsible personnel; AC 3 Given an investigative task exists, When its status changes, Then the solution shall track the task status; AC 4 Given an investigative task exists, When its status changes, Then the solution shall notify the responsible personnel of the change; AC 5 Given a task is completed, When the completion is recorded, Then the solution shall update the task status to complete; AC 6 Given tasks are assigned within a case, When a user reviews the case, Then the solution shall display the tasks and their statuses without reliance on separate spreadsheets; AC 7 Given a user lacks permission to create or assign investigative tasks, When the user attempts it, Then the solution shall prevent the action; AC 8 Given a task status change occurs, When it is saved, Then the solution shall record the change with the user and time;		
8230	Phonetic (Soundex) Name Search	As a Dispatcher or Authorized User, I want the solution to provide phonetic sounds-like (Soundex) name searching, so that I can locate persons and records when the exact spelling of a name is unknown or uncertain.	AC 1 Given a user enters a name using phonetic sounds-like search, When the search is executed, Then the solution shall return records that phonetically match the entered name.; AC 2 Given phonetic matches are returned, When the results are displayed, Then the solution shall present the matching records for the user to select.; AC 3 Given both exact and phonetic matches exist, When the search is performed, Then the solution shall include the phonetically matching records according to configured rules.; AC 4 Given a phonetic search returns no matches, When the search is completed, Then the solution shall indicate that no matching records were found.; AC 5 Given a user selects a phonetically matched record, When the selection is made, Then the solution shall make the associated record available for the configured workflow.;		
8233	Place-of-Last-Drink Reporting	As a Law Enforcement Officer, I want to capture place-of-last-drink information on incidents, so that the agency can retain and report the establishment associated with alcohol-related incidents consistent with current practice.	AC 1 Given an alcohol-related incident, When an officer records incident details, Then the solution shall provide a configured field to capture the place-of-last-drink location.; AC 2 Given place-of-last-drink information is entered, When the record is saved, Then the solution shall retain the information with the incident record.; AC 3 Given place-of-last-drink data has been captured, When an Authorized User runs the report, Then the solution shall include the place-of-last-drink information in the results.; AC 4 Given a place-of-last-drink location matches a known establishment, When the information is entered, Then the solution shall support association with the established location record where configured.;		
8816	Mobile Fingerprint Capture and Identification	As a Law Enforcement Officer, I need the RMS solution to support mobile fingerprint capture, submission, and identification processing through the State AFIS and the FBI's NGI system, so that I can obtain fingerprint-based identification results and verify a subject's identity in the field.	AC 1 Given a Law Enforcement Officer is authorized to use mobile fingerprint services, When the officer initiates a fingerprint capture, Then the RMS solution shall support capturing a subject's fingerprints using an approved mobile fingerprint capture device.; AC 2 Given fingerprints have been captured, When the officer submits them for identification, Then the solution shall securely transmit the fingerprint data to the configured identification destination(s) (State AFIS and/or FBI NGI) per the configured routing rules.; AC 3 Given fingerprint data is submitted for processing, When the State AFIS or FBI NGI processes the submission, Then the RMS solution shall receive and make the resulting identification response available to the authorized officer.; AC 4 Given an identification response is received, When the response includes a potential match or identification result, Then the RMS solution shall display the available result information to the authorized officer for review and identity verification.; AC 5 Given fingerprint submission or identification processing cannot be completed, When an error, rejection, or system unavailability occurs, Then the RMS solution shall notify the officer and provide the available error or status information.; AC 6 Given fingerprint data and identification results are processed, When the transaction is completed or an error occurs, Then the RMS solution shall retain the applicable submission status, response information, date and time, and associated user and subject or incident record for audit and traceability.; AC 7 Given fingerprint data or identification results are available in the RMS solution, When a user attempts to access the information, Then the system shall enforce applicable access permissions, privacy, and security requirements.		

8817	VJISS Integration	As an Investigator, I want the solution to query and exchange records with the Vermont Justice Information Sharing System (VJISS), so that I can retrieve a consolidated view of criminal-justice records held across separate agency systems.	AC 1 Given an authorized user initiates a query, When the query targets VJISS, Then the solution shall submit the request to VJISS.; AC 2 Given an authorized user initiates a query, When the query targets VJISS, Then the solution shall return the available consolidated records.; AC 3 Given VJISS returns records, When the response is received, Then the solution shall present the results to the authorized user.; AC 4 Given VJISS returns records, When the response is received, Then the solution shall associate them with the relevant person or incident.; AC 5 Given records are retrieved from VJISS, When they are displayed, Then the solution shall identify the source system for each record.; AC 6 Given a VJISS query fails or returns no results, When the outcome is received, Then the solution shall notify the user.; AC 7 Given a VJISS query fails or returns no results, When the outcome is received, Then the solution shall record the outcome.; AC 8 Given access to VJISS data is restricted by role, When an unauthorized user attempts access, Then the solution shall prevent the query.; AC 9 Given access to VJISS data is restricted by role, When an unauthorized user attempts access, Then the solution shall log the attempt.; AC 10 Given a VJISS transaction occurs, When the transaction completes, Then the solution shall log the request and response for audit.;		
8824	Warrant Query Integration	As a Dispatcher, I want the solution to query and receive warrant information from the NCIC, so that active warrants are visible to officers and dispatchers during call handling and person checks.	AC 1 Given an authorized user performs a person check, When the query is submitted to NCIC, Then the solution shall return any matching active warrant information.; AC 2 Given warrant information is returned from NCIC, When it is received, Then the solution shall present it to the authorized user.; AC 3 Given warrant information is returned from NCIC, When it is received, Then the solution shall associate it with the relevant person or incident.; AC 4 Given a warrant hit is returned, When it is displayed, Then the solution shall indicate the warrant status, issuing agency, and hit-confirmation requirement.; AC 5 Given a warrant hit requires confirmation, When the user initiates confirmation, Then the solution shall support the hit-confirmation exchange with the originating agency.; AC 6 Given an NCIC warrant query fails or returns no result, When the outcome is received, Then the solution shall notify the user.; AC 7 Given an NCIC warrant query fails or returns no result, When the outcome is received, Then the solution shall record the outcome.; AC 8 Given access to warrant data is restricted by role and CJIS requirements, When an unauthorized user attempts access, Then the solution shall prevent the query.; AC 9 Given access to warrant data is restricted by role and CJIS requirements, When an unauthorized user attempts access, Then the solution shall log the attempt.; AC 10 Given a warrant query transaction occurs, When the transaction completes, Then the solution shall log the request and response for audit.;		
8825	Vermont Intelligence Center (VIC) Integration	As an Investigator, I want the solution to exchange criminal-intelligence and threat information with the VIC, so that relevant intelligence is shared with and received from the VIC to support investigations and officer safety.	AC 1 Given an authorized user identifies information for intelligence sharing, When the user submits it to the VIC, Then the solution shall transmit the configured information to the VIC.; AC 2 Given the VIC provides intelligence or threat information, When it is received, Then the solution shall present it to authorized users.; AC 3 Given the VIC provides intelligence or threat information, When it is received, Then the solution shall associate it with the relevant person, location, or incident.; AC 4 Given intelligence information is exchanged, When it is handled, Then the solution shall restrict access according to role and handling caveats.; AC 5 Given a VIC exchange fails, When the failure is detected, Then the solution shall notify the user.; AC 6 Given a VIC exchange fails, When the failure is detected, Then the solution shall retain the status.; AC 7 Given a VIC transaction occurs, When the transaction completes, Then the solution shall log the exchange for audit.;		
8826	DOC Probation & Parole Supervision Status Exchange	As an Officer, I want the solution to retrieve probation and parole supervision information from the Department of Corrections community-supervision system, so that I am aware of a subject's supervision status and conditions during an encounter.	AC 1 Given an authorized user queries a person, When the person is under community supervision, Then the solution shall return the available probation or parole status from the DOC system.; AC 2 Given supervision information is returned, When it is received, Then the solution shall present the conditions of supervision and compliance status to the authorized user.; AC 3 Given supervision information is displayed, When it is shown, Then the solution shall associate it with the relevant person or incident record.; AC 4 Given supervision information is displayed, When it is shown, Then the solution shall identify the source.; AC 5 Given a supervision query fails or returns no result, When the outcome is received, Then the solution shall notify the user.; AC 6 Given a supervision query fails or returns no result, When the outcome is received, Then the solution shall record the outcome.; AC 7 Given access to supervision data is restricted by role, When an unauthorized user attempts access, Then the solution shall prevent the query.; AC 8 Given access to supervision data is restricted by role, When an unauthorized user attempts access, Then the solution shall log the attempt.; AC 9 Given a supervision data transaction occurs, When the transaction completes, Then the solution shall log the request and response for audit.;		

8834	Commercial Motor Vehicle Enforcement	As a Law Enforcement Officer, I need the solution to provide a Commercial Motor Vehicle (CMV) Enforcement module that supports the documentation and management of commercial vehicle inspections, vehicle and driver information, motor carrier information, inspection results, violations, citations, warnings, out-of-service orders, enforcement actions, and associated historical records, so that CMV enforcement activities can be efficiently administered, consistently documented, tracked, and reported to support commercial motor vehicle safety and regulatory compliance in Vermont.	AC 1 Given an authorized Law Enforcement Officer initiates a CMV enforcement activity, When the officer creates an inspection record, Then the CAD solution shall allow the officer to document the inspection date, time, location, inspection type, and applicable inspection details.; AC 2 Given a CMV inspection is being documented, When the officer enters commercial vehicle and driver information, Then the system shall allow the officer to record and associate the applicable vehicle identifiers, registration, driver identification, and other required information with the inspection record.; AC 3 Given a CMV inspection involves a motor carrier, When the officer documents the inspection, Then the system shall allow the officer to record and associate the applicable motor carrier identification and information with the inspection record.; AC 4 Given an inspection has been completed, When the officer records the inspection results, Then the system shall allow the officer to document applicable inspection findings, deficiencies, violations, and compliance information.; AC 5 Given an inspection identifies a violation or enforcement condition, When the officer records the enforcement outcome, Then the system shall support documentation of applicable citations, warnings, out-of-service orders, and other enforcement actions.; AC 6 Given an enforcement action is issued, When the officer completes the associated record, Then the system shall associate the enforcement action with the applicable inspection, vehicle, driver, and motor carrier records.; AC 7 Given a CMV inspection or enforcement record has been created, When an authorized user searches for historical information, Then the system shall retrieve applicable inspection results, violations, citations, warnings, out-of-service orders, and enforcement actions associated with the vehicle, driver, or motor carrier.; AC 8 Given an authorized user accesses CMV enforcement records, When the user views or updates an applicable record, Then the system shall enforce assigned access permissions and retain applicable record history and audit information.; AC 9 Given CMV inspection and enforcement information is available for reporting, When an authorized user generates a report, Then the system shall provide applicable information to support tracking, analysis, and reporting of CMV enforcement activities and regulatory compliance.		
8836	LexisNexis Integration	As an Authorized Law Enforcement User, I need the solution to securely access and retrieve authorized investigative and public-record information from LexisNexis through an approved interface, so that relevant information is available to support law enforcement investigations and decision-making.	AC 1 Given an authorized law enforcement user needs investigative or public-record information, When the user submits a search request through the CAD solution, Then the system shall securely transmit the request to LexisNexis through the approved interface.; AC 2 Given a search request meets applicable authorization requirements, When LexisNexis returns matching information, Then the CAD solution shall make the retrieved information available to the authorized requesting user.; AC 3 Given LexisNexis returns multiple matching records, When the search results are displayed, Then the system shall present the available results and associated identifying information to support review and selection.; AC 4 Given an authorized user selects retrieved information for an investigation, When the user associates the information with an incident, case, person, vehicle, or other applicable record, Then the system shall retain the information or an accessible reference to it with the selected record.; AC 5 Given a user requests information or attempts to access retrieved information, When the system evaluates the request, Then the system shall enforce applicable access permissions and restrictions on investigative and public-record information.; AC 6 Given a LexisNexis request fails or returns an error, When the failure is detected, Then the system shall identify the unsuccessful transaction and make the error available for authorized review.; AC 7 Given information is retrieved from LexisNexis, When the information is accessed or associated with an operational record, Then the system shall retain applicable source, retrieval date and time, and transaction information for traceability.		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 05: Fire, EMS & Patient Care Operations					
7816	Fire and EMS Tone-Out	As a Dispatcher, I want to initiate multi-channel tone-out notifications for fire and EMS responders, so that the responders receive notification of an incident.	AC 1 Given an incident requires volunteer fire or EMS notification, When the dispatcher initiates a tone-out, Then the solution shall identify the configured responders or responder groups.; AC 2 Given multiple notification channels are configured, When the dispatcher initiates the tone-out, Then the solution shall transmit the notification through each supported channel.; AC 3 Given a notification channel fails, When the solution detects the failure, Then the solution shall record the failed notification status.; AC 4 Given a tone-out has been transmitted, When an Authorized User reviews the incident, Then the solution shall display the notification status.; AC 5 Given a responder group is not eligible for the incident, When the tone-out is initiated, Then the solution shall exclude the group according to configured rules.;		
7860	EMS Incident Management	As a Dispatcher, I want to manage an EMS incident from creation through disposition and records completion, so that EMS incidents are documented.	AC 1 Given an EMS incident is received, When the dispatcher creates the incident, Then the solution shall establish the EMS incident using the configured EMS workflow.; AC 2 Given an EMS incident is active, When dispatch or incident information changes, Then the solution shall update the EMS record.; AC 3 Given EMS resources are assigned, When the assignments are recorded, Then the solution shall associate the resources with the EMS incident.; AC 4 Given an EMS incident reaches disposition, When the dispatcher records the disposition, Then the solution shall retain the final EMS disposition.; AC 5 Given required EMS records information is missing, When the dispatcher attempts to complete the incident, Then the solution shall identify the missing information.; AC 6 Given all required EMS information is complete, When the incident is finalized, Then the solution shall retain the completed EMS record.;		
7861	Fire Incident Management	As a Dispatcher, I want to manage a fire incident from dispatch through disposition and records completion, so that fire incidents are documented.	AC 1 Given a fire incident is received, When the dispatcher creates the incident, Then the solution shall establish the fire incident using the configured fire workflow.; AC 2 Given a fire incident is dispatched, When resources are assigned, Then the solution shall record the resource assignments.; AC 3 Given fire incident status changes, When the dispatcher records the change, Then the solution shall update the incident status.; AC 4 Given a fire incident reaches disposition, When the dispatcher records the disposition, Then the solution shall retain the final fire disposition.; AC 5 Given required fire records information is missing, When the dispatcher attempts to complete the incident, Then the solution shall identify the missing information.; AC 6 Given all required fire information is complete, When the incident is finalized, Then the solution shall retain the completed fire incident record.;		

7862	NEMSIS Data Submission	As a Responder, I need the solution to transfer required EMS patient-care and incident information to SIREN in accordance with NEMSIS and Vermont reporting requirements, so that mandatory EMS reporting is complete, accurate, and available to the reporting authority.	AC 1 Given an EMS incident contains the information required for regulatory reporting, When the authorized user prepares the incident for submission, Then the solution shall validate and format the NEMSIS and Vermont-specific data elements in accordance with the current reporting specifications established by the Vermont Department of Health.; AC 2 Given the NEMSIS data passes validation, When the responder submits the data, Then the solution shall transmit the submission to the configured reporting authority.; AC 3 Given the submission is accepted, When the reporting authority returns an acceptance, Then the solution shall record the submission outcome.; AC 4 Given the submission fails, When the reporting authority returns an error, Then the solution shall record the error and submission status.; AC 5 Given required NEMSIS information is missing, When the responder attempts submission, Then the solution shall identify the missing information.;		
7863	NEMSIS Submission Status	As an EMS Responder, I want to view NEMSIS submission status, errors, and outcomes, so that staff can identify successful, failed, and pending submissions.	AC 1 Given a NEMSIS submission has been transmitted, When the solution receives a response, Then the solution shall record the submission status.; AC 2 Given a NEMSIS submission is successful, When the response is received, Then the solution shall identify the submission as successful.; AC 3 Given a NEMSIS submission fails, When the response is received, Then the solution shall identify the submission as failed.; AC 4 Given a NEMSIS submission fails, When the response is received, Then the solution shall display available error information.; AC 5 Given a NEMSIS submission remains pending, When the status is received, Then the solution shall identify the submission as pending.; AC 6 Given a submission has an error, When an Authorized User reviews the submission, Then the user shall be able to access the available error information.;		
7864	NEMSIS Validation and Correction	As an EMS Responder, I want to validate NEMSIS records, identify errors, correct authorized errors, and revalidate records, so that compliant EMS data can be submitted.	AC 1 Given a NEMSIS record is prepared for submission, When the solution validates the record, Then the solution shall identify errors.; AC 2 Given a NEMSIS validation error is identified, When an authorized responder reviews the record, Then the affected information shall be identifiable.; AC 3 Given an authorized responder corrects an error, When the correction is saved, Then the solution shall update the NEMSIS record.; AC 4 Given corrections have been made, When the responder revalidates the record, Then the solution shall return the current validation status.; AC 5 Given the NEMSIS record passes validation, When the responder prepares the submission, Then the solution shall identify the record as eligible for submission.;		
7865	NERIS Data Submission	As a Fire Responder, I want to prepare and submit NERIS data using the required reporting structure and process, so that fire incident data is reported.	AC 1 Given fire incident records contain required NERIS information, When an authorized responder prepares an NERIS submission, Then the solution shall generate the configured NERIS reporting structure.; AC 2 Given NERIS data is ready for submission, When the responder validates the data, Then the solution shall return the validation status.; AC 3 Given NERIS data passes validation, When the responder submits the data, Then the solution shall transmit the submission through the configured reporting process.; AC 4 Given an NERIS submission fails, When the failure is returned, Then the solution shall record the failure and available error information.; AC 5 Given an NERIS submission is accepted, When the acceptance is returned, Then the solution shall record the submission outcome.;		
7866	NERIS Submission Status	As a Fire Responder, I want to view NERIS submission status, errors, and outcomes, so that staff can identify successful, failed, and pending submissions.	AC 1 Given an NERIS submission has been transmitted, When the reporting authority returns a status, Then the solution shall record the status.; AC 2 Given an NERIS submission is successful, When the response is received, Then the solution shall identify the submission as successful.; AC 3 Given an NERIS submission fails, When the response is received, Then the solution shall identify the submission as failed.; AC 4 Given an NERIS submission is pending, When the pending status is received, Then the solution shall identify the submission as pending.; AC 5 Given an NERIS submission has an error, When an authorized responder views the submission, Then the solution shall display the available error information.;		
7867	NERIS Validation and Correction	As a Fire Responder, I want to validate NERIS records, identify errors, correct authorized errors, and revalidate records, so that compliant fire data can be submitted.	AC 1 Given an NERIS record is prepared for submission, When the solution validates the record, Then the solution shall identify errors.; AC 2 Given an NERIS validation error is identified, When an authorized responder reviews the record, Then the affected information shall be identifiable.; AC 3 Given an authorized responder corrects an NERIS error, When the correction is saved, Then the solution shall update the record.; AC 4 Given NERIS errors have been corrected, When the responder revalidates the record, Then the solution shall return the current validation status.; AC 5 Given the NERIS record passes validation, When the responder prepares the submission, Then the solution shall identify the record as eligible for submission.;		
7991	Response and Transport Mileage	As a Responder, I want the solution to capture and validate beginning and ending mileage for responses and transports, so that mileage associated with each response or transport is recorded.	AC 1 Given a response or transport requires mileage capture, When a responder enters beginning and ending mileage, Then the solution shall record the mileage values associated with that response or transport; AC 2 Given a responder enters ending mileage that is less than the beginning mileage, When the mileage is submitted, Then the solution shall identify the invalid entry; AC 3 Given a responder enters ending mileage that is less than the beginning mileage, When the mileage is submitted, Then the solution shall prevent acceptance until corrected; AC 4 Given required mileage fields are incomplete for a response, When the responder submits the record, Then the solution shall identify the missing mileage; AC 5 Given required mileage fields are incomplete for a response, When the responder submits the record, Then the solution shall prevent completion; AC 6 Given beginning and ending mileage are recorded, When an Authorized User views the response or transport record, Then the solution shall display the captured mileage associated with that record; AC 7 Given mileage is captured for a transport, When the record is persisted, Then the solution shall retain the mileage as part of the transport record for reporting purposes;		
7992	AVL-Assisted Mileage and Reporting	As a Responder, I want the solution to support available AVL-assisted mileage, authorized mileage corrections, and downstream reporting, so that response and transport mileage can be captured, corrected when authorized, and reported.	AC 1 Given AVL-assisted mileage is available for a response, When mileage is captured, Then the solution shall populate the response mileage using the available AVL-derived value; AC 2 Given an Authorized User identifies an incorrect mileage value, When the user applies a mileage correction, Then the solution shall update the mileage; AC 3 Given an Authorized User identifies an incorrect mileage value, When the user applies a mileage correction, Then the solution shall retain the original value, the corrected value, the reason, and the user; AC 4 Given a user without correction authorization attempts to change recorded mileage, When the change is submitted, Then the solution shall prevent the correction; AC 5 Given mileage has been captured or corrected, When an Authorized User generates mileage reporting, Then the solution shall include the current mileage values in the report output; AC 6 Given a mileage correction has been made, When an Authorized User reviews the mileage history, Then the solution shall provide an auditable record of the original and corrected values;		

7993	Supplemental Resource Provider Management	As a Dispatcher, I want to maintain authorized supplemental resource providers, services, contacts, and preferences, so that supplemental resources can be identified and contacted using current and approved information.	AC 1 Given an Authorized User maintains supplemental resource provider information, When the user adds or updates a provider, service, contact, or preference, Then the solution shall persist the current provider information; AC 2 Given required provider information is incomplete, When the user attempts to save the provider record, Then the solution shall identify the missing required information; AC 3 Given required provider information is incomplete, When the user attempts to save the provider record, Then the solution shall prevent saving; AC 4 Given a user without configured permissions attempts to modify supplemental provider information, When the change is submitted, Then the solution shall prevent the modification; AC 5 Given supplemental providers are maintained, When a dispatcher searches for a supplemental resource, Then the solution shall return current and approved provider information; AC 6 Given provider information is changed, When an Authorized User reviews the provider record history, Then the solution shall provide a record of the change and the user who made it;		
7994	Supplemental Resource Dispatch	As a Dispatcher, I want to select, contact, dispatch, track, and document supplemental resources, so that supplemental resources can be incorporated into incident response and their involvement is recorded.	AC 1 Given approved supplemental providers exist, When a dispatcher selects a supplemental resource for an incident, Then the solution shall associate the selected supplemental resource with the incident; AC 2 Given a supplemental resource is selected, When the dispatcher records contact and dispatch of the resource, Then the solution shall record the contact and dispatch actions with date/time stamps; AC 3 Given a supplemental resource is dispatched, When the resource's involvement progresses, Then the solution shall allow the dispatcher to track its status on the incident; AC 4 Given a supplemental resource's involvement is complete, When the dispatcher documents the outcome, Then the solution shall persist the documentation with the incident record; AC 5 Given a supplemental resource has been incorporated into an incident, When an Authorized User reviews the incident history, Then the solution shall present the supplemental resource's selection, contact, dispatch, and documentation; AC 6 Given required information to dispatch a supplemental resource is incomplete, When the dispatcher attempts to dispatch it, Then the solution shall identify the missing information; AC 7 Given required information to dispatch a supplemental resource is incomplete, When the dispatcher attempts to dispatch it, Then the solution shall prevent dispatch;		
7995	EMS Patient Destination and Disposition	As a Responder, I want to associate patients with EMS incidents and track destination and disposition information, so that patient movement and disposition are associated with the EMS incident.	AC 1 Given an EMS incident, When a responder associates a patient with the incident, Then the solution shall link the patient to the EMS incident; AC 2 Given a patient is associated with an EMS incident, When the responder records destination information, Then the solution shall persist the destination with the patient and incident; AC 3 Given a patient is transported, When the responder records disposition information, Then the solution shall associate the disposition with the patient and the EMS incident; AC 4 Given multiple patients are associated with a single EMS incident, When the responder enters patient information, Then the solution shall maintain each patient's destination and disposition independently; AC 5 Given required patient association information is incomplete, When the responder submits the record, Then the solution shall identify the missing information; AC 6 Given required patient association information is incomplete, When the responder submits the record, Then the solution shall prevent completion; AC 7 Given patient movement and disposition are recorded, When an Authorized User reviews the EMS incident, Then the solution shall display the associated patient destination and disposition information;		
7996	Hospital Status and Diversion	As a Responder, I want the solution to receive approved hospital status and diversion information and make it available for destination decisions, so that hospital availability can be considered during EMS transport coordination.	AC 1 Given approved hospital status and diversion information is received, When the solution processes the information, Then the solution shall make the current hospital status and diversion status available for destination decisions; AC 2 Given hospital diversion status changes, When updated information is received, Then the solution shall update the displayed hospital status accordingly; AC 3 Given a responder is determining a transport destination, When the responder views hospital availability, Then the solution shall present the current approved hospital status and diversion information; AC 4 Given hospital status information is unavailable or not received, When a responder views hospital availability, Then the solution shall indicate that current status is unavailable; AC 5 Given hospital status information is received, When the information is processed, Then the solution shall retain a record of the received hospital status for the EMS incident;		
8013	EMS Hospital Information Exchange	As a Responder, I want the solution to securely share approved EMS incident and patient information with the receiving hospital, so that hospital personnel receive information needed to support patient care and transport coordination.	AC 1 Given a responder is authorized to share EMS information, When the responder shares approved EMS incident and patient information with the receiving hospital, Then the solution shall transmit the information securely to the receiving hospital; AC 2 Given a user is not authorized to share patient information, When the user attempts to share it, Then the solution shall prevent the sharing; AC 3 Given EMS information is shared with a hospital, When the transmission completes, Then the solution shall confirm successful delivery to the responder; AC 4 Given a secure transmission to the hospital fails, When the failure occurs, Then the solution shall notify the responder that the information was not delivered; AC 5 Given EMS and patient information is shared, When the exchange occurs, Then the solution shall retain an auditable record of the information shared and the recipient; AC 6 Given approved EMS information is shared, When the hospital receives it, Then the solution shall associate the shared information with the EMS incident;		
8014	Hospital Notification and Workflow	As a Responder, I want the solution to notify the receiving hospital and initiate configured hospital workflows when specified EMS events occur, so that required hospital coordination actions occur within the operational timeframe.	AC 1 Given configured hospital workflows for specified EMS events, When a specified EMS event occurs, Then the solution shall notify the receiving hospital and initiate the configured workflow; AC 2 Given a configured EMS event triggers hospital coordination, When the workflow is initiated, Then the solution shall perform the configured actions within the operational timeframe; AC 3 Given a hospital notification fails, When the failure occurs, Then the solution shall identify the failure for follow-up; AC 4 Given an EMS event does not meet the configured notification conditions, When the event occurs, Then the solution shall initiate the hospital workflow only when the configured notification conditions are met.; AC 5 Given a hospital workflow is initiated, When the workflow executes, Then the solution shall record the notification and workflow actions with date/time stamps; AC 6 Given an authorized administrator configures hospital notification rules, When the configuration is saved, Then the solution shall apply the rules to subsequent qualifying EMS events;		

8065	Multiple Patient Transports	As a Dispatcher, I want the solution to allow multiple transports by the same unit on the same incident, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a single unit performs multiple transports on the same incident, When the responder records each transport, Then the solution shall allow multiple transports by the same unit on the same incident; AC 2 Given multiple transports are recorded for one unit on an incident, When they are saved, Then the solution shall maintain each transport as a distinct record associated with the incident; AC 3 Given multiple transports exist on an incident, When an Authorized User views the incident, Then the solution shall display each transport and its associated details; AC 4 Given required transport information is incomplete, When the responder submits a transport, Then the solution shall identify the missing information; AC 5 Given required transport information is incomplete, When the responder submits a transport, Then the solution shall prevent completion;		
8152	Automatic Premises Information Retrieval	As a Dispatcher, I want the solution to retrieve and display premises information and information about the surrounding or adjacent area during CFS creation, so that associated location and safety information is available to support fire and EMS response operations.	AC 1 Given a CFS is being created, When premises information and information about the surrounding or adjacent area exists, Then the solution shall retrieve and display that information; AC 2 Given premises and area information is displayed during CFS creation, When the dispatcher reviews it, Then the solution shall present the associated location and safety information to support fire and EMS response; AC 3 Given no premises or area information exists, When the CFS is created, Then the solution shall indicate that none is available; AC 4 Given the CFS location changes during creation, When the new location is validated, Then the solution shall update the retrieved premises and area information;		
8205	Automated Field Medical Alert Workflows	As an EMS Dispatcher, I want the solution to identify qualifying medical conditions and initiate configurable, region-specific medical alert workflows, so that required notifications and resources can be initiated.	AC 1 Given configurable, region-specific medical alert workflows, When an EMS dispatcher identifies a qualifying field medical condition, Then the solution shall initiate the configured medical alert workflow; AC 2 Given a medical alert workflow is initiated, When it executes, Then the solution shall initiate the required notifications and resources limited to hospital notification, air medical coordination, and landing zone identification; AC 3 Given a field medical condition does not qualify, When it is evaluated, Then the solution shall initiate the medical alert workflow only for qualifying conditions.; AC 4 Given an Authorized User configures region-specific medical alert workflows, When the configuration is saved, Then the solution shall persist the workflow configuration; AC 5 Given a medical alert workflow is initiated, When the actions occur, Then the solution shall record the notifications and resource actions with date/time stamps; AC 6 Given a required notification within the workflow fails, When the failure occurs, Then the solution shall identify the failure for follow-up;		
8212	Career & Combination Fire/EMS Alerting: Unit and Station Specific	As a Dispatcher, I need the solution to initiate station alerting addressed to specific units and specific stations for career and combination fire/EMS departments, so that the correct stations and units are alerted for each incident.	AC 1 Given an incident requires fire or EMS response, When the dispatcher initiates station alerting, Then the solution shall allow selection of the configured target units and stations.; AC 2 Given a resource recommendation identifies responding units and their assigned stations, When the dispatcher initiates alerting, Then the solution shall target the stations associated with the recommended units.; AC 3 Given a station-specific alert is initiated, When the solution transmits the alert, Then the solution shall deliver it only to the selected stations and units.; AC 4 Given a unit or station is not associated with the incident, When the alert is initiated, Then the solution shall exclude that unit or station according to configured rules.; AC 5 Given a station alert is transmitted, When an Authorized User reviews the incident, Then the solution shall display the targeted stations and units and the alert status.; AC 6 Given a station alert fails to transmit, When the failure is detected, Then the solution shall record the failure.; AC 7 Given a station alert fails to transmit, When the failure is detected, Then the solution shall notify the dispatcher according to configured rules.;		
8213	Simultaneous Multi-Station and Multi-Agency Alerting	As a Dispatcher, I want the solution to alert multiple stations and multiple agencies simultaneously for a single incident, so that all required stations and agencies are notified at the same time without sequential delay.	AC 1 Given an incident requires response from multiple stations or agencies, When the dispatcher initiates alerting, Then the solution shall transmit the alert to all selected stations and agencies simultaneously.; AC 2 Given multiple stations or agencies are targeted, When the alert is transmitted, Then the solution shall send the alert to all targeted stations or agencies in a single action.; AC 3 Given automatic-aid or mutual-aid agreements apply, When alerting is initiated, Then the solution shall include the configured aid stations and agencies according to the agreement.; AC 4 Given one or more targeted destinations fail, When the failure is detected, Then the solution shall record each destination's status individually.; AC 5 Given one or more targeted destinations fail, When the failure is detected, Then the solution shall notify the dispatcher.; AC 6 Given a simultaneous alert is transmitted, When an Authorized User reviews the incident, Then the solution shall display each targeted station and agency and its individual delivery status.;		
8214	Automated Station Device Activation	As a Dispatcher, I want the solution to activate approved station alerting devices, so that responders are alerted through all configured mechanisms.	AC 1 Given a station has configured approved alerting devices, When a station alert is initiated, Then the solution shall activate each configured device with voice, tones, lights, displays, printers, and mobile applications.; AC 2 Given an alert includes incident information, When the devices are activated, Then the solution shall transmit the configured information to each device in its supported format.; AC 3 Given the solution does not supply the station hardware, When it activates station devices, Then the solution shall control the alerting process through the approved interfaces to that hardware.; AC 4 Given a device is unavailable or not configured, When the alert is initiated, Then the solution shall process the alert through the remaining configured devices.; AC 5 Given a device is unavailable or not configured, When the alert is initiated, Then the solution shall record the exception.; AC 6 Given a device activation fails, When the failure is detected, Then the solution shall record the per-device delivery or failure status.; AC 7 a Given station devices have been activated, When an Authorized User reviews the incident, Then the solution shall display the activated devices and their individual status.; AC 8 b Given station devices have been activated, When an Authorized User reviews the incident, Then the solution shall retain an auditable record of the activation and its outcome.;		

8215	Day and Night Alerting Profiles	As a System Administrator, I want the solution to support configurable day and night alerting profiles per station, so that alerting behavior (devices, intensity, and routing) matches each station's time-of-day operational needs.	AC 1 Given an authorized administrator configures alerting profiles, When the administrator defines day and night profiles per station with devices, intensity, routing, and schedule, Then the solution shall persist the configured profiles.; AC 2 Given day and night profiles are configured with an effective schedule, When a station alert is initiated, Then the solution shall apply the profile in effect for the current time of day.; AC 3 Given a profile or its schedule is changed, When a subsequent alert is initiated, Then the solution shall apply the current approved profile.; AC 4 Given an authorized administrator overrides the active profile, When the override is applied, Then the solution shall use the overriding profile.; AC 5 Given an authorized administrator overrides the active profile, When the override is applied, Then the solution shall record the change.; AC 6 Given an invalid profile configuration is entered, When the administrator attempts to save it, Then the solution shall identify the invalid configuration.; AC 7 Given an invalid profile configuration is entered, When the administrator attempts to save it, Then the solution shall prevent saving.; AC 8 Given a profile is applied to an alert, When an Authorized User reviews the incident, Then the solution shall identify which profile, day or night, was in effect.;		
8216	EMS Information Transfer to Siren/ePCR	As an EMS User, I want the solution to transfer EMS information to the Siren/ePCR platform at the conclusion of the call, so that complete documentation is available for EMS reporting and follow-up.	AC 1 Given an EMS call has concluded, When the solution processes the completed call, Then the solution shall transfer the EMS information to the Siren/ePCR platform.; AC 2 Given EMS information is associated with the completed call, When the transfer is initiated, Then the solution shall transmit the required information to the corresponding Siren/ePCR record.; AC 3 Given the Siren/ePCR platform successfully receives the EMS information, When the transfer is completed, Then the solution shall record the transfer status.; AC 4 Given the Siren/ePCR platform successfully receives the EMS information, When the transfer is completed, Then the solution shall make the result available to authorized users.; AC 5 Given the EMS information transfer fails or is incomplete, When the failure is detected, Then the solution shall identify the unsuccessful transfer.; AC 6 Given the EMS information transfer fails or is incomplete, When the failure is detected, Then the solution shall make the error available for authorized review.; AC 7 Given EMS information has been transferred to Siren/ePCR, When an Authorized User reviews the record, Then the transferred information shall be available for EMS reporting and follow-up.; AC 8 Given EMS information is transferred for a completed call, When the transfer is processed, Then the solution shall maintain the association between the EMS information and the originating CAD call or incident.;		
8237	Emergency Medical Dispatch (EMD) Protocol Integration	As a Dispatcher, I want the solution to integrate with an Emergency Medical Dispatch (EMD) protocol tool, so that medical calls are triaged using approved protocols and the resulting determinant codes drive call classification and response recommendations.	AC 1 Given a configured EMD protocol interface, When a medical call is processed, Then the solution shall launch or exchange data with the EMD protocol tool.; AC 2 Given an EMD determinant code is produced, When triage completes, Then the solution shall associate the determinant code with the call or incident.; AC 3 Given a determinant code is assigned, When the solution evaluates response rules, Then it shall apply the configured response recommendation for that determinant.; AC 4 Given EMD triage is performed, When the incident record is reviewed, Then the solution shall retain the protocol responses and determinant code with the record.; AC 5 Given the EMD interface is unavailable, When a medical call is processed, Then the solution shall allow manual classification.; AC 6 Given the EMD interface is unavailable, When a medical call is processed, Then the solution shall record that EMD triage was not completed.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 06: Records, Data, Reporting & Compliance					
7829	RMS Data Quality and Duplicate Resolution	As a Dispatcher, I want to identify and resolve duplicate, invalid, or incomplete records using approved data-quality rules, so that existing CAD/RMS data is accurate and usable.	AC 1 Given an RMS record contains duplicate information, When the solution evaluates the record using approved data-quality rules, Then the solution shall identify the potential duplicate.; AC 2 Given an RMS record contains invalid information, When the solution validates the record, Then the solution shall identify the validation error.; AC 3 Given an RMS record contains incomplete required information, When validation occurs, Then the solution shall identify the missing information.; AC 4 Given an Authorized User resolves a data-quality issue, When the correction is saved, Then the solution shall update the record.; AC 5 Given a data-quality issue has been resolved, When the record is revalidated, Then the solution shall reflect the updated validation status.; AC 6 Given a data-quality correction is made, When the record history is reviewed, Then the solution shall retain the correction history.;		
7838	Public Records Request Management	As an Authorized User, I want to manage public-records requests through intake, review, response, and disposition, so that requests are documented and completed.	AC 1 Given an Authorized User receives a public-records request, When the request is entered, Then the solution shall create a request record.; AC 2 Given a public-records request is created, When required intake information is entered, Then the solution shall retain the information with the request.; AC 3 Given a request requires review, When the request enters review, Then the solution shall record the review status.; AC 4 Given a response is issued, When the response is recorded, Then the solution shall retain the response information and date.; AC 5 Given a request is completed, When the disposition is recorded, Then the solution shall retain the final disposition and history.; AC 6 Given a request is restricted to authorized users, When an unauthorized user attempts to access it, Then the solution shall prevent access.;		
7842	Data Validation and Quality Controls	As a Dispatcher, I want the solution to identify missing, invalid, or inconsistent information when records are created or updated, so that records meet defined data-quality requirements.	AC 1 Given a record is being created, When the solution evaluates required fields, Then the solution shall identify missing required information.; AC 2 Given a record contains an invalid value, When validation occurs, Then the solution shall identify the invalid value.; AC 3 Given a record contains inconsistent information, When configured validation rules are executed, Then the solution shall identify the inconsistency.; AC 4 Given a record contains a validation error, When the user attempts to complete the transaction, Then the solution shall prevent completion or identify the error according to configured rules.; AC 5 Given identified errors are corrected, When the record is revalidated, Then the solution shall reflect the current validation status.;		

7845	Records Retention, Legal Holds and Disposition	As a System Administrator, I need the solution to apply approved State records-retention pursuant to 1 V.S.A. ?315, legal-hold, and disposition requirements to records, so that records are retained and disposed of according to configured law and policy.	AC 1 Given a record is subject to an approved State retention schedule, When the solution evaluates the record, Then the solution shall apply the configured retention period.; AC 2 Given a record is subject to a legal hold, When the solution evaluates the record, Then the solution shall prevent disposition while the legal hold remains active.; AC 3 Given a legal hold is released, When the release is recorded, Then the solution shall update the record's hold status.; AC 4 Given a record reaches its approved disposition date and is not subject to a legal hold, When the disposition process is initiated, Then the solution shall apply the approved disposition rule.; AC 5 Given a record is disposed, When the disposition is completed, Then the solution shall retain the required disposition history.; AC 6 Given a record is subject to conflicting retention or disposition conditions, When the solution evaluates the record, Then the solution shall apply the configured precedence rules.;		
7857	UCR/NIBRS Crime Data Submission	As a Law Enforcement Officer, I need to prepare and submit crime incident data in accordance with FBI NIBRS specifications and Vermont UCR reporting requirements, so that crime data is complete, accurate, and compliant with federal and State reporting requirements.	AC 1 Given a crime incident contains the data elements required for NIBRS and Vermont UCR reporting, When an authorized user prepares the incident for submission, Then the solution shall validate and format the data per current FBI NIBRS specifications and Vermont UCR requirements.; AC 2 Given the crime data passes validation, When the user submits the data, Then the solution shall transmit the submission to the configured State reporting authority.; AC 3 Given required NIBRS/UCR elements are missing or invalid, When the user attempts submission, Then the solution shall identify the missing or invalid information and prevent submission.; AC 4 Given a submission is accepted, When the reporting authority returns acceptance, Then the solution shall record the submission outcome.; AC 5 Given a submission is rejected, When the reporting authority returns an error, Then the solution shall record the error and submission status.		
7858	NIBRS Validation and Correction	As a Dispatcher, I want to validate NIBRS records, identify errors, correct authorized errors, and revalidate records, so that compliant data can be submitted.	AC 1 Given a NIBRS record is prepared for submission, When the solution validates the record, Then the solution shall identify errors.; AC 2 Given a NIBRS record contains an invalid value, When validation occurs, Then the solution shall identify the affected data element.; AC 3 Given an Authorized User corrects a NIBRS validation error, When the correction is saved, Then the solution shall update the record.; AC 4 Given NIBRS errors have been corrected, When the user revalidates the record, Then the solution shall return the current validation status.; AC 5 Given the NIBRS record passes validation, When the user prepares the submission, Then the solution shall identify the record as eligible for submission according to configured rules.;		
7859	VIBRS Data Submission	As a Dispatcher, I need to prepare and submit crime incident data in accordance with Vermont's VIBRS-specific reporting requirements, so that Vermont crime data is complete, accurate, and submitted in accordance with configured State reporting procedures.	AC 1 Given Vermont crime records contain required VIBRS information, When an authorized dispatcher prepares VIBRS data, Then the solution shall generate the Vermont reporting structure.; AC 2 Given VIBRS data contains required information, When the dispatcher validates the data, Then the solution shall identify validation results.; AC 3 Given VIBRS data passes validation, When the dispatcher submits the data, Then the solution shall transmit the submission through the configured reporting process.; AC 4 Given a VIBRS submission fails, When the failure is returned, Then the solution shall record the failure and available error information.; AC 5 Given a VIBRS submission is accepted, When the acceptance is returned, Then the solution shall record the submission outcome.;		
7868	Configurable Ad-Hoc Queries	As a Dispatcher, I want the solution to create and run ad-hoc queries using configurable data fields and search criteria with date and geographic ranges and user-defined fields, so that I can retrieve associated historical incident information in accordance with system configuration and local SOP without relying on vendor-developed reports.	AC 1 Given a dispatcher has authorized access to CAD/RMS data, When the dispatcher creates an ad-hoc query using supported data fields, Then the solution shall allow the query to be saved or executed.; AC 2 Given an ad-hoc query includes a date range, When the dispatcher executes the query, Then the solution shall return records within the selected date range.; AC 3 Given an ad-hoc query includes a geographic range, When the dispatcher executes the query, Then the solution shall return records within the configured geographic criteria.; AC 4 Given an ad-hoc query includes user-defined fields, When the dispatcher executes the query, Then the solution shall apply the configured user-defined criteria.; AC 5 Given an ad-hoc query is valid, When the dispatcher executes the query, Then the solution shall return results without requiring vendor-developed report changes.; AC 6 Given a dispatcher saves an approved query, When the query is saved, Then the solution shall retain the configured search criteria for future use.;		
7869	Data Quality Monitoring	As a Dispatcher, I want to monitor defined data-quality measures and identify records requiring correction, so that ongoing data-quality problems can be detected and addressed.	AC 1 Given data-quality measures have been configured, When the solution evaluates records, Then the solution shall calculate or identify the defined measures.; AC 2 Given records fail a defined quality measure, When the quality results are generated, Then the solution shall identify the affected records.; AC 3 Given a record has been identified for correction, When an Authorized User reviews the record, Then the solution shall display the data-quality issue.; AC 4 Given a data-quality issue has been corrected, When the record is reevaluated, Then the solution shall update the quality result.; AC 5 Given multiple data-quality issues exist, When the quality results are reviewed, Then the solution shall identify each issue according to configured rules.;		
7870	Data Analysis	As a Dispatcher, I want to analyze approved datasets using defined criteria and analytical outputs, so that operational and management questions can be answered using CAD/RMS data.	AC 1 Given an authorized dispatcher has access to an approved dataset, When the dispatcher applies defined analytical criteria, Then the solution shall generate the analytical output.; AC 2 Given an analytical query contains multiple criteria, When the analysis is executed, Then the solution shall apply the configured criteria.; AC 3 Given analytical results are generated, When the dispatcher reviews the results, Then the solution shall display the calculated or summarized information.; AC 4 Given an authorized analytical output is generated, When the dispatcher saves or exports it through a supported function, Then the solution shall make the output available according to configured permissions.; AC 5 Given no records satisfy the analytical criteria, When the analysis is executed, Then the solution shall indicate that no matching data was found.;		
7871	Query Result Export	As a Dispatcher, I want to export query results in supported formats, so that approved data can be shared or further analyzed.	AC 1 Given a dispatcher has generated query results, When the dispatcher selects a supported export format, Then the solution shall generate an export in the selected format.; AC 2 Given query results contain authorized records, When the export is generated, Then the exported file shall contain the authorized results.; AC 3 Given query results contain restricted information, When the dispatcher exports the results, Then the solution shall apply the configured access restrictions.; AC 4 Given an export is generated, When the dispatcher accesses the exported file, Then the file shall be available through the supported download or file-access mechanism.; AC 5 Given an unsupported export format is selected, When the dispatcher attempts the export, Then the solution shall prevent the unsupported export.; AC 6 Given an unsupported export format is selected, When the dispatcher attempts the export, Then the solution shall identify the supported formats.;		

7872	Performance Dashboards	As a Supervisor, I want the solution to provide dashboards displaying approved performance measures for defined reporting periods, so that I can monitor operational performance and identify trends over time.	AC 1 Given approved performance measures and a reporting period are configured, When a supervisor opens the dashboard, Then the solution shall display the approved measures for the selected period.; AC 2 Given dashboard data exists for multiple reporting periods, When the supervisor changes the reporting period, Then the dashboard shall display the measures for the selected period.; AC 3 Given a measure has supporting detail, When the supervisor selects the measure, Then the solution shall display the supporting information.; AC 4 Given no data is available for a selected reporting period, When the dashboard loads, Then the solution shall indicate that no data is available.; AC 5 Given dashboard data is refreshed, When updated source information is available, Then the dashboard shall display the updated results according to the configured refresh process.;		
7873	Operational and Compliance Dashboards	As a Supervisor, I want the solution to provide dashboards displaying approved operational, performance, and compliance measures, so that I can monitor service performance, operational activity, and compliance.	AC 1 Given approved operational measures are configured, When a supervisor accesses the dashboard, Then the solution shall display the operational measures.; AC 2 Given approved performance measures are configured, When a supervisor accesses the dashboard, Then the solution shall display the performance measures.; AC 3 Given approved compliance measures are configured, When a supervisor accesses the dashboard, Then the solution shall display the compliance measures.; AC 4 Given a supervisor selects a reporting period, When the dashboard refreshes, Then the solution shall display results for the selected period.; AC 5 Given a displayed measure has supporting information, When the supervisor selects the measure, Then the solution shall display the configured supporting details.;		
7874	Operational Performance Reporting	As a Dispatcher, I want to run operational performance reports using approved measures and reporting periods, so that operational performance can be evaluated.	AC 1 Given approved operational performance measures are available, When a dispatcher selects a reporting period, Then the solution shall generate the performance report.; AC 2 Given the selected reporting period contains operational data, When the report executes, Then the solution shall include the results.; AC 3 Given no operational data exists, When the report executes, Then the solution shall indicate that no results are available.; AC 4 Given the report is generated, When an authorized dispatcher reviews the report, Then the report shall display the configured measures and reporting period.; AC 5 Given an authorized dispatcher exports the report, When the export is requested, Then the solution shall generate the report in the supported selected format.;		
7875	Standard Reports	As a Dispatcher, I want to run standard reports provided with the solution, so that I can access needed information without vendor assistance.	AC 1 Given a standard report is available in the solution, When an authorized dispatcher selects the report, Then the solution shall execute the report.; AC 2 Given a standard report requires parameters, When the dispatcher enters the required parameters, Then the solution shall validate the parameters before execution.; AC 3 Given the standard report executes successfully, When the results are returned, Then the solution shall display the configured report information.; AC 4 Given a standard report cannot execute, When the failure occurs, Then the solution shall identify the error.; AC 5 Given a standard report supports export, When the dispatcher selects a supported export format, Then the solution shall generate the report in the selected format.;		
7876	Report Scheduling and Configuration	As a Dispatcher, I want to configure approved report schedules, filters, and access controls, so that reporting can be maintained without unnecessary vendor intervention.	AC 1 Given a dispatcher has authorization to configure a report, When the dispatcher sets supported report filters, Then the solution shall save the configured filters.; AC 2 Given a dispatcher configures a report schedule, When the schedule is saved, Then the solution shall retain the configured schedule.; AC 3 Given access controls are configured for a report, When the settings are saved, Then the solution shall apply the configured access controls.; AC 4 Given a report has a configured schedule, When the scheduled execution time occurs, Then the solution shall execute the report according to the saved configuration.; AC 5 Given a dispatcher changes an approved report schedule, When the change is saved, Then subsequent executions shall use the updated schedule.;		
7877	Report Filtering	As a Dispatcher, I want to apply supported filters to reports, so that I can focus results on the information relevant to my analysis.	AC 1 Given a report supports filtering by date, When a dispatcher selects a date range, Then the solution shall limit the report results to the selected period.; AC 2 Given a report supports filtering by location, When a dispatcher selects a supported location criterion, Then the solution shall limit the report results according to the criterion.; AC 3 Given a report supports filtering by incident type, When the dispatcher selects an incident type, Then the solution shall limit the results accordingly.; AC 4 Given multiple supported filters are applied, When the dispatcher executes the report, Then the solution shall apply all selected filters according to configured rules.; AC 5 Given filters return no matching records, When the report executes, Then the solution shall indicate that no records match the selected criteria.;		
7878	Report Validation	As a Dispatcher, I want to review and validate report results before operational use, so that reporting outputs are accurate and reliable.	AC 1 Given a report has been generated, When a dispatcher reviews the report results, Then the solution shall display the configured report data.; AC 2 Given a report contains source information that can be reviewed, When the dispatcher validates the results, Then the dispatcher shall be able to access the supporting information.; AC 3 Given a report contains an apparent discrepancy, When the dispatcher investigates the result, Then the solution shall provide the information required to identify the affected record or data element.; AC 4 Given report results have been validated, When the dispatcher completes the review, Then the report shall remain available for operational use according to configured permissions.; AC 5 Given the report cannot be validated because required source information is unavailable, When the dispatcher reviews the report, Then the solution shall identify the unavailable information according to configured rules.;		
7879	Configurable Report and Data Views	As an Authorized User, I want the solution to provide configurable summary and detailed views of reports, incidents, and resource information with the ability to drill down from summary data to supporting details and configure the displayed data and presentation, so that information can be reviewed and presented according to operational needs. The RMS also needs to assemble the reports into professional final report formatting.	AC 1 Given an Authorized User accesses report, incident, or resource information, When the user selects a summary view, Then the solution shall display the configured summary information.; AC 2 Given an Authorized User selects a detailed view, When the view loads, Then the solution shall display the configured detailed information.; AC 3 Given summary information has supporting detail, When the user selects a supported drill-down function, Then the solution shall display the associated detail.; AC 4 Given an Authorized User changes supported display settings, When the settings are saved, Then the solution shall display the configured information according to those settings.; AC 5 Given a user is not authorized to access supporting detail, When the user selects the drill-down function, Then the solution shall restrict access to the unauthorized information.; AC 6 Given report or incident information changes, When the user refreshes the view, Then the solution shall display the current authorized information.;		

7880	Saved Searches and Queries	As a Dispatcher, I want to save approved search criteria and ad-hoc queries for future use, so that used searches can be run again without rebuilding them.	AC 1 Given a dispatcher has created a valid ad-hoc query, When the dispatcher selects the save function, Then the solution shall retain the query criteria.; AC 2 Given a saved query has a user-defined name, When the query is saved, Then the solution shall retain the name with the query.; AC 3 Given a saved query exists, When the dispatcher selects the query, Then the solution shall load the saved criteria.; AC 4 Given a saved query is executed, When the dispatcher runs it, Then the solution shall return results using the saved criteria.; AC 5 Given an authorized dispatcher updates a saved query, When the changes are saved, Then the solution shall retain the updated criteria.; AC 6 Given a saved query is deleted by an Authorized User, When the deletion is confirmed, Then the solution shall remove the query from the user's available saved searches according to configured rules.;		
7881	External Report Submission Status	As a Dispatcher, I want to view the status and errors of external report submissions, so that I can correct failed submissions and confirm successful submissions.	AC 1 Given an external report has been submitted, When the external system returns a status, Then the solution shall record the submission status.; AC 2 Given an external report submission succeeds, When the success response is received, Then the solution shall identify the submission as successful.; AC 3 Given an external report submission fails, When the failure response is received, Then the solution shall identify the submission as failed.; AC 4 Given an external report submission contains an error, When the dispatcher views the submission status, Then the solution shall display the available error information.; AC 5 Given a failed submission is corrected, When the dispatcher resubmits the report, Then the solution shall create or update the submission status according to configured rules.;		
7892	Shift Summary	As a Supervisor, I want to generate a shift summary that consolidates personnel, resources, incidents, and significant activity for a defined shift, so that I can conduct roll call and brief incoming personnel.	AC 1 Given personnel, resources, incidents, and significant activity that meets the configured significance criteria have been recorded for a shift, When a Supervisor generates a shift summary for the defined shift, Then the solution shall consolidate the information into a shift summary.; AC 2 Given a defined shift has a start and end time, When the Supervisor generates the shift summary, Then the solution shall include activity occurring within the defined shift period.; AC 3 Given the shift summary has been generated, When the Supervisor views the summary, Then the solution shall present personnel, resources, incidents, and significant activity that meets the configured significance criteria in a format suitable for roll call and briefing.;		
7893	Call Statistics	As a Supervisor, I want to generate call statistics for defined periods and call types, so that I can monitor call volume, workload, and communications center performance.	AC 1 Given call records exist for a defined reporting period, When a Supervisor generates call statistics, Then the solution shall calculate statistics for the specified period.; AC 2 Given call types are available in the call records, When the Supervisor filters the statistics by call type, Then the solution shall include only records matching the selected call types.; AC 3 Given call statistics have been generated, When the Supervisor views the results, Then the solution shall present information that supports analysis of call volume, workload, and communications center performance.;		
7894	Traffic Stop Reporting and Analysis	As a Supervisor, I want to generate, filter, and analyze traffic-stop reports using approved traffic-stop, disposition, and demographic data with race, based on authorized reporting and analysis dimensions, so that traffic-stop activity can be reviewed, monitored, and reported in accordance with defined requirements.	AC 1 Given approved traffic-stop records contain authorized reporting data, When a Supervisor or authorized Analyst generates a traffic-stop report, Then the solution shall include data from the approved traffic-stop records.; AC 2 Given authorized reporting dimensions are available, When the user applies filters or analysis dimensions, Then the solution shall return results based on the selected dimensions.; AC 3 Given demographic data with race, is authorized for reporting, When the user selects an approved demographic dimension, Then the solution shall include the demographic information in the results.; AC 4 Given a traffic-stop report has been generated, When the user applies a disposition filter, Then the solution shall limit the results to the selected dispositions.; AC 5 Given the user is not authorized to access a reporting dimension, When the user attempts to use that dimension, Then the solution shall prevent access to the unauthorized data.;		
7953	Solution Snapshot and Event Replay	As a Supervisor, I want to generate a point-in-time solution snapshot and replay eligible incident activity, so that I can review historical solution state and operational events.	AC 1 Given eligible incident activity has occurred, When an authorized Supervisor requests a point-in-time snapshot, Then the solution shall generate a snapshot representing the system or incident state.; AC 2 Given eligible incident activity is available for replay, When the Supervisor selects a historical period, Then the solution shall replay the eligible activity in chronological sequence.; AC 3 Given the Supervisor selects a specific point in time, When the snapshot is displayed, Then the solution shall present the eligible information to that point in time.;		
7970	Records Disposition and Audit	As a System Administrator, I want the solution to execute authorized records-disposition actions and retain the associated authorization and audit history, so that records are disposed of only when permitted and the disposition activity can be reviewed.	AC 1 Given a record meets the configured criteria for disposition, When an authorized Agency Administrator initiates disposition, Then the solution shall validate the authorization and disposition requirements.; AC 2 Given disposition is authorized, When the action is completed, Then the solution shall execute the approved disposition action.; AC 3 Given a disposition action is completed, When the disposition history is reviewed, Then the solution shall retain the authorization and audit information.; AC 4 Given disposition is not authorized, When the user attempts the action, Then the solution shall prevent the disposition.;		
8006	Response-Time Compliance Metrics	As a Supervisor, I want to view turnout and response-time compliance metrics using configured thresholds and authorized organizational dimensions, so that operational performance can be monitored against established service-level measures.	AC 1 Given configured thresholds and authorized organizational dimensions, When a supervisor views compliance metrics, Then the solution shall display turnout and response-time compliance against the configured thresholds; AC 2 Given a supervisor selects an authorized organizational dimension, When the metrics are displayed, Then the solution shall present compliance results filtered by the selected dimension; AC 3 Given a user lacks permission for a requested dimension, When the user attempts to view it, Then the solution shall prevent access to that dimension's metrics; AC 4 Given compliance metrics are displayed, When presented to the supervisor, Then the solution shall express response-time measures in HH:MM:SS format; AC 5 Given underlying incident data changes, When the supervisor refreshes the metrics, Then the solution shall recalculate compliance using current data;		
8007	Response-Time Report Scheduling	As a Supervisor, I want to schedule recurring reports containing turnout and response-time metrics in HH:MM:SS format, so that leadership receives consistent performance summaries at defined intervals.	AC 1 Given a supervisor or authorized analyst defines a recurring report containing turnout and response-time metrics, When the report schedule is saved, Then the solution shall persist the recurring report schedule; AC 2 Given a recurring report is scheduled, When the scheduled interval is reached, Then the solution shall generate and distribute the report to the defined recipients; AC 3 Given the report contains response-time metrics, When the report is generated, Then the solution shall present the metrics in HH:MM:SS format; AC 4 Given a user lacks permission to schedule reports, When the user attempts to create a schedule, Then the solution shall prevent the action; AC 5 Given a scheduled report fails to generate or distribute, When the failure occurs, Then the solution shall record the failure for administrator review;		

8008	Timestamp Correction and Audit	As a System Administrator, I want a controlled process to correct dispatch, enroute, or arrival timestamps and retain the original values, reason, user, and time of the correction, so that calculated durations remain accurate and the changes remain auditable.	AC 1 Given an authorized user is permitted to correct timestamps, When the user corrects a dispatch, enroute, or arrival timestamp, Then the solution shall apply the corrected value.; AC 2 Given a timestamp is corrected, When the change is saved, Then the solution shall retain the original value, reason, user, and time of the correction.; AC 3 Given a timestamp is corrected, When calculated durations depend on it, Then the solution shall recalculate the affected durations using the corrected value.AC 4 Given a user is not authorized to correct timestamps, When the user attempts a correction, Then the solution shall prevent the change.; AC 5 Given an authorized user reviews a corrected timestamp, When the review occurs, Then the solution shall make the correction history available.		
8010	Incident Duration Recalculation	As a System Administrator, I want incident-duration metrics to recalculate when unit timestamps are reassigned to another incident, so that affected incidents have accurate metrics and an auditable record of the change.	AC 1 Given a unit timestamp is reassigned from one incident to another, When the reassignment is saved, Then the solution shall recalculate the incident-duration metrics for each affected incident; AC 2 Given incident-duration metrics are recalculated, When the recalculation completes, Then the solution shall update the affected incidents with the recalculated metrics; AC 3 Given a timestamp reassignment changes incident-duration metrics, When the metrics are recalculated, Then the solution shall retain an auditable record of the change; AC 4 Given a timestamp reassignment is invalid, When the reassignment is attempted, Then the solution shall prevent the recalculation; AC 5 Given a timestamp reassignment is invalid, When the reassignment is attempted, Then the solution shall notify the user of the invalid reassignment; AC 6 Given recalculated incident-duration metrics exist, When an Authorized User reviews an affected incident, Then the solution shall display the recalculated metrics;		
8049	Agency Usage and Cost-Sharing Reports	As a Program Administrator, I want reports showing system usage by agency, so that cost-sharing can be based on actual usage.	AC 1 Given system usage data is recorded by agency, When a program administrator generates a usage report, Then the solution shall report system usage by agency; AC 2 Given a usage report is generated, When it is produced, Then the solution shall express usage in a manner that supports cost-sharing based on actual usage; AC 3 Given a reporting period is specified, When the report is generated, Then the solution shall report usage for the specified period; AC 4 Given a user lacks permission to view usage reports, When the user attempts access, Then the solution shall prevent access; AC 5 Given usage data changes, When the report is regenerated, Then the solution shall reflect the current usage;		
8106	Agency Report Requirement Determination	As a Dispatcher, I need the solution to be able to determine, based upon incident type or disposition, whether an agency report is required, so that the capability is available in accordance with approved operational requirements.	AC 1 Given incident type and disposition values, When the solution evaluates whether an agency report is required, Then the solution shall determine, based on incident type or disposition, whether an agency report is required; AC 2 Given a configured rule indicates a report is required, When the event meets the rule, Then the solution shall indicate that an agency report is required; AC 3 Given a configured rule indicates a report is not required, When the event meets the rule, Then the solution shall make the agency report optional for that event.; AC 4 Given report-requirement rules are configured, When an Authorized User changes them, Then the solution shall apply the updated rules to subsequent events;		
8142	Specialty Personnel Assignment Reporting	As a Dispatcher, I want to generate a report that lists the personnel assigned to a specified specialty code, so that I can view, manage, and update personnel assignments associated with specific specialty functions.	AC 1 Given personnel are assigned specialty codes limited to Search and Rescue, When a dispatcher generates a report for a specified specialty code, Then the solution shall list the personnel assigned to that specialty code; AC 2 Given the specialty personnel report is generated, When it is displayed, Then the solution shall allow the user to view and manage the listed assignments; AC 3 Given a personnel specialty assignment is updated, When the change is saved, Then the solution shall reflect the updated assignment in subsequent reports; AC 4 Given no personnel are assigned to a specified specialty code, When the report is generated, Then the solution shall indicate that no personnel are assigned to that code;		
8143	Alarm and Rotation Records	As a Records Clerk, I want to access and report on alarms tables, record rotations, and historical data, so that accurate records management and operational tracking are maintained.	AC 1 Given alarms tables, record rotations, and historical data, When a records clerk accesses them, Then the solution shall provide access to the alarms tables, record rotations, and historical data; AC 2 Given a records clerk generates a report on this data, When the report is produced, Then the solution shall report on the alarms tables, record rotations, and historical data; AC 3 Given a user lacks permission to access or report on this data, When the user attempts access, Then the solution shall prevent it; AC 4 Given the underlying data changes, When a report is regenerated, Then the solution shall reflect the current data;		
8144	Records Retention Alerts	As a Records Manager, I want the solution to alert me when specified case or person records reach legal retention limits, so that our agency can handle expungements, sealing, or record disposals in compliance with state regulations.	AC 1 Given legal retention limits are configured for case or person records, When a specified record reaches its retention limit, Then the solution shall alert the records manager; AC 2 Given a retention alert is generated, When the records manager reviews it, Then the solution shall identify the records that have reached the retention limit; AC 3 Given a record is handled for expungement, sealing, or disposal, When the action is taken, Then the solution shall record the action for compliance purposes; AC 4 Given retention limits are configured by state regulations, When an Authorized User changes them, Then the solution shall apply the updated retention limits; AC 5 Given a user lacks permission to manage retention actions, When the user attempts the action, Then the solution shall prevent it;		
8151	Reopened CAD Event Data Integrity	As a System Administrator, I want the solution to restrict, based on agency policy, the modification or deletion of previously entered data in reopened closed CAD events, so that the integrity and historical record of CAD event information are preserved.	AC 1 Given agency policy restricts modification or deletion of previously entered data in reopened closed CAD events, When a user attempts to modify or delete such data, Then the solution shall restrict the action in accordance with agency policy; AC 2 Given a reopened closed event is updated within policy, When permitted changes are made, Then the solution shall preserve the integrity and historical record of the event information; AC 3 Given a user lacks the rights to modify data in a reopened closed event, When the user attempts it, Then the solution shall prevent the action; AC 4 Given a permitted change is made in a reopened closed event, When it is saved, Then the solution shall record the change in the event history with the user and time; AC 5 Given the restriction policy is configured, When an Authorized User changes it, Then the solution shall apply the updated restriction to subsequent reopened events;		
8206	Selective Case Document Printing and Export	As an Authorized User, I want the solution to allow me to select specific notes, reports, pages, attachments, or other case content for printing or export, so that I can produce only the records required for a records request, operational purpose, or other authorized use without exporting the entire case file.	AC 1 Given case content with notes, reports, pages, attachments, or other items, When an Authorized User selects specific content for printing or export, Then the solution shall produce only the selected records; AC 2 Given specific case content is selected, When the user exports or prints it, Then the solution shall exclude content that was not selected; AC 3 Given a user lacks permission to print or export selected case content, When the user attempts it, Then the solution shall prevent the action; AC 4 Given selected content is printed or exported, When the action occurs, Then the solution shall record the action for audit purposes; AC 5 Given no content is selected, When the user attempts to print or export, Then the solution shall indicate that no content has been selected;		

8207	Report-Level Review, Approval and Locking	As a Case Supervisor, I want the solution to review and approve individual reports within a case and lock approved reports from unauthorized modification, while recording any authorized post-approval changes, so that case reports are reviewed, their approval status is visible, and changes after approval are controlled and auditable.	AC 1 Given a case with individual reports, When a case supervisor reviews and approves a report, Then the solution shall record the report's approval status; AC 2 Given a report is approved, When the approval is applied, Then the solution shall lock the approved report from unauthorized modification; AC 3 Given an authorized post-approval change is made, When the change occurs, Then the solution shall record the change while retaining the approval history; AC 4 Given a user lacks permission to approve or modify approved reports, When the user attempts it, Then the solution shall prevent the action; AC 5 Given approved and unapproved reports exist in a case, When a user views the case, Then the solution shall make each report's approval status visible; AC 6 Given a post-approval change is recorded, When an Authorized User reviews the report, Then the solution shall present the change as auditable;		
8208	Discovery Package Management and Numbering	As an Authorized User, I want the solution to organize discovery submissions, assign unique identifiers to individual documents and files within each submission, and generate a corresponding discovery list when content is printed or exported, so that discovery packages can be assembled, tracked, and provided to authorized recipients.	AC 1 Given discovery submissions, When an Authorized User organizes a submission, Then the solution shall organize the discovery submission; AC 2 Given discovery submissions, When an Authorized User organizes a submission, Then the solution shall assign unique identifiers to individual documents and files within it; AC 3 Given discovery content is printed or exported, When the output is produced, Then the solution shall generate a corresponding discovery list; AC 4 Given discovery submissions are assembled, When they are tracked, Then the solution shall allow the submissions to be tracked and provided to authorized recipients; AC 5 Given a user lacks permission to organize or export discovery, When the user attempts it, Then the solution shall prevent the action; AC 6 Given a discovery submission is produced, When it is generated, Then the solution shall record the production for audit purposes;		
8762	Enter and Maintain NIBRS/UCR Crime Data	As a Law Enforcement Officer, I want to enter and maintain crime incident data required by FBI NIBRS specifications and Vermont UCR reporting requirements, so that crime data is complete and compliant.	AC 1 Given an authorized law enforcement user needs to report a crime incident, When the user prepares the incident data, Then the solution shall support entry and maintenance of the information required by FBI NIBRS specifications and Vermont UCR reporting requirements.; AC 2 Given crime incident data is being entered, When a required NIBRS or Vermont UCR data element is missing or invalid, Then the solution shall identify the missing or invalid data element before the record is finalized.; AC 3 Given a crime incident record has been entered, When an authorized user updates the record, Then the solution shall save the changes.; AC 4 Given a crime incident record has been entered, When an authorized user updates the record, Then the solution shall retain the prior values in accordance with configured audit requirements.;		
8763	Validate NIBRS/UCR Crime Data	As a Law Enforcement Officer, I want the solution to validate crime incident data against NIBRS and Vermont UCR rules, so that errors are identified before submission.	AC 1 Given crime incident data is entered or updated, When the solution validates the data, Then the solution shall identify missing, invalid, or inconsistent information according to FBI NIBRS specifications and Vermont UCR reporting requirements.; AC 2 Given a crime incident contains information required for NIBRS or Vermont UCR reporting, When the user prepares the incident for submission, Then the solution shall validate the required data elements and reporting rules before submission.; AC 3 Given crime incident data fails a validation rule, When the user attempts to submit the data, Then the solution shall identify the validation errors.; AC 4 Given crime incident data fails a validation rule, When the user attempts to submit the data, Then the solution shall provide the information needed for the user to correct them.;		
8764	Submit NIBRS/UCR Crime Data	As a Law Enforcement Officer, I want to submit validated crime incident data in the approved reporting format, so that reporting is completed and tracked.	AC 1 Given crime incident data meets reporting requirements, When an authorized user submits the data, Then the solution shall prepare and transmit the data using the approved reporting format and submission process.; AC 2 Given crime incident data is submitted, When the submission is processed, Then the solution shall record the submission status.; AC 3 Given crime incident data is submitted, When the submission is processed, Then the solution shall retain the confirmation or rejection information for traceability.;		
8765	Handle NIBRS/UCR Rejections and Corrections	As a Law Enforcement Officer, I want rejected or returned submissions surfaced for correction, so that reporting errors are resolved.	AC 1 Given submitted crime incident data is rejected or returned for correction, When the rejection or correction request is received, Then the solution shall make the errors or feedback available to an authorized user for review and correction.; AC 2 Given a rejected submission has been corrected, When an authorized user resubmits the data, Then the solution shall submit the corrected data.; AC 3 Given a rejected submission has been corrected, When an authorized user resubmits the data, Then the solution shall update the submission status.; AC 4 Given a submission has been rejected or returned, When an authorized user reviews the submission, Then the solution shall display the rejection reason and current correction status.;		
8766	Retain NIBRS/UCR Reporting History	As a Law Enforcement Officer, I want reporting data and submission history retained, so that records remain auditable.	AC 1 Given crime incident data is prepared or submitted for NIBRS or Vermont UCR reporting, When an authorized user reviews the reporting record, Then the solution shall retain the incident data and submission history in accordance with configured retention and audit requirements.; AC 2 Given reporting data and submission history are retained, When an authorized user searches the reporting history, Then the solution shall retrieve the matching records and their submission history.; AC 3 Given a retention period is configured, When retained reporting records reach the end of the retention period, Then the solution shall apply the configured retention disposition.;		
8828	DPS Data Lake and Enterprise BI Export	As a Data Analyst, I want the solution to export authorized data to the DPS data lake and statewide business-intelligence (BI) environment, so that incident and operational data is available for enterprise reporting and analytics.	AC 1 Given the solution is configured for data export, When the scheduled or on-demand export runs, Then the solution shall transmit the configured data to the DPS data lake.; AC 2 Given data is exported to the data lake, When the export completes, Then the solution shall record the export status.; AC 3 Given data is exported to the data lake, When the export completes, Then the solution shall record counts.; AC 4 Given an export fails or is incomplete, When the failure is detected, Then the solution shall notify the administrator.; AC 5 Given an export fails or is incomplete, When the failure is detected, Then the solution shall support retry or recovery.; AC 6 Given data is exported for business intelligence, When the data is transmitted, Then the solution shall restrict and protect the data according to role and security requirements.; AC 7 Given an export transaction occurs, When the transaction completes, Then the solution shall log the export for audit.;		

8829	Expungement Order Intake and Authorization	As a Records Manager, I want to intake and validate an expungement order and authorize its scope before any record is expunged, so that only lawfully ordered records are expunged and the authorization is documented.	AC 1 Given an expungement order is received, When the order is entered, Then the solution shall create an expungement request.; AC 2 Given an expungement order is received, When the order is entered, Then the solution shall capture the order source, authority, and effective date.; AC 3 Given an expungement request is created, When the records are identified, Then the solution shall associate the specific case, person, or records within the expungement scope.; AC 4 Given an expungement request is pending, When the required authorization is applied, Then the solution shall verify the user's authority.; AC 5 Given an expungement request is pending, When the required authorization is applied, Then the solution shall prevent execution until authorization is complete.; AC 6 Given a record is subject to an active legal hold, When an expungement is requested, Then the solution shall prevent the expungement.; AC 7 Given a record is subject to an active legal hold, When an expungement is requested, Then the solution shall notify the user of the conflict.; AC 8 Given an expungement request is authorized, When the authorization is recorded, Then the solution shall retain the authorizing user, order reference, and date/time.; AC 9 Given a user lacks permission to authorize expungements, When the user attempts the action, Then the solution shall prevent it.; AC 10 Given a user lacks permission to authorize expungements, When the user attempts the action, Then the solution shall log the attempt.;		
8830	Record Expungement Execution	As a Records Manager, I want the solution to execute an authorized expungement in the configured outcome mode, so that the ordered records are irreversibly expunged as either full data destruction or de-identified statistics-only retention.	AC 1 Given an expungement is authorized and configured for full destruction, When the expungement is executed, Then the solution shall permanently and irreversibly remove the record and all associated identifiable data, including narratives, attachments, images, and linked records.; AC 2 Given an expungement is authorized and configured for statistics-only retention, When the expungement is executed, Then the solution shall remove all identifiable data while retaining only de-identified aggregate statistical data required for mandated reporting.; AC 3 Given an expungement has been executed, When an authorized or unauthorized user searches for the record, Then the solution shall ensure the expunged identifiable data is not retrievable or viewable.; AC 4 Given an expungement is executed, When the action completes, Then the solution shall prevent reversal or restoration of the expunged identifiable data.; AC 5 Given an expungement execution fails or is incomplete, When the failure is detected, Then the solution shall halt the action, preserve the record's prior state.; AC 6 Given an expungement execution fails or is incomplete, When the failure is detected, Then the solution shall notify the records manager.; AC 7 Given an expungement is executed, When the action completes, Then the solution shall retain a non-identifiable audit entry recording the expungement, outcome mode, authority, and date/time.;		
8831	Expungement Propagation and Certification	As a Records Manager, I want the solution to propagate an executed expungement to integrated and downstream systems and produce a compliance certification, so that expunged data is consistently removed everywhere and the agency can demonstrate compliance.	AC 1 Given a record has been expunged, When reporting or statistics are generated, Then the solution shall exclude the expunged record's identifiable data and reflect only de-identified aggregate values where statistics-only retention is configured.; AC 2 Given a record has been expunged, When data is shared with integrated or interfaced systems, Then the solution shall transmit or record the expungement so that identifiable data is removed or flagged in those systems according to configuration.; AC 3 Given an expungement is completed, When certification is requested, Then the solution shall generate a compliance certificate identifying the order, scope, outcome mode, and completion date without exposing the expunged identifiable data.; AC 4 Given an expungement propagation to a downstream system fails, When the failure is detected, Then the solution shall notify the administrator.; AC 5 Given an expungement propagation to a downstream system fails, When the failure is detected, Then the solution shall support retry or manual reconciliation.; AC 6 Given an expungement certification or propagation occurs, When the transaction completes, Then the solution shall log the activity for audit using non-identifiable references.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 07: Interoperability, Interfaces & Standards					
7810	Mutual Aid Coordination	As a Mutual Aid User, I want to coordinate mutual-aid requests, assignments, and status with participating agencies, so that external resources can be requested and managed.	AC 1 Given an incident requires mutual aid, When an Authorized User creates a mutual-aid request, Then the solution shall record the requesting agency and incident.; AC 2 Given a mutual-aid request identifies a participating agency, When the request is submitted, Then the solution shall transmit the request through the configured supported process.; AC 3 Given an external agency accepts the mutual-aid request, When the acceptance is received, Then the solution shall record the participating agency and request status.; AC 4 Given mutual-aid resources are assigned, When the assignment is recorded, Then the solution shall associate the resources with the incident.; AC 5 Given mutual-aid resource status changes, When the status update is received or entered, Then the solution shall update the resource status and mutual-aid request.;		
7821	CAD-to-RMS Data Population	As an Investigator, I want CAD information to populate the corresponding RMS records, regardless of whether the RMS vendor differs from the CAD vendor, and maintain the required relationships between records, so that dispatch information is available within RMS to support accurate records management and retrieval.	AC 1 Given a CAD incident contains information configured for RMS population, When the CAD-to-RMS process executes, Then the RMS shall populate the record.; AC 2 Given an RMS record is populated from CAD, When the record is created, Then the solution shall maintain the relationship to the originating CAD incident.; AC 3 Given CAD information is updated before RMS completion, When the configured synchronization occurs, Then the RMS record shall reflect the updated information.; AC 4 Given required information cannot be transferred, When the population process fails, Then the solution shall identify the failure for authorized users.; AC 5 Given an RMS record has been populated from CAD, When an investigator views the record, Then the originating CAD information shall be traceable according to configured rules.;		
7826	Incident Communications History	As a Dispatcher, I want to retain and view communications associated with an incident or case, so that authorized users can access the communication history to support incident management, review, and documentation.	AC 1 Given communications are associated with an incident or case, When an Authorized User accesses the record, Then the user shall be able to view the communication history.; AC 2 Given a new supported communication is received, When the communication is associated with an incident, Then the solution shall retain the communication with the incident.; AC 3 Given multiple communications are associated with an incident, When the communication history is viewed, Then the solution shall display the communications according to configured chronological or other supported ordering.; AC 4 Given a communication contains restricted information, When an unauthorized user accesses the history, Then the solution shall restrict the communication according to configured rules.; AC 5 Given communication information is unavailable, When an Authorized User views the incident, Then the solution shall indicate that no communication is available.;		

7882	AHS/988 and Mobile Crisis Data Exchange	As a Dispatcher, I want the solution to exchange defined information with AHS/988 and mobile crisis services, so that authorized crisis-response coordination can occur.	AC 1 Given an authorized crisis-response exchange is required, When the solution sends information to AHS/988 or an approved mobile crisis service, Then the solution shall transmit the configured information.; AC 2 Given an authorized crisis-response service sends information to CAD/RMS, When the information is received, Then the solution shall associate the information with the incident.; AC 3 Given a crisis-response exchange fails, When the failure is detected, Then the solution shall record the failure.; AC 4 Given a crisis-response exchange fails, When the failure is detected, Then the solution shall notify the authorized user according to configured rules.; AC 5 Given crisis-response information is received, When an Authorized User views the incident, Then the exchanged information shall be available.; AC 6 Given crisis-response information is restricted, When an unauthorized user accesses the incident, Then the solution shall prevent access to the restricted information.;		
7883	CarFax Vehicle History	As an Officer, I want the solution to retrieve authorized vehicle-history information from CarFax or an approved provider, so that vehicle history can support investigations and enforcement activities.	AC 1 Given an officer is authorized to request vehicle history, When the officer enters an approved vehicle identifier, Then the solution shall submit the inquiry to CarFax or another approved provider.; AC 2 Given the provider returns matching vehicle-history information, When the response is received, Then the solution shall display the authorized vehicle history.; AC 3 Given no matching vehicle history is returned, When the response is received, Then the solution shall indicate that no matching information was found.; AC 4 Given the vehicle-history provider is unavailable, When the officer submits the inquiry, Then the solution shall identify the unavailable service according to configured rules.; AC 5 Given an officer is not authorized to retrieve vehicle history, When the officer attempts the inquiry, Then the solution shall prevent the transaction.;		
7884	Data Mapping Management	As a System Administrator, I want to maintain source-to-target data mappings for integrated systems, so that shared information is interpreted across solutions.	AC 1 Given an integrated system requires source-to-target mapping, When an authorized administrator creates a mapping, Then the solution shall retain the source field, target field, and configured mapping rule.; AC 2 Given an existing mapping requires modification, When an authorized administrator updates the mapping, Then the solution shall retain the revised mapping.; AC 3 Given an approved mapping is active, When data is exchanged between solutions, Then the interface shall apply the configured mapping.; AC 4 Given a required source-to-target mapping is missing, When the interface processes the data, Then the solution shall identify the unmapped data according to configured error handling.; AC 5 Given a mapping configuration changes, When subsequent data is exchanged, Then the interface shall use the current approved mapping.;		
7885	DMV Vehicle and Plate Exchange	As an Officer, I need the CAD/RMS solution to retrieve authorized vehicle and license plate information from the DMV through an approved interface, so that current vehicle information can be accessed without unnecessary manual entry.	AC 1 Given an officer enters an authorized vehicle or plate identifier, When the officer initiates a DMV inquiry, Then the solution shall transmit the authorized inquiry through the approved interface.; AC 2 Given DMV returns an authorized response, When the response is received, Then the solution shall display the vehicle and plate information.; AC 3 Given DMV returns no matching result, When the response is received, Then the solution shall indicate that no matching information was found.; AC 4 Given the DMV interface is unavailable, When the officer initiates an inquiry, Then the solution shall identify the unavailable service according to configured rules.; AC 5 Given an officer is not authorized to submit DMV inquiries, When the officer initiates an inquiry, Then the solution shall prevent the transaction.;		
7886	DOC Offender Information	As an Officer, I want the solution to retrieve authorized offender information from DOC, so that offender information is available to support dispatch, response, and investigative activities.	AC 1 Given an officer is authorized to request DOC offender information, When the officer submits an approved offender inquiry, Then the solution shall transmit the inquiry through the configured DOC interface.; AC 2 Given DOC returns an authorized response, When the response is received, Then the solution shall display the offender information.; AC 3 Given DOC returns no matching offender information, When the response is received, Then the solution shall indicate that no matching information was found.; AC 4 Given the DOC interface is unavailable, When the officer submits an inquiry, Then the solution shall identify the unavailable service according to configured rules.; AC 5 Given an officer is not authorized to retrieve DOC information, When the officer initiates an inquiry, Then the solution shall prevent the transaction.;		
7887	911 and GIS Location Information Exchange	As a Dispatcher, I want the solution to exchange available caller and incident location information with authorized 911 and GIS services through supported interfaces, so that caller and incident locations can be identified and validated.	AC 1 Given a caller or incident contains location information, When the solution exchanges information with supported 911 or GIS services, Then the solution shall transmit the configured location information through the applicable interface.; AC 2 Given a supported 911 or GIS service returns location information, When the response is received, Then the solution shall associate the returned information with the applicable call or incident record.; AC 3 Given a supported 911 or GIS service returns geographic coordinates, When the coordinates are received, Then the solution shall associate the coordinates with the applicable call or incident location.; AC 4 Given a supported 911 or GIS service identifies a location discrepancy, When the response is processed, Then the solution shall identify the discrepancy to the dispatcher.; AC 5 Given an applicable location information interface is unavailable, When a location exchange is attempted, Then the solution shall record the interface failure.; AC 6 Given an applicable location information interface is unavailable, When a location exchange is attempted, Then the solution shall provide the configured notification to the appropriate user.; AC 7 Given an authorized dispatcher corrects location information, When the corrected information is saved, Then the solution shall retain the updated location information and associated validation status.;		
7889	NCIC Inquiry & Response	As an Officer, I want the solution to submit authorized NCIC inquiries and receive responses, so that criminal justice information is available to support emergency response and investigations.	AC 1 Given an officer is authorized to conduct an NCIC inquiry, When the officer submits a valid inquiry, Then the solution shall transmit the inquiry through the approved NCIC interface.; AC 2 Given NCIC returns a response, When the response is received, Then the solution shall display the authorized response information.; AC 3 Given NCIC returns no matching information, When the response is received, Then the solution shall indicate that no matching information was returned.; AC 4 Given the NCIC interface is unavailable, When the officer submits an inquiry, Then the solution shall identify the unavailable service according to configured rules.; AC 5 Given an NCIC transaction is completed, When the transaction is recorded, Then the solution shall retain the transaction information according to configured requirements.; AC 6 Given an officer is not authorized to conduct the inquiry, When the officer attempts the transaction, Then the solution shall prevent the inquiry.;		

7890	Enterprise Justice (Odyssey) Integration	As an Officer, I want the solution to retrieve court-order information from Enterprise Justice (Odyssey), so that current court-order information is available when making enforcement and investigative decisions.	AC 1 Given an officer is authorized to retrieve court-order information, When the officer submits an approved Enterprise Justice (Odyssey) inquiry, Then the solution shall transmit the inquiry through the configured interface.; AC 2 Given Enterprise Justice (Odyssey) returns court-order information, When the response is received, Then the solution shall display the authorized information.; AC 3 Given Enterprise Justice (Odyssey) returns no court-order information, When the response is received, Then the solution shall indicate that no matching information was returned.; AC 4 Given the Enterprise Justice (Odyssey) interface is unavailable, When the officer submits an inquiry, Then the solution shall identify the unavailable service according to configured rules.; AC 5 Given a court-order response is received, When the transaction is completed, Then the solution shall retain the transaction information according to configured requirements.; AC 6 Given an officer is not authorized to retrieve court-order information, When the officer initiates the inquiry, Then the solution shall prevent the transaction.;		
7891	Radio Log Integration	As a Dispatcher, I want the solution to receive and associate radio log information with incidents and operational records, so that users can review related radio history.	AC 1 Given radio log information is received for an incident, When the solution processes the radio information, Then the solution shall associate the radio log with the incident.; AC 2 Given radio log information is associated with an operational record, When an Authorized User views the record, Then the radio history shall be available.; AC 3 Given multiple radio log entries are associated with an incident, When an Authorized User views the radio history, Then the solution shall display the entries according to configured ordering.; AC 4 Given radio log information cannot be associated, When the solution identifies the association failure, Then the solution shall identify the information requiring authorized review.; AC 5 Given radio log information is restricted, When an unauthorized user attempts to access the radio history, Then the solution shall restrict access according to configured security rules.; AC 6 Given radio log information is received after an incident is closed, When the information is associated with the incident, Then the solution shall retain the radio history without reopening the incident.;		
7895	VCIC Data Exchange	As an authorized law enforcement user, I need the CAD/RMS solution to exchange authorized criminal justice information with VCIC through approved interfaces, so that permitted information is available to support public-safety and investigative activities.	AC 1 Given an Authorized User initiates a VCIC information exchange, When the request meets configured authorization requirements, Then the solution shall exchange the approved information with VCIC.; AC 2 Given VCIC returns an authorized response, When the solution receives the response, Then the solution shall make the returned information available to the authorized user.; AC 3 Given a VCIC exchange fails or returns an error, When the solution receives the error, Then the solution shall identify the exchange as unsuccessful.; AC 4 Given a VCIC exchange fails or returns an error, When the solution receives the error, Then the solution shall provide an error indication.;		
7896	VT Parcel Locator	As a Dispatcher, I want the solution to retrieve property and property-owner information from the VT Parcel Locator, so that incidents and investigations can be associated with accurate property information.	AC 1 Given a property or property-owner lookup is requested, When the Dispatcher provides the required search information, Then the solution shall query the approved VT Parcel Locator source.; AC 2 Given matching property information is returned, When the search results are received, Then the solution shall display the property and property-owner information to the Dispatcher.; AC 3 Given returned property information is associated with an incident or investigation, When the Dispatcher selects the property, Then the solution shall associate the property information with the record.;		
7897	Recording System Integration	As a Dispatcher, I want CAD to interface with the approved recording system, so that call and communications recordings can be associated with the corresponding call or incident.	AC 1 Given a call or incident has an associated recording, When the solution exchanges information with the approved recording system, Then the solution shall associate the recording with the call or incident.; AC 2 Given a recording is available for an associated call or incident, When an Authorized User accesses the record, Then the solution shall provide access to the associated recording or recording reference.; AC 3 Given a recording exchange fails, When the failure is detected, Then the solution shall record or identify the unsuccessful exchange.;		
7898	VT Alert Data Exchange	As a Dispatcher, I want the solution to exchange approved emergency notification information with VT Alert, so that authorized alerts can be initiated or received through the State alerting process.	AC 1 Given an authorized emergency notification is required, When the Dispatcher initiates the notification through CAD/RMS, Then the solution shall exchange the approved notification information with VT Alert.; AC 2 Given an approved alert is received from VT Alert, When the alert is received by the solution, Then the solution shall make the alert available to authorized users.; AC 3 Given an alert exchange is unsuccessful, When the solution detects the failure, Then the solution shall indicate that the notification was not successfully exchanged.;		
7899	Local Tax Information	As a Dispatcher, I want the solution to retrieve current local tax information from an approved source, so that authorized users can access tax information for investigative and operational activities.	AC 1 Given an Authorized User requests local tax information, When the required search information is entered, Then the solution shall retrieve information from the approved source.; AC 2 Given current local tax information is returned, When the retrieval is completed, Then the solution shall display the information to the authorized user.; AC 3 Given no matching local tax information is available, When the search is completed, Then the solution shall indicate that no information was found.;		
7900	State Tax Information	As a Dispatcher, I need the solution to retrieve authorized State tax information from VTax, Vermont?s State tax system, so that authorized users can access associated tax information to support investigative and operational activities.	AC 1 Given an Authorized User requests State tax information, When the required search information is entered, Then the solution shall retrieve information from the approved source.; AC 2 Given current State tax information is returned, When the retrieval is completed, Then the solution shall display the information to the authorized user.; AC 3 Given the approved State tax source is unavailable, When the user attempts a lookup, Then the solution shall indicate that the information could not be retrieved.;		
7901	Radio System Integration	As a Dispatcher, I need the CAD solution to exchange incident, unit assignment, and dispatch status information with the approved radio communications software, so that radio operations and dispatch activities remain synchronized with current incidents and resource assignments.	AC 1 Given an incident has associated radio communications or resources, When CAD exchanges operational information with the approved radio software, Then the solution shall synchronize the information between the solutions.; AC 2 Given a resource or incident status changes in an approved exchange, When the change is received, Then the solution shall update the operational information.; AC 3 Given the radio-system exchange fails, When the failure is detected, Then the solution shall identify the unsuccessful exchange.;		

7928	VTrans Integration	As a Dispatcher, I need the CAD solution to identify and transmit authorized incident and response information to VTrans through the designated ATMS interface when approved applicability criteria are met, so that VTrans receives timely, accurate, and traceable information for transportation operations while protecting PII and sensitive information.	AC 1 Given an incident meets the approved applicability criteria for VTrans exchange, When an authorized exchange is initiated, Then the solution shall transmit the approved incident and response information to VTrans through the designated ATMS interface.; AC 2 Given information is prepared for transmission to VTrans, When the outbound information is assembled, Then the solution shall exclude PII and sensitive information unless explicitly authorized and required.; AC 3 Given information is transmitted to VTrans, When the transaction is processed, Then the solution shall record the transaction status for traceability.; AC 4 Given a VTrans transmission fails, When the failure is detected, Then the solution shall notify the authorized user and retain the transaction status.		
7929	Vermont Department of Health EMS Integration	As an EMS Agency User, I want the solution to exchange approved EMS information with the Vermont Department of Health through supported interfaces, so that required information can be shared without duplicate entry.	AC 1 Given an EMS information exchange is required, When an authorized exchange is initiated, Then the solution shall transmit the approved information through the supported interface.; AC 2 Given approved EMS information is received from the Vermont Department of Health, When the information is received, Then the solution shall make the information available to authorized users.; AC 3 Given the interface exchange fails, When the failure occurs, Then the solution shall identify the unsuccessful exchange.;		
7930	Service Management Integration	As a System Administrator, I need the solution to exchange approved service-management information with the State's designated service-management platform, so that incidents, requests, problems, and support activities can be managed.	AC 1 Given a CAD/RMS issue, request, problem, or support activity requires service-management tracking, When an authorized exchange is initiated, Then the solution shall transmit the approved information to the designated service-management platform.; AC 2 Given the service-management platform returns an approved status or identifier, When the response is received, Then the solution shall retain or display the information.; AC 3 Given the service-management exchange fails, When the failure is detected, Then the solution shall identify the unsuccessful exchange.;		
7932	State Financial System (VISION) Integration	As a System Administrator, I need the CAD/RMS solution to exchange approved expense and cost information with the State's VISION financial system, so that expense management, financial tracking, and reporting can be supported without redundant data entry.	AC 1 Given approved expense and cost information has been recorded in CAD/RMS, When an authorized exchange is initiated, Then the system shall securely transmit the applicable information to the State's VISION financial system through the approved interface.; AC 2 Given VISION provides financial or cost information required by CAD/RMS, When the system retrieves the information, Then the CAD/RMS solution shall make the applicable information available to authorized users.; AC 3 Given expense or cost information is exchanged between CAD/RMS and VISION, When the transaction is processed, Then the system shall apply approved data mappings and validation rules to ensure the information is accurately exchanged.; AC 4 Given expense or cost information is transmitted to VISION, When the exchange is completed, Then the system shall record the transaction status, applicable financial reference, and date and time for traceability.; AC 5 Given an information exchange fails or VISION rejects the submitted information, When the failure or rejection is received, Then the system shall identify the unsuccessful transaction and make the applicable error information available for authorized review and resolution.; AC 6 Given expense or cost information is exchanged, When an authorized user accesses the information, Then the system shall enforce applicable access permissions and financial data security requirements.; AC 7 Given previously exchanged expense or cost information is updated, When the approved changes are transmitted, Then the system shall apply the changes in accordance with configured synchronization rules without creating unintended duplicate financial records.		
7940	OpenFox Integration	As an Officer or Investigator, I want the solution to securely exchange authorized law-enforcement information with OpenFox, so that required information can be accessed within the RMS workflow without unnecessary duplicate data entry.	AC 1 Given an authorized Officer or Investigator requests OpenFox information, When the request meets configured authorization requirements, Then the solution shall securely exchange the approved information with OpenFox.; AC 2 Given OpenFox returns approved information, When the response is received, Then the information shall be available within the authorized CAD/RMS workflow.; AC 3 Given the OpenFox exchange fails, When the failure is detected, Then the solution shall identify the unsuccessful exchange.;		
7941	State's Attorney Information Exchange	As an Officer or Investigator, I want the solution to securely exchange authorized incident, case, person, vehicle, evidence, and related information with Vermont State's Attorneys, so that authorized users can access information needed for investigations, prosecutions, court proceedings, and law enforcement operations.	AC 1 Given an authorized Officer or Investigator needs to exchange incident, case, person, vehicle, evidence, or related information with Vermont State's Attorneys, When the exchange is initiated, Then the solution shall transmit the approved information securely.; AC 2 Given an authorized recipient receives the information, When the exchange is completed, Then the information shall be available to the recipient according to authorization.; AC 3 Given the exchange includes protected information, When the information is transmitted, Then the solution shall apply required security controls.; AC 4 Given an exchange fails, When the failure occurs, Then the solution shall identify the unsuccessful exchange.;		
7942	Attorney General Case Documentation Exchange	As an Officer or Investigator, I need the solution to securely transmit authorized criminal case documentation to the Vermont Attorney General's Office, so that authorized prosecutors can access the information needed to review and support criminal case prosecution.	AC 1 Given an authorized criminal case is eligible for transmission to the Vermont Attorney General's Office, When the Officer or Investigator initiates the transmission, Then the solution shall transmit the authorized case documentation.; AC 2 Given the transmission is successful, When the Attorney General's Office receives the documentation, Then the solution shall retain the transmission status or reference.; AC 3 Given the transmission fails, When the failure is detected, Then the solution shall identify the unsuccessful transmission.;		
7977	API and Interface Documentation	As a System Administrator, I want documented APIs and interface contracts that identify authentication methods, message formats, supported versions, operations, and data mappings, so that integrations can be configured, maintained, and supported using consistent technical information.	AC 1 Given an interface is supported by CAD/RMS, When the solution Administrator accesses the interface documentation, Then the documentation shall identify the authentication method.; AC 2 Given an interface exchanges information with another system, When the interface documentation is reviewed, Then the documentation shall identify message formats and operations.; AC 3 Given an interface supports multiple versions, When the interface documentation is reviewed, Then the solution shall identify the supported versions.; AC 4 Given an interface requires data transformation or mapping, When the interface documentation is reviewed, Then the solution shall document the data mappings.;		
7979	Vermont Sheriff's Office Information Exchange	As a Partner Agency User, I want the solution to securely exchange approved information with participating Vermont Sheriffs' Offices, so that authorized information can be shared between participating agencies while protecting its integrity and confidentiality.	AC 1 Given an authorized Partner Agency User initiates an exchange with a participating Vermont Sheriff's Office, When the request meets configured authorization requirements, Then the solution shall securely transmit the approved information.; AC 2 Given approved information is received from a participating Sheriff's Office, When the information is validated, Then the information shall be made available to authorized users.; AC 3 Given the information is protected, When it is exchanged, Then the solution shall apply required confidentiality and integrity controls.;		

7980	Sheriff's Office Exchange Authorization and Audit	As a System Administrator, I want Sheriffs' Office information exchanges to enforce authorization and record transmission status, errors, and audit history, so that exchanges are limited to authorized activity and transmission events can be monitored and reviewed.	AC 1 Given a Sheriff's Office information exchange is initiated, When authorization is evaluated, Then the solution shall permit the exchange only when the user or system is authorized.; AC 2 Given an exchange is transmitted, When the transmission is completed, Then the solution shall record the transmission status.; AC 3 Given an exchange encounters an error, When the error occurs, Then the solution shall record the error information.; AC 4 Given an Authorized User reviews exchange history, When the audit history is retrieved, Then the solution shall provide the transmission and error history.;		
7997	NG9-1-1/i3 Interface Support	As a System Administrator, I want the solution to support approved NG9-1-1/i3 interfaces and message formats, so that required emergency communications information can be exchanged with compatible systems using approved standards.	AC 1 Given approved NG9-1-1/i3 interfaces and message formats are configured, When the solution exchanges information with a compatible system, Then the solution shall use the approved standards and message formats for the exchange; AC 2 Given an NG9-1-1/i3 message is received in an approved format, When the solution processes the message, Then the solution shall interpret and make the exchanged information available; AC 3 Given a message does not conform to a supported NG9-1-1/i3 format, When the solution receives it, Then the solution shall reject or flag the message as unsupported; AC 4 Given a system administrator configures an NG9-1-1/i3 interface, When the configuration is saved, Then the solution shall apply the interface configuration without custom code changes; AC 5 Given an NG9-1-1/i3 exchange occurs, When the exchange completes, Then the solution shall log the transaction for traceability;		
7998	NG9-1-1/i3 Metadata Processing	As a System Administrator, I want the solution to process supported NG9-1-1/i3 metadata and identify invalid or unsupported transactions, so that exchanged information can be interpreted and invalid transactions can be handled.	AC 1 Given supported NG9-1-1/i3 metadata accompanies a transaction, When the solution processes the transaction, Then the solution shall interpret the supported metadata; AC 2 Given supported NG9-1-1/i3 metadata accompanies a transaction, When the solution processes the transaction, Then the solution shall make it available; AC 3 Given a transaction contains invalid or unsupported content, When the solution processes it, Then the solution shall identify the transaction as invalid or unsupported; AC 4 Given an invalid or unsupported transaction is identified, When the solution handles it, Then the solution shall apply the configured handling; AC 5 Given an invalid or unsupported transaction is identified, When the solution handles it, Then the solution shall prevent the invalid transaction from corrupting incident data; AC 6 Given a transaction is identified as invalid, When an Authorized User reviews transaction processing, Then the solution shall provide a record of the invalid transaction and its handling; AC 7 Given metadata is successfully interpreted, When the information is used in operations, Then the solution shall associate the interpreted metadata with the record;		
7999	External Query Follow-On Search	As an Officer or Investigator, I want to use information returned from an authorized external database query to initiate a follow-on query, so that I can obtain additional authorized information related to the initial search.	AC 1 Given results have been returned from an authorized external database query, When an officer or investigator selects returned information to initiate a follow-on query, Then the solution shall initiate the follow-on query using the selected information; AC 2 Given a user is not authorized for the follow-on query source, When the user attempts the follow-on query, Then the solution shall prevent the query; AC 3 Given a follow-on query is initiated, When the query returns results, Then the solution shall present the additional authorized information to the user; AC 4 Given a follow-on query is performed, When the query executes, Then the solution shall record the query and its association with the initiating record for audit purposes; AC 5 Given the follow-on query source is unavailable, When the user initiates the query, Then the solution shall notify the user that the query could not be completed;		
8000	External Database Queries	As an Officer or Investigator, I want to submit authorized queries to approved external databases and receive the resulting responses, so that I can obtain authorized information from external sources to support incident and field operations.	AC 1 Given an officer or investigator is authorized to query an approved external database, When the user submits a query, Then the solution shall transmit the query to the approved external database; AC 2 Given an officer or investigator is authorized to query an approved external database, When the user submits a query, Then the solution shall return the response; AC 3 Given a user is not authorized for a requested external database, When the user submits the query, Then the solution shall prevent the query; AC 4 Given required query parameters are incomplete, When the user submits the query, Then the solution shall identify the missing parameters; AC 5 Given required query parameters are incomplete, When the user submits the query, Then the solution shall prevent submission; AC 6 Given a query is submitted to an external database, When a response is received, Then the solution shall present the response to the requesting user; AC 7 Given an external database is unavailable or returns an error, When the user submits a query, Then the solution shall notify the user that the query could not be completed; AC 8 Given an external query is performed, When the query and response are processed, Then the solution shall log the transaction with user, date, and time for audit purposes;		
8001	External Query Alerts and Significant Matches	As an Officer or Investigator, I want the solution to identify and manage configured alerts and significant matches returned from authorized queries, so that information requiring attention can be recognized and acted upon.	AC 1 Given configured alert and significant-match criteria, When a query returns information that meets those criteria, Then the solution shall identify the significant match or alert to the user; AC 2 Given a significant match is identified, When the user views the query results, Then the solution shall present the match with distinguishable visual indication; AC 3 Given an alert requires acknowledgment, When the user acts on the alert, Then the solution shall record the acknowledgment and the acting user; AC 4 Given an authorized administrator configures alert and match criteria, When the configuration is saved, Then the solution shall apply the criteria to subsequent query responses; AC 5 Given a significant match is identified, When the match is processed, Then the solution shall retain a record of the match for audit and review; AC 6 Given multiple alerts are returned, When the user manages the alerts, Then the solution shall allow the user to act on and clear individual alerts while retaining alert history;		
8012	CalTopo Mapping Integration	As a Dispatcher or Field Personnel, I want the solution to exchange approved operational mapping information with CalTopo when the integration is enabled, so that dispatch and field personnel can use coordinated mapping information.	AC 1 Given the CalTopo integration is enabled, When approved operational mapping information is exchanged, Then the solution shall send and receive the mapping information with CalTopo; AC 2 Given the CalTopo integration is disabled, When a user attempts a CalTopo exchange, Then the solution shall withhold the CalTopo exchange while the integration is disabled.; AC 3 Given mapping information is received from CalTopo, When the solution processes it, Then the solution shall make the coordinated mapping information available to dispatch and field personnel; AC 4 Given a CalTopo exchange fails, When the failure occurs, Then the solution shall notify the user that the exchange could not be completed; AC 5 Given a CalTopo exchange occurs, When the exchange completes, Then the solution shall log the exchange for traceability;		

8027	Mutual Aid Agreement Configuration	As a System Administrator, I want the solution to configure and maintain mutual aid agreements with participating agencies, response levels, activation criteria, resource requirements, and configured rules, so that mutual aid resources are identified, requested, and managed according to established agreements and agency policies.	AC 1 Given an administrator configures a mutual aid agreement, When rules and levels are defined and saved, Then the solution shall persist the mutual aid agreement with its rules and levels; AC 2 Given a mutual aid agreement is in effect, When mutual aid utilization is evaluated, Then the solution shall apply the agreement's rules and levels; AC 3 Given required agreement information is incomplete, When the administrator attempts to save it, Then the solution shall identify the missing information; AC 4 Given required agreement information is incomplete, When the administrator attempts to save it, Then the solution shall prevent saving; AC 5 Given a user lacks permission to configure agreements, When the user attempts the change, Then the solution shall prevent the modification; AC 6 Given a mutual aid agreement is changed, When an Authorized User reviews the configuration history, Then the solution shall provide a record of the change and the user;		
8028	CAD-to-CAD EIDD Integration	As an Authorized User, I want the solution to support CAD-to-CAD exchange using the Emergency Incident Data Document (EIDD) standard with the automated exchange and population of incident data, so that information can be shared between interoperable solutions.	AC 1 Given CAD-to-CAD integration supporting EIDD is enabled, When incident data is exchanged with another CAD, Then the solution shall auto-populate the incident using the exchanged EIDD data; AC 2 Given EIDD data is received, When the solution processes it, Then the solution shall validate the data against the EIDD standard; AC 3 Given received EIDD data does not conform to the standard, When the solution processes it, Then the solution shall identify the nonconforming data; AC 4 Given received EIDD data does not conform to the standard, When the solution processes it, Then the solution shall handle it; AC 5 Given a CAD-to-CAD exchange occurs, When incident data is auto-populated, Then the solution shall associate the exchanged data with the incident; AC 6 Given a CAD-to-CAD exchange fails, When the failure occurs, Then the solution shall notify the authorized user; AC 7 Given a CAD-to-CAD exchange fails, When the failure occurs, Then the solution shall retain the incident data already received; AC 8 Given a CAD-to-CAD exchange occurs, When the exchange completes, Then the solution shall log the transaction for traceability;		
8029	Partner Agency Resource Visibility	As a Dispatcher, I want the solution to display the current status and availability of authorized partner agency units and resources, so that partner resources can be identified and considered when coordinating incident response.	AC 1 Given partner agency unit status and availability are shared, When a dispatcher views resource awareness, Then the solution shall display the partner units' current status and availability; AC 2 Given a partner unit's status changes, When the update is received, Then the solution shall update the displayed partner unit status; AC 3 Given partner unit status information is unavailable, When a dispatcher views partner resources, Then the solution shall indicate that current status is unavailable; AC 4 Given partner units are displayed, When the dispatcher views resources, Then the solution shall distinguish partner units from local units;		
8031	Automatic Aid Agreements and Triggers	As a Supervisor, I want automatic aid agreements and triggers, so that partner resources are dispatched under configured conditions.	AC 1 Given automatic aid agreements and triggers are configured, When a configured trigger condition occurs, Then the solution shall dispatch the partner resources defined by the agreement; AC 2 Given an administrator configures an automatic aid trigger, When the configuration is saved, Then the solution shall persist the automatic aid agreement and its triggers; AC 3 Given a trigger condition is not met, When an incident is processed, Then the solution shall initiate automatic aid only when the trigger condition is met.; AC 4 Given automatic aid is dispatched, When the dispatch occurs, Then the solution shall record the automatic aid action with the triggering condition and time; AC 5 Given a partner resource is unavailable when automatic aid triggers, When the solution attempts the automatic dispatch, Then the solution shall notify the dispatcher of the condition; AC 6 Given a user lacks permission to configure automatic aid, When the user attempts the change, Then the solution shall prevent the modification;		
8041	ASAP-to-PSAP Alarm Integration	As an Authorized User, I want an ASAP-to-PSAP interface, so that alarm monitoring companies can submit alarms to CAD.	AC 1 Given the ASAP-to-PSAP interface is configured, When an alarm monitoring company submits an alarm, Then the solution shall receive the alarm into CAD; AC 2 Given an ASAP alarm is received, When the solution processes it, Then the solution shall create or associate the CAD event from the alarm data; AC 3 Given an ASAP alarm message is invalid or incomplete, When the solution receives it, Then the solution shall identify the invalid message; AC 4 Given an ASAP alarm message is invalid or incomplete, When the solution receives it, Then the solution shall handle it per the configured rules; AC 5 Given an ASAP alarm is processed, When the transaction completes, Then the solution shall acknowledge receipt to the alarm monitoring company per the ASAP standard; AC 6 Given an ASAP transaction occurs, When it is processed, Then the solution shall log the transaction for traceability;		
8061	Automated Individual Information Queries	As a Dispatcher, I want the solution to initiate an automatic query, upon entry of information about an individual associated with an event, using the following guidelines at a minimum: 1) If the name only is known, then a name query be initiated to local files capable of performing a lookup based only on a name. 2) If the minimum required fields contain enough data for state and federal queries, then the solution will initiate queries to local, state, and federal databases, so that the capability is available in accordance with approved operational requirements.	AC 1 Given information about an individual associated with an event is entered and only the name is known, When the automatic query is initiated, Then the solution shall initiate a name query to local files capable of a name-only lookup; AC 2 Given the minimum required fields contain the data required for state and federal queries, When the automatic query is initiated, Then the solution shall initiate queries to local, state, and federal databases; AC 3 Given insufficient data exists for state and federal queries, When an individual's information is entered, Then the solution shall limit the automatic query to the sources supported by the available data; AC 4 Given an automatic query is initiated, When the query executes, Then the solution shall associate the query and its results with the event; AC 5 Given a queried database is unavailable, When the automatic query runs, Then the solution shall notify the user that the query could not be completed; AC 6 Given an automatic query is performed, When it executes, Then the solution shall log the query with user, date, and time for audit purposes;		
8085	Early CAD-to-RMS Transfer	As a Dispatcher, I want the solution to support data transfer prior to the normal chronological transfer point to provide the public safety responders with an RMS incident number when needed, and if this method is required to retrieve an RMS incident number, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a public safety responder needs an RMS incident number before the normal chronological transfer point, When data transfer is initiated, Then the solution shall transfer the data early; AC 2 Given a public safety responder needs an RMS incident number before the normal chronological transfer point, When data transfer is initiated, Then the solution shall provide an RMS incident number; AC 3 Given early transfer is the required method to retrieve an RMS incident number, When the transfer occurs, Then the solution shall return the RMS incident number to the requesting user; AC 4 Given an early transfer fails, When the failure occurs, Then the solution shall notify the user that the RMS incident number could not be retrieved; AC 5 Given an early transfer occurs, When it is processed, Then the solution shall associate the RMS incident number with the originating CAD event;		

8105	CAD-to-RMS Event Data Transfer	As a Dispatcher, I need the solution to support/make the updated CFS data available for transfer to an RMS, so that the capability is available consistently, traceably, and in accordance with approved operational requirements.	AC 312.1 Given a CFS event has been updated, When the updated data is prepared for transfer, Then the system shall make the updated CFS data available for transfer to an RMS; AC 312.2 Given updated CFS data is transferred to an RMS, When the transfer occurs, Then the system shall associate the transferred data with the applicable RMS record; AC 312.3 Given a transfer to the RMS fails, When the failure occurs, Then the system shall identify the failure and apply the configured handling; AC 312.4 Given a transfer occurs, When it is processed, Then the system shall log the transfer for traceability;		
8141	CAD-to-AVL Location Exchange	As a Dispatcher, I want the solution to pass any changes in unit location information to the AVL system if unit location changes are generated within the proposed system (as opposed to the AVL navigation system), so that the capability is available in accordance with approved operational requirements.	AC 1 Given unit location changes are generated within the proposed system rather than the AVL navigation system, When a unit location change occurs, Then the solution shall pass the change to the AVL system; AC 2 Given a unit location change is passed to the AVL system, When the transfer occurs, Then the solution shall maintain consistency between the proposed system and the AVL system; AC 3 Given the AVL system is unavailable, When a unit location change is generated, Then the solution shall identify the failure; AC 4 Given the AVL system is unavailable, When a unit location change is generated, Then the solution shall apply the configured handling; AC 5 Given a unit location change originates in the AVL navigation system, When the change is received, Then the solution shall apply the AVL-originated location change for internal use only.;		
8153	RMS Data Input and Integration	As an Authorized User, I want the solution to support required data being entered, uploaded in bulk, or loaded through live interfaces with RMS systems, so that required information can be available across the solution.	AC 1 Given required data is provided, uploaded in bulk, or loaded through live interfaces with RMS systems, When the data is submitted, Then the solution shall support the data entry method; AC 2 Given data is uploaded in bulk, When the upload is processed, Then the solution shall make the required information available across the solution; AC 3 Given a live RMS interface provides data, When the data is received, Then the solution shall load and make it available; AC 4 Given a data entry or upload fails, When the failure occurs, Then the solution shall identify the failure; AC 5 Given a data entry or upload fails, When the failure occurs, Then the solution shall apply the configured handling;		
8157	SMS Messaging Integration	As an Authorized User, I want the solution to support sending SMS messages through a cellular modem or a common carrier's SMTP interface, so that operational messages can be transmitted using supported communication methods.	AC 1 Given a cellular modem or a common carrier SMTP interface is available, When an Authorized User sends an SMS message, Then the solution shall send the SMS message through the supported communication method; AC 2 Given an SMS message fails to send, When the failure occurs, Then the solution shall notify the user that the message was not sent; AC 3 Given an SMS message is sent, When it is transmitted, Then the solution shall record the message transmission; AC 4 Given the configured communication method is unavailable, When the user attempts to send an SMS, Then the solution shall notify the user that message delivery is unavailable through the configured method.;		
8169	MDC-to-RMS Incident Data Exchange	As an Authorized User, I want the solution to support both push and pull exchange of incident and event data between the MDC and RMS, so that information can be exchanged and maintained across solutions.	AC 1 Given incident and event data to exchange between the MDC and RMS, When a push exchange is initiated, Then the solution shall push the incident and event data to the RMS; AC 2 Given incident and event data is requested from the RMS, When a pull exchange is initiated, Then the solution shall pull the data to the MDC; AC 3 Given a push or pull exchange occurs, When the exchange completes, Then the solution shall maintain the data across the MDC and RMS; AC 4 Given an exchange fails, When the failure occurs, Then the solution shall identify the failure; AC 5 Given an exchange fails, When the failure occurs, Then the solution shall apply the configured handling; AC 6 Given a user lacks permission for an MDC-to-RMS exchange, When the exchange is attempted, Then the solution shall prevent it; AC 7 Given an MDC-to-RMS exchange occurs, When it is processed, Then the solution shall log the transaction for traceability;		
8170	Agency-Specific Report and Case Number Assignment	As a Dispatcher, I want the solution to assign an agency-specific report or case number, when required by agency policy and when a report is required, in addition to the CAD incident/event number before transferring CFS event data to RMS, so that the RMS record contains the required agency-specific identifier.	AC 1 Given agency policy requires a report and a report is required, When CFS event data is prepared for transfer to the RMS, Then the solution shall assign an agency-specific report or case number in addition to the CAD incident/event number; AC 2 Given an agency-specific report number is assigned, When the data is transferred to the RMS, Then the solution shall ensure the RMS record contains the agency-specific identifier; AC 3 Given a report is not required by agency policy, When the CFS data is transferred, Then the solution shall make the agency-specific report number optional for the transfer.; AC 4 Given a duplicate agency-specific number would be assigned, When the assignment is attempted, Then the solution shall identify the duplicate; AC 5 Given a duplicate agency-specific number would be assigned, When the assignment is attempted, Then the solution shall prevent it; AC 6 Given an agency-specific number is assigned, When the transfer occurs, Then the solution shall associate the number with both the CAD and RMS records;		
8185	CAD Access to RMS Information and Attachments	As a Dispatcher, I want the solution to provide authorized access to associated RMS information and associated attachments from within the CAD application with linked person, location, and vehicle information and attachments limited to photographs and video, so that associated RMS information is available within the CAD workflow to support incident response and decision-making.	AC 1 Given associated RMS information and associated attachments, When an Authorized User accesses RMS information from within the CAD application, Then the solution shall provide access to the linked person, location, and vehicle information and attachments limited to photographs and video; AC 2 Given a user is authorized, When the user opens an attachment from CAD, Then the solution shall make the attachment accessible within the CAD workflow; AC 3 Given a user lacks permission to access RMS information, When the user attempts access, Then the solution shall prevent it; AC 4 Given linked RMS information is displayed in CAD, When the user reviews it, Then the solution shall associate the information with the incident; AC 5 Given RMS information is unavailable, When the user requests it from CAD, Then the solution shall indicate that the information is unavailable;		
8186	Cross-System Report Number Management	As an Authorized User, I want the solution to support creating, recording, updating, and using an agency-specific report number separate from the CAD incident number, so that CAD and RMS records can be cross-referenced and associated across both solutions.	AC 1 Given an agency-specific report number separate from the CAD incident number, When an Authorized User creates, records, or updates the report number, Then the solution shall maintain the agency-specific report number; AC 2 Given an agency-specific report number is recorded, When CAD and RMS records are cross-referenced, Then the solution shall associate the records across both solutions using the report number; AC 3 Given a duplicate agency-specific report number is entered, When it is submitted, Then the solution shall identify the duplicate; AC 4 Given a duplicate agency-specific report number is entered, When it is submitted, Then the solution shall prevent it; AC 5 Given the agency-specific report number is updated, When the change is saved, Then the solution shall maintain the cross-reference between CAD and RMS; AC 6 Given a user lacks permission to maintain the report number, When the user attempts the change, Then the solution shall prevent it;		

8195	GPS and AVL Location Tracking	As a System Administrator, I need the CAD solution to support GPS-based location tracking and coordinate-based operations using location data from AVL systems, GPS-enabled mobile devices, and portable radios, with native CAD functionality or integration capabilities as needed, so that real-time responder locations can be used to support dispatch, mapping, and field operations.	AC 1 Given an AVL system, GPS-enabled mobile device, or portable radio provides location data, When the CAD solution receives the data, Then the system shall support receiving and processing responder location coordinates through native functionality or approved integrations.; AC 2 Given location data is received from an authorized source, When the data is processed, Then the CAD solution shall associate the location coordinates with the corresponding responder, unit, or device.; AC 3 Given current responder location data is available, When an authorized user views the CAD map or dispatch interface, Then the system shall display the responder's location using the received coordinates.; AC 4 Given updated GPS location data is received, When the responder's location changes, Then the CAD solution shall update the displayed location in accordance with configured update intervals and processing rules.; AC 5 Given responder location data is available, When dispatch operations are performed, Then the CAD solution shall make the location information available to support unit selection, dispatch decisions, and coordination of field operations.; AC 6 Given location data is received, When the coordinates are processed, Then the CAD solution shall support the coordinate formats, geographic reference systems, and mapping capabilities required for accurate location display and location-based operations.; AC 7 Given location data is unavailable, invalid, or cannot be updated, When the CAD solution detects the condition, Then the system shall indicate the applicable location status and retain the last known location with its associated timestamp, when available.; AC 8 Given responder location data is received or updated, When the transaction is processed, Then the CAD solution shall retain the applicable source, responder or device association, coordinates, and date and time to support operational traceability.; AC 9 Given responder location information is available, When a user attempts to view or use the information, Then the CAD solution shall enforce applicable role-based access, privacy, and security requirements.		
8209	Electronic Citation / E-Ticket Integration	As a Law Enforcement Officer or Dispatcher, I want the solution to integrate with electronic citation capabilities, so that DMV information can be imported into the incident, associated with the person and vehicle records, and used to populate citation information without redundant data entry.	AC 1 Given integration with electronic citation capabilities, When DMV information is imported into the incident, Then the solution shall import the DMV information; AC 2 Given integration with electronic citation capabilities, When DMV information is imported into the incident, Then the solution shall associate it with the person and vehicle records; AC 3 Given DMV information is imported, When a citation is created, Then the solution shall use the imported information to populate the citation without redundant data entry; AC 4 Given the electronic citation interface is unavailable, When import is attempted, Then the solution shall identify the failure; AC 5 Given the electronic citation interface is unavailable, When import is attempted, Then the solution shall apply the configured handling; AC 6 Given citation information is populated, When it is saved, Then the solution shall associate the citation with the incident, person, and vehicle; AC 7 Given a user lacks permission to import citation or DMV information, When the user attempts it, Then the solution shall prevent the action;		
8210	State and Municipal Evidence Management System Integration	As an Authorized User, I need the RMS solution to support integration with State (FileOnQ) and municipal evidence management systems and associate evidence records and related custody information with applicable incidents and cases, so that evidence information can be accessed, tracked, and maintained across systems without requiring duplicate data entry.	AC 1 Given an incident or case has associated evidence records in a State or municipal evidence management system, When an authorized user accesses the incident or case, Then the solution shall provide access to the associated evidence information.; AC 2 Given evidence information is available in an external evidence management system, When the information is retrieved, Then the solution shall associate the evidence information with the applicable incident or case.; AC 3 Given evidence information is exchanged between the RMS solution and an external evidence management system, When the exchange occurs, Then the solution shall support the transfer of available evidence identifiers, descriptions, status, and custody information without requiring duplicate data entry.; AC 4 Given evidence custody information is updated in an external evidence management system, When the updated information is made available to the RMS solution, Then the solution shall reflect the associated custody information for the applicable incident or case.; AC 5 Given an authorized user accesses evidence information, When the user attempts to view or retrieve evidence records, Then the solution shall enforce applicable user roles, permissions, and evidence access restrictions.; AC 6 Given evidence information is accessed or exchanged, When the activity occurs, Then the solution shall maintain an auditable record of the access and associated information exchange.		
8221	Structured Query-Result Retention (DMV/NCIC)	As a Dispatcher, I want the solution to retain DMV, NCIC, and related query results in a structured section separate from free-form incident notes, so that pertinent record information is preserved.	AC 1 Given a DMV, NCIC, or related query returns authorized results, When the dispatcher retains the results, Then the solution shall store them in a structured query-results section associated with the incident or record.; AC 2 Given query results are retained in the structured section, When an Authorized User views the incident, Then the solution shall display the results separately from free-form incident notes.; AC 3 Given multiple query results are retained, When the incident is reviewed, Then the solution shall retain each result as a distinct entry with its source and date/time.; AC 4 Given query results are restricted, When an unauthorized user accesses the incident, Then the solution shall restrict access to the retained results according to configured security rules.;		
8222	Person Query from CAD and Involved-Party Association	As a Dispatcher, I want the solution to run DMV and NCIC person queries from a person already entered in the CAD without re-entering identifiers, and to add returned involved parties to the incident or MDC, so that person checks avoid duplicate data entry and results are associated with the incident.	AC 1 Given a person is entered or identified in CAD, When the dispatcher initiates a DMV or NCIC person query, Then the solution shall submit the query using the existing person identifiers without requiring re-entry.; AC 2 Given a person query returns an authorized response, When the response is received, Then the solution shall display the person information to the authorized user.; AC 3 Given a returned party is to the incident, When the dispatcher selects it, Then the solution shall allow the party to be added to the incident or made available to the MDC.; AC 4 Given a person query returns no match, When the response is received, Then the solution shall indicate that no matching information was found.; AC 5 Given the DMV or NCIC interface is unavailable, When the dispatcher initiates a query, Then the solution shall indicate that the query could not be completed.; AC 6 Given a person query is submitted, When the transaction occurs, Then the solution shall record the query for audit purposes.;		

8231	VCIC/DMV Image File Upload and Association	As a Dispatcher or Authorized User, I need the solution to allow upload and association of VCIC or DMV image files (limited to mugshots and driver's license photos) with the person, incident, or record, so that identifying images are available to support response and investigation.	AC 1 Given an Authorized User has a VCIC or DMV image file, When the user uploads the image, Then the solution shall associate the image with the person, incident, or record.; AC 2 Given an image is uploaded, When the upload is completed, Then the solution shall retain the image in a supported format.; AC 3 Given an image is uploaded, When the upload is completed, Then the solution shall record its source and date/time.; AC 4 Given an image is associated with a record, When an Authorized User views the record, Then the solution shall make the image available for viewing.; AC 5 Given an uploaded file does not meet configured type or size rules, When the user attempts the upload, Then the solution shall reject the file and indicate the configured requirement.; AC 6 Given an image is restricted, When an unauthorized user attempts to access it, Then the solution shall prevent access according to configured security rules.;		
8235	Sex Offender Registry Search and Information Retrieval	As a Law Enforcement Officer, I need the CAD solution to support searches of the VSOR and NSOR, using available State and National information exchange capabilities (including NLETS), and associate returned registry information with applicable persons and incidents, so that officers can access relevant sex offender registration information to support identity verification, incident assessment, and field operations.	AC 1 Given an officer is conducting a person or incident inquiry, When the officer initiates a sex offender registry search, Then the solution shall support querying the Vermont Sex Offender Registry and National Sex Offender Registry for matching records.; AC 2 Given a registry search is submitted, When matching records are returned, Then the solution shall display available registry information, including identifying information and registration details.; AC 3 Given registry information is returned for a person, When a matching record is identified, Then the solution shall allow the officer to associate the returned information with the applicable person and incident.; AC 4 Given a registry search is submitted through an available State or national information exchange, When the search is processed, Then the solution shall support the exchange of information through applicable interfaces, including NLETS.; AC 5 Given no matching registry records are returned, When the search results are received, Then the solution shall indicate that no matching records were found.; AC 6 Given registry search results are received, When the results are accessed or associated with a person or incident, Then the solution shall retain the search activity and enforce applicable access permissions and information-sharing restrictions.		
8239	Marijuana Registry Integration	As an Authorized User, I want the solution to exchange information with the Marijuana Registry where required, so that registry information is available to support dispatch and records functions.	AC 1 Given a configured Marijuana Registry interface, When an Authorized User initiates an exchange, Then the solution shall transmit the request.; AC 2 Given a configured Marijuana Registry interface, When an Authorized User initiates an exchange, Then the solution shall return the results.; AC 3 Given registry information is returned, When the user reviews it, Then the solution shall allow association with the record where permitted.; AC 4 Given a registry transaction is performed, When it completes, Then the solution shall record the transaction in the audit log.; AC 5 Given the registry interface is unavailable, When an exchange is attempted, Then the solution shall notify the user.; AC 6 Given the registry interface is unavailable, When an exchange is attempted, Then the solution shall record the attempt.;		
8240	Forensic Lab Digital Imaging Integration	As an Investigator, I want the solution to integrate with the forensic lab digital imaging system where required, so that forensic images can be associated with the case or evidence record.	AC 1 Given a configured forensic imaging interface, When an Authorized User links a forensic image, Then the solution shall associate the image reference with the case or evidence record.; AC 2 Given a forensic image is associated, When an Authorized User reviews the case, Then the image reference shall be available consistent with access permissions.; AC 3 Given forensic image data is exchanged, When the transaction completes, Then the solution shall record the transaction.; AC 4 Given forensic image data is exchanged, When the transaction completes, Then the solution shall maintain chain-of-custody information where.; AC 5 Given the imaging interface is unavailable, When an exchange is attempted, Then the solution shall notify the user.; AC 6 Given the imaging interface is unavailable, When an exchange is attempted, Then the solution shall retain the request status.;		
8767	Monitor Interface Status and Activity	As a System Administrator, I want to monitor interface status and activity, so that integration health is visible.	AC 1 Given an interface is configured, When interface activity occurs, Then the solution shall record the interface activity.; AC 2 Given an interface is operational, When an authorized administrator views interface status, Then the solution shall display the current status.;		
8768	Detect and Notify Interface Failures	As a System Administrator, I want interface failures detected and notified, so that problems are addressed before they disrupt operations.	AC 1 Given an interface failure occurs, When the failure is detected, Then the solution shall record the failure.; AC 2 Given an interface failure is detected, When the configured notification condition is met, Then the solution shall notify the designated administrator or support user.;		
8769	Recover Failed Interface Transactions	As a System Administrator, I want failed transactions recovered when an interface is restored, so that integrations resume cleanly.	AC 1 Given an interface is restored, When successful communication is detected, Then the solution shall record the recovery status.; AC 2 Given failed transactions are eligible for recovery, When the interface is restored, Then the solution shall process the configured recovery or retry workflow.;		
8770	Review Interface History	As a System Administrator, I want to review interface failure and recovery history, so that recurring problems can be analyzed.	AC 1 Given an interface has experienced failures, When an authorized administrator reviews interface history, Then the solution shall display the failures, recovery actions, and status history.; AC 2 Given interface history contains multiple records, When an authorized administrator filters by interface or date range, Then the solution shall display the interface history matching the selected criteria.; AC 3 Given an interface history record is displayed, When the administrator selects a record, Then the solution shall present the failure details, timestamps, and recovery outcome for that record.;		
8771	Transmit Incident Information to VTrans	As a Dispatcher, I want to transmit approved incident and response information to VTrans through the designated interface, so that VTrans receives the required information.	AC 1 Given an incident requires information exchange with VTrans, When an authorized exchange is initiated, Then the solution shall transmit the approved incident and response information through the designated VTrans/NEC interface.; AC 2 Given an authorized dispatcher identifies an applicable incident, When the dispatcher initiates a VTrans/NEC exchange, Then the solution shall transmit the required incident information, including all approved incident and response data elements and applicable public-facing or free-form message content.; AC 3 Given an incident is prepared for transmission to VTrans, When the outbound information is assembled, Then the solution shall validate the transaction against the configured NEC XML schema, message structure, and interface requirements.; AC 4 Given an incident is prepared for transmission to VTrans, When the outbound information is assembled, Then the solution shall exclude PII, CJIS-protected, and other sensitive information unless explicitly authorized and required.		

8772	Determine VTrans Applicability	As a Dispatcher, I want the solution to determine whether an incident is applicable for VTrans transmission, so that only approved incidents are transmitted.	AC 1 Given an incident may require transmission to VTrans, When the incident is evaluated against approved applicability criteria, Then the solution shall identify whether the incident is applicable for transmission based on business rules and guidance approved by DPS and VTrans.; AC 2 Given an incident does not meet the approved VTrans applicability criteria, When the incident is evaluated, Then the solution shall identify the incident as not applicable.; AC 3 Given an incident does not meet the approved VTrans applicability criteria, When the incident is evaluated, Then the solution shall exclude it from VTrans transmission.; AC 4 Given an incident is evaluated for VTrans applicability, When the determination is made, Then the solution shall record the applicability result with the incident record.;		
8773	Handle VTrans Response and Failures	As a Dispatcher, I want the solution to handle VTrans responses and exchange failures, so that exchanges complete reliably.	AC 1 Given VTrans returns approved information, When the response is received, Then the solution shall make the applicable information available to authorized CAD users.; AC 2 Given an exchange fails, When the failure is detected, Then the solution shall identify the unsuccessful exchange.; AC 3 Given an exchange fails, When the failure is detected, Then the solution shall support configurable retry and failure-handling processes, including notification when manual intervention is required.; AC 4 Given the VTrans/NEC interface is unavailable or a transaction cannot be completed, When the solution detects the condition, Then the solution shall preserve the transaction status and applicable information needed to support subsequent retry, resolution, and audit.;		
8774	Log and Secure VTrans Exchanges	As an authorized user, I want VTrans exchanges logged, traceable, and secured, so that exchange activity is auditable and compliant.	AC 1 Given a VTrans/NEC exchange is initiated, When the transaction is processed, Then the solution shall log the incident identifier, transmission date and time, initiating user or solution process, transaction status, response or error information, and applicable transaction identifier.; AC 2 Given an authorized user needs to review VTrans/NEC exchange activity, When the user searches for a transaction, Then the solution shall provide searchable transaction history and end-to-end traceability from incident identification and transmission through response, retry, and final disposition.; AC 3 Given VTrans/NEC information is exchanged, When the transaction is processed, Then the solution shall enforce applicable authentication, authorization, security, auditability, and records-retention requirements.;		
8815	CAD-to-RMS Event Data Transfer	As a Dispatcher, I want updated CFS event data in CAD made available for transfer to the RMS, so that field updates are shared with the RMS.	AC 1 Given a CFS event is updated in CAD, When the update is applied, Then the solution shall make the updated data available for transfer to the RMS; AC 2 Given updated CFS data is transferred to an RMS, When the transfer occurs, Then the solution shall associate the transferred data with the RMS record; AC 3 Given a transfer to the RMS occurs, When the transfer is processed, Then the solution shall log the transfer for traceability;		
8818	Vermont Judiciary Electronic Filing Integration	As a Records Officer, I need the CAD solution to support electronic filing of case documents, citations, and associated records with the Vermont Judiciary through its designated electronic filing system, so that required court documentation can be submitted electronically, filing data can be transferred accurately, and filing status and acknowledgments can be tracked.	AC 1 Given a case document, citation, or associated record is ready for filing, When an authorized user submits it, Then the solution shall electronically transmit the record to the Vermont Judiciary's designated electronic filing system.; AC 2 Given a document or record is submitted to the Vermont Judiciary, When the electronic filing system acknowledges receipt, Then the solution shall record the filing confirmation and associate it with the applicable case.; AC 3 Given an electronic filing is rejected or cannot be completed, When the filing system returns an error or rejection, Then the solution shall notify the submitting user and provide the available error or rejection details.; AC 4 Given an electronic filing has been submitted, When the filing status is updated, Then the solution shall record and display the current filing status and associated acknowledgments.		
8819	Motor Vehicle Crash Report (WebCrash) Submission	As an Officer, I want the solution to create motor-vehicle crash reports and submit them to the statewide crash reporting system (WebCrash), so that crash data is captured once and reported to the State without duplicate entry.	AC 1 Given an officer documents a motor-vehicle crash, When the officer completes the configured crash report, Then the solution shall capture the required crash data elements.; AC 2 Given a completed crash report, When the officer submits it, Then the solution shall transmit the report to the statewide crash reporting system (WebCrash).; AC 3 Given incident information already exists in the CAD or RMS record, When a crash report is created, Then the solution shall prefill the report with the available information.; AC 4 Given a crash report submission is acknowledged, When the response is received, Then the solution shall record the submission status with the report.; AC 5 Given a crash report fails validation or submission, When the failure is detected, Then the solution shall notify the officer.; AC 6 Given a crash report fails validation or submission, When the failure is detected, Then the solution shall identify the errors for correction.; AC 7 Given a crash report transaction occurs, When the transaction completes, Then the solution shall log the submission for audit.;		
8823	VLETS Statewide Message Switch Integration	As a Dispatcher, I want the solution to connect to the Vermont Law Enforcement Telecommunications System (VLETS) message switch to route records queries and interagency messages, so that authorized users can reach state and national databases and exchange messages through the statewide switch.	AC 1 Given the solution is configured for VLETS, When an authorized user submits a query or message, Then the solution shall transmit it to the VLETS message switch.; AC 2 Given the solution is configured for VLETS, When an authorized user submits a query or message, Then the solution shall return the response.; AC 3 Given a VLETS response is received, When the response is returned, Then the solution shall associate it with the relevant person, vehicle, or incident record.; AC 4 Given the VLETS connection is unavailable, When a query or message is attempted, Then the solution shall notify the user and queue or fail the request according to configured rules.; AC 5 Given access to VLETS is restricted by role and CJIS requirements, When an unauthorized user attempts access, Then the solution shall prevent the transaction.; AC 6 Given access to VLETS is restricted by role and CJIS requirements, When an unauthorized user attempts access, Then the solution shall log the attempt.; AC 7 Given a VLETS transaction occurs, When the transaction completes, Then the solution shall log the request and response for audit.;		

8832	VTHR Integration	As a System Administrator, I need the solution to automatically transmit approved employee time and attendance information to the State's VTHR system for timesheet processing, so that employee hours are accurately recorded and timesheets can be processed without duplicate data entry.	AC 1 Given employee time and attendance information has been recorded and approved in the solution, When the configured transmission process is initiated, Then the system shall automatically transmit the approved information to the State's VTHR system for timesheet processing.; AC 2 Given approved employee time and attendance information is transmitted to VTHR, When the transmission is processed, Then the system shall associate the submitted information with the applicable employee and reporting period.; AC 3 Given VTHR successfully receives the transmitted information, When the exchange is completed, Then the solution shall record the transmission status and applicable confirmation information.; AC 4 Given employee time and attendance information is missing, invalid, or incomplete, When the system prepares the transmission, Then the system shall identify the information requiring correction and prevent unsuccessful or incomplete data from being submitted.; AC 5 Given a transmission to VTHR fails or is rejected, When the failure or rejection is received, Then the system shall record the unsuccessful transaction and make the applicable error information available for authorized review and resolution.; AC 6 Given employee time and attendance information is transmitted to VTHR, When the transaction is completed, Then the system shall retain the applicable employee reference, reporting period, transmission status, and date and time for audit and traceability.; AC 7 Given previously transmitted employee time and attendance information is updated and reapproved, When the configured transmission process runs, Then the system shall transmit the approved changes in accordance with established synchronization rules without creating unintended duplicate timesheet entries.		
8833	WorkDay Integration	As an Authorized User, I need the CAD solution to securely exchange authorized personnel, organizational, and financial information with the State of Vermont's Workday ERP system through approved interfaces, so that CAD operations remain synchronized with authoritative State information and support personnel administration, resource management, and financial reporting.	AC 1 Given an authorized CAD user requires personnel, organizational, or financial information maintained in Workday ERP, When the CAD solution initiates an approved information request, Then the system shall securely retrieve the authorized information through the designated interface.; AC 2 Given Workday ERP provides updated personnel or organizational information, When the CAD solution receives the information, Then the system shall update the applicable CAD records in accordance with approved data mappings and synchronization rules.; AC 3 Given approved financial information is exchanged between CAD and Workday ERP, When the exchange is processed, Then the system shall transmit or retrieve the applicable information in accordance with the approved interface specifications and data mappings.; AC 4 Given personnel, organizational, or financial information is exchanged, When the information is transmitted or received, Then the system shall enforce applicable authentication, authorization, encryption, and data-protection requirements.; AC 5 Given an information exchange is initiated, When the transaction is completed, Then the system shall record the exchange status, applicable data category, source or destination, and date and time for traceability.; AC 6 Given Workday ERP or the designated interface is unavailable or returns an error, When an information exchange fails, Then the CAD solution shall identify the unsuccessful transaction and make the error available for authorized review and resolution.; AC 7 Given an authorized user reviews information received from Workday ERP, When the information is accessed or used in CAD operations, Then the system shall retain the applicable source and update information to support data integrity and auditability.		
8846	911 System Compatibility and Evolving Industry Standards	As an Authorized User, I want the CAD/RMS solution to support the receipt, exchange, processing, and retention of available 911 call, caller, and location information through interfaces compatible with the State's current 911 environment and evolving industry standards, including NG911, so that the solution can support current operations and accommodate future 911 technology and interface changes.	AC 1 Given the State's current 911 environment provides call, caller, or location information, When the CAD/RMS solution receives that information through a supported interface, Then the solution shall receive and process the available information for use in the applicable call or incident record.; AC 2 Given the CAD/RMS solution exchanges information with the State's 911 environment, When information is transmitted or received, Then the solution shall support the configured data elements and exchange requirements necessary to support the applicable business processes.; AC 3 Given the State's 911 environment or associated interfaces evolve, When new or revised industry standards or interface specifications are adopted by the State, Then the solution shall support the required interface changes through configuration, integration updates, or other supported modifications without requiring replacement of the CAD/RMS solution.; AC 4 Given the State transitions to NG911 or another 911 technology environment, When the applicable interfaces and exchange requirements are established, Then the solution shall support the receipt, exchange, processing, and retention of available 911 information in accordance with the State-approved interface specifications.; AC 5 Given a 911 interface or information exchange is unavailable or experiences an error, When the solution attempts to receive or exchange information, Then the solution shall identify and record the communication failure and provide configured notifications to appropriate users.; AC 6 Given 911 information is received through a supported interface, When the information is associated with a CAD call or incident record, Then the solution shall preserve the received information and maintain its association with the applicable record in accordance with configured retention and audit requirements.		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 08: Accessibility, Usability & User Experience					
7904	Accessibility Standards Compliance	As an Authorized User, I want the solution to meet configured accessibility standards with Section 504, Title II of the ADA, and WCAG 2.1 Level AA, so that users with disabilities can access and use required services and functions.	AC 1 Given an Authorized User accesses CAD/RMS using a supported interface, When the user performs a function, Then the solution shall provide the required function in accordance with configured accessibility requirements.; AC 2 Given a user requires keyboard-based access, When the user navigates supported functions, Then the interface shall provide keyboard access to controls.; AC 3 Given supported accessibility features are used, When the user accesses required content and functions, Then the content shall remain perceivable, operable, understandable, and usable in accordance with the configured accessibility standards identified in the user story.;		

7905	Browser and Mobile Device Compatibility	As an Authorized User, I want the solution to operate on approved browsers and supported mobile devices, so that users can access required functions without browser-specific limitations.	AC 1 Given a user accesses CAD/RMS using an approved browser, When the user performs supported functions, Then the solution shall operate as specified without browser-specific functional limitations.; AC 2 Given a user accesses supported mobile functionality using an approved mobile device, When the user performs supported functions, Then the solution shall provide the functionality.; AC 3 Given a browser or mobile device is not supported, When the user attempts access, Then the solution shall identify the unsupported environment.;		
7925	Keyboard Navigation and Shortcuts	As a Dispatcher, I want to navigate and perform supported CAD/RMS functions using configurable keyboard shortcuts and designated keys without requiring a mouse, so that I can complete operational activities using keyboard-driven workflows.	AC 1 Given a configurable keyboard shortcut is assigned to a supported function, When the Dispatcher uses the shortcut, Then the solution shall execute the associated function.; AC 2 Given a supported function is designated for keyboard access, When the Dispatcher navigates using designated keys, Then the function shall be accessible without requiring a mouse.; AC 3 Given a shortcut is not authorized or configured for a function, When the Dispatcher uses the shortcut, Then the solution shall execute only authorized functions.;		
7926	Data Entry Validation	As an Authorized User, I want data-entry fields to validate information against defined data types, formats, ranges, required fields, and business rules, so that inaccurate, incomplete, or invalid information is identified before it is saved.	AC 1 Given a data-entry field has a defined data type or format, When the user enters a value that does not meet the requirement, Then the solution shall identify the value as invalid.; AC 2 Given a field has a defined valid range, When the user enters a value outside the range, Then the solution shall prevent the invalid value from being saved.; AC 3 Given a field is required, When the user attempts to save without entering the required value, Then the solution shall identify the missing information.; AC 4 Given an entered value violates a configured business rule, When the user attempts to save the record, Then the solution shall identify the business-rule violation.; AC 5 Given an entered value violates a configured business rule, When the user attempts to save the record, Then the solution shall prevent saving when required.;		
7956	Narrative Shorthand and Auto-Text	As a Dispatcher, I want configurable shorthand and auto-text expansion in narrative fields, so that used terms can be entered while the resulting narrative remains complete, readable, and stored as the record.	AC 1 Given a configured shorthand or auto-text term is entered in a supported narrative field, When the Dispatcher invokes the expansion, Then the solution shall replace or expand the shorthand with the configured text.; AC 2 Given auto-text expansion has occurred, When the narrative is saved, Then the solution shall store the resulting complete text as part of the record.; AC 3 Given a shorthand term is not configured, When the Dispatcher enters the term, Then the solution shall retain the entered term unchanged when no expansion is configured.;		
8076	Automatic CFS Event Updates and Notifications	As a Dispatcher, I want the solution to display CFS event updates as they occur, highlight newly added or changed information using distinguishable formatting, and notify authorized users monitoring the event, so that current event information is immediately visible and accessible based on assigned user permissions.	AC 1 Given a CFS event is being monitored, When event updates occur, Then the solution shall display the CFS event updates as they occur; AC 2 Given new or changed information is added to an event, When it is displayed, Then the solution shall highlight the newly added or changed information using distinguishable formatting; AC 3 Given authorized users are monitoring the event, When an update occurs, Then the solution shall notify the authorized users based on their assigned permissions; AC 4 Given a user lacks permission to view an event update, When the update occurs, Then the solution shall display the update only to authorized users.; AC 5 Given updated event information is displayed, When the user reviews it, Then the solution shall make the current event information immediately visible;		
8082	Event Update Navigation	As a Dispatcher, I want the solution to provide the user the option of specifying the CFS event to update by entering the call sign of any assigned unit or by entering the incident number, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a dispatcher needs to specify a CFS event to update, When the dispatcher enters the call sign of any assigned unit, Then the solution shall identify the corresponding CFS event; AC 2 Given a dispatcher needs to specify a CFS event to update, When the dispatcher enters the incident number, Then the solution shall identify the corresponding CFS event; AC 3 Given an entered call sign or incident number does not match an event, When the dispatcher submits it, Then the solution shall indicate that no matching event was found; AC 4 Given a matching CFS event is identified, When the dispatcher proceeds, Then the solution shall make the event available for update;		
8149	Supplemental Data Entry Navigation	As a Dispatcher, I want the solution to provide a method for accessing supplemental data entry by event number or assigned unit, so that I can navigate to and enter supplemental information for an active event.	AC 1 Given an active event, When a dispatcher accesses supplemental data entry by event number, Then the solution shall navigate to the supplemental data entry for that event; AC 2 Given an active event, When a dispatcher accesses supplemental data entry by assigned unit, Then the solution shall navigate to the supplemental data entry for the associated event; AC 3 Given an entered event number or unit does not match an active event, When the dispatcher submits it, Then the solution shall indicate that no matching active event was found; AC 4 Given the supplemental data entry is accessed, When the dispatcher enters information, Then the solution shall apply the information to the correct event;		
8150	CAD Event Information Update Navigation	As a Dispatcher, I want the solution to provide a method for accessing and updating information previously entered into a CAD event by event number or assigned unit, so that I can locate and maintain event information.	AC 1 Given information previously entered into a CAD event, When a dispatcher accesses it by event number, Then the solution shall retrieve the event information for review and update; AC 2 Given information previously entered into a CAD event, When a dispatcher accesses it by assigned unit, Then the solution shall retrieve the associated event information for review and update; AC 3 Given an entered event number or unit does not match an event, When the dispatcher submits it, Then the solution shall indicate that no matching event was found; AC 4 Given previously entered information is updated, When the update is saved, Then the solution shall record the change in the event history;		
8164	CFS Update Identification and Retrieval	As a Dispatcher, I want the solution to distinguish newly received or updated CFS information from previously viewed information and provide a method, limited to an Update function, to retrieve the updated event, so that I can identify and review the latest event information.	AC 1 Given newly received or updated CFS information, When it is presented, Then the solution shall distinguish the new or updated information from previously viewed information; AC 2 Given updated CFS information exists, When a dispatcher uses the Update function, Then the solution shall retrieve the updated event; AC 3 Given the dispatcher reviews the updated information, When it is displayed, Then the solution shall allow the dispatcher to identify the latest event information; AC 4 Given updated information has been reviewed, When the dispatcher acknowledges it, Then the solution shall update the distinction to reflect reviewed status;		
8167	CFS Event Update Notifications	As an Authorized User, I need the solution to provide configurable visual or audible notifications when information is added to or changed in a CFS event, so that I can identify and review important event updates.	AC 1 Given configurable visual or audible notifications, When information is added to or changed in a CFS event, Then the solution shall provide the configured notification; AC 2 Given a notification is presented, When an Authorized User reviews it, Then the solution shall allow the user to identify and review the event update; AC 3 Given notification behavior is configured, When an Authorized User changes it, Then the solution shall apply the updated notification behavior; AC 4 Given a user acknowledges a notification, When the acknowledgment occurs, Then the solution shall clear the notification indication;		

8211	Command-Line CAD Event Entry	As a Dispatcher, I want the solution to support keyboard-driven, command-style event entry using configurable hotkeys and syntax, with a form-based entry alternative, so that I can create and update incidents while maintaining a usable fallback for less frequent or complex transactions.	AC 1 Given keyboard-driven, command-style event entry with configurable hotkeys and syntax, When a dispatcher enters or updates an incident using commands, Then the solution shall process the keyboard-driven command entry; AC 2 Given a form-based entry alternative is available, When a dispatcher chooses the form-based method, Then the solution shall provide the form-based entry alternative; AC 3 Given configurable hotkeys and syntax are defined, When an Authorized User configures them, Then the solution shall persist the hotkey and syntax configuration; AC 4 Given an invalid command or syntax is entered, When the dispatcher submits it, Then the solution shall identify the invalid entry; AC 5 Given an invalid command or syntax is entered, When the dispatcher submits it, Then the solution shall prevent an erroneous transaction; AC 6 Given a command-style or form-based entry is completed, When the transaction is submitted, Then the solution shall create or update the incident regardless of the entry method;		
8228	Persistent Time-of-Day Clock Display	As a Call-Taker or Dispatcher, I want the solution to display a persistent time-of-day clock that is accessible from every screen and shown in 24-hour (military) time, so that the current time is always available at a glance during operations.	AC 1 Given any CAD screen is displayed, When a call-taker or dispatcher is operating CAD, Then the solution shall display a persistent time-of-day clock that remains accessible from every screen.; AC 2 Given the clock is displayed, When time elapses, Then the solution shall update the displayed time in real time.; AC 3 Given the clock is displayed, When the time is presented, Then the solution shall present the time in 24-hour format.; AC 4 Given the solution uses a synchronized time source, When the clock is displayed, Then the solution shall present time consistent with the synchronized source.; AC 5 Given an authorized administrator configures the clock, When the configuration is saved, Then the solution shall apply the configured display settings while retaining 24-hour format.;		
8229	Per-User Display Personalization	As a Dispatcher or Authorized User, I want the solution to allow me to set and retain my own display preferences with at minimum font size, sort order, and color coding, so that each user can tailor the interface to individual operational needs.	AC 1 Given an Authorized User sets display preferences with font size, sort order, and color coding, When the preferences are saved, Then the solution shall persist the preferences for that user.; AC 2 Given a user has saved display preferences, When the user logs on, Then the solution shall apply that user's preferences to the display.; AC 3 Given a user changes a display preference, When the change is saved, Then the solution shall apply the updated preference to the user's subsequent sessions.; AC 4 Given user-level preferences are set, When they are applied, Then the solution shall apply them without altering other users' preferences or configured agency defaults.; AC 5 Given an Authorized User sorts a queue or list by a personal choice, When the sort is applied, Then the solution shall retain the user's selected sort order according to configured rules.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 09: Implementation, Transition & Adoption					
7909	Non-Production Test Environment	As a System Administrator, I want access to a regularly updated non-production test environment, so that staff can train, test configuration changes, and evaluate enhancements without affecting production.	AC 1 Given a non-production environment is available, When authorized staff access the environment, Then they shall be able to perform approved training and testing activities without affecting production.; AC 2 Given approved configuration changes are being evaluated, When the changes are applied in the non-production environment, Then the changes shall remain isolated from production.; AC 3 Given the environment requires updates, When the defined update process is performed, Then the solution shall maintain the non-production environment at the required current configuration.;		
7910	Vendor Upgrade and Enhancement Management	As a System Administrator, I want a controlled process for vendor upgrades and enhancements, so that new functionality can be introduced with minimal operational disruption.	AC 1 Given a vendor upgrade or enhancement is proposed, When the controlled upgrade process is initiated, Then the solution shall document and evaluate the change before production implementation.; AC 2 Given an upgrade has been approved for implementation, When the change is deployed, Then the solution shall complete the testing and validation activities before production use.; AC 3 Given an upgrade cannot be successfully implemented, When the defined rollback condition is met, Then the solution shall support the approved rollback process.;		
7911	Legacy Data Migration	As a System Administrator, I want legacy CAD/RMS data mapped and migrated to the successor solution, so that I can access and maintain historical records.	AC 1 Given legacy CAD/RMS records are identified for migration, When the migration process is executed, Then the solution shall map the records to the successor solution's approved data structures.; AC 2 Given a legacy record has a corresponding successor data element, When the record is migrated, Then the solution shall populate the mapped information in the successor field.; AC 3 Given required historical records have been migrated, When an Authorized User searches the successor solution, Then the migrated records shall be available according to access permissions.;		
7912	Legacy Data Cleansing	As a System Administrator, I want legacy data cleansed before migration, so that duplicate, invalid, or incomplete records do not compromise successor data quality.	AC 1 Given legacy data contains duplicate records, When the data-cleansing process is executed, Then the solution shall identify duplicate records according to defined rules.; AC 2 Given legacy data contains invalid or incomplete information, When cleansing is performed, Then the solution shall identify the records for correction, exclusion, or approved treatment.; AC 3 Given data has been cleansed, When the migration dataset is validated, Then the dataset shall meet the defined data-quality requirements before production migration.;		
7913	Migration Testing	As a System Administrator, I want to conduct migration test runs using legacy data, so that migration issues can be identified, validated, and corrected before production conversion.	AC 1 Given a migration test run is scheduled, When the test migration is executed using approved legacy data, Then the solution shall produce a test migration result.; AC 2 Given migration errors occur during a test run, When the results are reviewed, Then the errors shall be identifiable for correction.; AC 3 Given corrections have been made to migration mappings or data, When another test run is executed, Then the corrected results shall be available for validation.;		
7914	Legacy System Continuity	As a System Administrator, I want the solution to support continued operation of the legacy system during the transition to the replacement solution and preserve all previously stored data if rollback to a prior application version is required due to a failure, so that essential operations can continue and existing data remains complete and accessible during recovery.	AC 1 Given the successor solution is not yet ready for a required operational function, When authorized users perform that function during the transition period, Then the required legacy-system capability shall remain available.; AC 2 Given the transition period has ended and the successor function is operational, When legacy continuity is no longer required, Then the legacy function may be retired according to the approved transition plan.;		

7915	User Acceptance Testing	As an Authorized User, I want vendor-provided UAT test cases mapped to approved user stories and requirements, so that delivered functionality can be validated before deployment.	AC 1 Given vendor-provided UAT test cases are delivered, When the test cases are reviewed, Then each test case shall be traceable to an approved user story or requirement.; AC 2 Given a user story or requirement has UAT coverage, When the traceability is reviewed, Then the associated test case shall be identifiable.; AC 3 Given a required user story or requirement has no UAT test case, When traceability is reviewed, Then the missing test coverage shall be identifiable.;		
7916	Requirements, Testing and Defect Traceability	As an Authorized User, I want the vendor to use the State of Vermont Azure DevOps (ADO) instance to document requirements decisions, trace requirements to tests, and track defects, so that requirements, testing, and defects remain traceable throughout the project lifecycle.	AC 1 Given a requirements decision is made, When the decision is documented, Then the vendor shall record the decision in the State of Vermont ADO instance.; AC 2 Given an approved requirement or user story has associated tests, When test traceability is documented, Then the ADO instance shall identify the relationship between the requirement and test.; AC 3 Given a defect is identified, When the defect is entered into ADO, Then the solution shall associate the defect with the configured requirement, user story, or test when traceability is available.; AC 4 Given a defect is resolved, When the resolution is recorded, Then the solution shall maintain the defect status and resolution information in ADO.;		
7917	Role-Based Training and Train-the-Trainer	As a Training Administrator, I want role-based training and train-the-trainer materials, so that users can perform assigned CAD/RMS functions.	AC 1 Given users have different CAD/RMS responsibilities, When training is developed, Then the solution shall organize training materials according to user roles.; AC 2 Given train-the-trainer materials are required, When the Training Administrator accesses the materials, Then the materials shall support delivery of role-based training.; AC 3 Given a user completes assigned training, When the training is completed, Then the solution shall record completion according to the defined training process.;		
7918	User Guides and Job Aids	As an Authorized User, I want current user guides and concise job aids for supported CAD/RMS functions, so that users can perform routine tasks and resolve common questions without vendor assistance.	AC 1 Given a supported CAD/RMS function has an approved user guide, When an Authorized User accesses the guide, Then the current guide shall be available.; AC 2 Given a routine task has a job aid, When an Authorized User accesses the job aid, Then concise instructions for the task shall be available.; AC 3 Given documentation is updated, When users access the documentation, Then the solution shall present the current approved version.;		
7919	Agency Readiness and Transition	As an Authorized User, I want the solution to support agency readiness activities with training, communications, testing, and transition planning, so that participating career and volunteer agencies are prepared to use the new system.	AC 1 Given an agency is scheduled to transition to the solution, When readiness activities are planned, Then the solution shall identify training, communications, testing, and transition activities.; AC 2 Given participating agencies include career or volunteer organizations, When readiness activities are conducted, Then the solution shall include the agencies according to the approved readiness plan.; AC 3 Given readiness activities are completed, When readiness is assessed, Then completion status and identified outstanding activities shall be available for review.;		
7938	Cutover, Rollback and Legacy Retirement	As a System Administrator, I want a phased cutover, rollback, and legacy retirement process, so that the new solution can be implemented while maintaining operational continuity.	AC 1 Given the successor solution is ready for phased implementation, When a cutover phase is initiated, Then the solution and transition process shall follow the approved cutover plan.; AC 2 Given a rollback condition occurs, When the condition is declared according to the approved process, Then the transition shall support rollback to the designated operational state.; AC 3 Given the successor solution has completed an approved transition phase, When legacy retirement criteria are met, Then the solution shall retire the legacy components according to the approved plan.; AC 4 Given a cutover or rollback is performed, When the transition activity is completed, Then the solution shall maintain required operational continuity.;		
7962	Training and Test Environment	As an Authorized User, I want an isolated training and test environment that uses approved production-equivalent configuration without affecting production operations, so that users can train and proposed changes can be validated before deployment.	AC 1 Given an isolated training and test environment is available, When an Authorized User performs training or testing, Then the solution shall preserve production data and configuration.; AC 2 Given the environment requires production-equivalent configuration, When the environment is refreshed or maintained, Then the approved production-equivalent configuration shall be available.; AC 3 Given a proposed change is being evaluated, When the change is implemented in the test environment, Then the change shall remain isolated from production until approved for deployment.;		
8044	Agency Adoption and Usage Reporting	As a Program Manager, I want the solution to report active user accounts by agency against an approved expected-user baseline, so that career-agency adoption can be measured and verified following cutover.	AC 1 Given an approved expected-user baseline per agency, When a program manager generates the adoption report, Then the solution shall report active user accounts by agency against the baseline; AC 2 Given the report is generated following cutover, When the report is produced, Then the solution shall express adoption relative to the Act 78 program target; AC 3 Given active user account data changes, When the report is regenerated, Then the solution shall reflect the current active user counts; AC 4 Given a user lacks permission to view the adoption report, When the user attempts access, Then the solution shall prevent access; AC 5 Given the baseline is updated, When the report is generated, Then the solution shall use the current approved baseline;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 10: System Administration & Service Operations					
7850	Shift Assignment Management	As a System Administrator, I want to assign personnel and resources to the shift, so that staffing and resource organization remain accurate.	AC 1 Given personnel or resources require shift assignment, When an authorized administrator selects a shift, Then the solution shall associate the personnel or resources with the selected shift.; AC 2 Given a shift assignment already exists, When an authorized administrator changes the assignment, Then the solution shall update the current shift association.; AC 3 Given a personnel or resource assignment changes, When the change is saved, Then the solution shall retain the assignment history.; AC 4 Given a personnel or resource is inactive, When the administrator attempts to assign it to an active shift, Then the solution shall apply the configured eligibility rules.; AC 5 Given an Authorized User views shift staffing, When the shift is selected, Then the solution shall display the current personnel and resource assignments.;		
7856	Volunteer Responder Onboarding	As a System Administrator, I want to onboard volunteer responders using required identity, agency, role, and qualification information, so that approved volunteers can participate in operational workflows.	AC 1 Given a volunteer responder is being onboarded, When the administrator enters required identity information, Then the solution shall retain the identity information.; AC 2 Given required agency information is entered, When the administrator saves the onboarding record, Then the solution shall associate the responder with the agency.; AC 3 Given required role and qualification information is entered, When the onboarding record is validated, Then the solution shall evaluate the configured requirements.; AC 4 Given all required onboarding information is valid, When the administrator completes onboarding, Then the solution shall establish the volunteer responder's approved operational profile.; AC 5 Given required onboarding information is missing, When the administrator attempts to complete onboarding, Then the solution shall identify the missing information.;		

7888	Interface Monitoring and Recovery	As a System Administrator, I want to monitor interface status, activity, failures, and recovery, so that problems with system integrations can be identified and addressed before they disrupt operations.	AC 1 Given the solution operates configured interfaces, When an authorized administrator views interface monitoring, Then the solution shall display the current status and activity of each configured interface.; AC 2 Given a configured interface fails, When the failure is detected, Then the solution shall record the failure and notify the authorized administrator.; AC 3 Given a failed interface recovers, When connectivity is restored, Then the solution shall record the recovery and update the interface status.AC 4 Given an interface is unavailable, When transactions cannot be delivered, Then the solution shall retain the affected transactions for reprocessing per configured rules.; AC 5 Given an administrator reviews interface history, When the review occurs, Then the solution shall provide the recorded status, activity, failure, and recovery information.		
7907	Table-Driven and Directly Modifiable CAD Configuration	As a System Administrator, I want the solution to provide table-driven configuration parameters that authorized administrators can modify without custom development, where supported, so that approved solution and agency settings can be maintained to meet changing operational requirements.	AC 1 Given a configuration parameter is designated as table-driven, When an authorized System Administrator accesses the configuration, Then the solution shall allow the parameter to be modified without custom development where supported.; AC 2 Given an administrator modifies an approved configuration parameter, When the change is saved, Then the solution shall apply the new value to system behavior.; AC 3 Given an administrator enters an invalid configuration value, When the change is submitted, Then the solution shall prevent the invalid value from being saved.;		
7908	Vendor Support and Maintenance	As a System Administrator, I want access to vendor maintenance and production support through defined support channels, service levels, escalation procedures, and response targets, so that solution issues are resolved and ongoing operations are supported.	AC 1 Given a production or support issue requires vendor assistance, When the solution Administrator submits the issue through a defined support channel, Then the vendor shall accept the support request through the process.; AC 2 Given a support request has a service level or response target, When the request is submitted, Then the solution shall handle the request according to the defined service level and response target.; AC 3 Given an issue requires escalation, When the defined escalation condition is met, Then the support process shall provide the escalation path.;		
7920	System Capacity and Performance	As a System Administrator, I want the solution to support expected user and transaction volumes, so that performance remains within configured performance requirements as demand increases.	AC 1 Given the solution is operating at specified user and transaction volumes, When users and transactions are processed, Then the solution shall operate within the specified performance requirements.; AC 2 Given transaction volume increases within the specified expected range, When the increased workload is processed, Then the solution shall continue to meet configured performance requirements.; AC 3 Given performance requirements are exceeded during testing, When the results are evaluated, Then the condition shall be identifiable for remediation.;		
7927	Federated and Consolidated Operations	As a System Administrator, I want the solution to support participating agencies and jurisdictions in approved federated or consolidated operating models, so that statewide operations can be supported as organizational and governance requirements change.	AC 1 Given participating agencies operate under an approved federated or consolidated model, When authorized users access CAD/RMS, Then the solution shall support the approved organizational model.; AC 2 Given an agency or jurisdiction is configured for participation, When the agency uses CAD/RMS functions, Then the solution shall apply the configured organizational and access relationships.; AC 3 Given governance or organizational requirements change, When authorized configuration changes are implemented, Then the solution shall support the approved updated operating model.;		
7935	Cloud Hosting and Architecture	As a System Administrator, I want the solution to support the State's cloud-first hosting preference while accommodating approved exceptions for CJIS, latency, availability, or operational continuity, so that deployment aligns with State enterprise architecture and public-safety operational requirements.	AC 1 Given the solution is deployed in an approved hosting environment, When the deployment architecture is evaluated, Then the solution shall support the State cloud-first hosting preference.; AC 2 Given an approved exception is required for CJIS, latency, availability, or operational continuity, When the exception is documented and approved, Then the solution shall support the approved exception.; AC 3 Given the deployment architecture is changed, When the change is implemented, Then the resulting environment shall remain consistent with approved enterprise architecture requirements.;		
7960	Time and Administrative Synchronization	As a System Administrator, I want administrative interfaces to synchronize solution time and exchange approved administrative and resource information, so that timestamps and administrative data remain consistent across the CAD environment.	AC 1 Given solution time requires synchronization, When the solution performs time synchronization, Then CAD components shall use the approved synchronized time.; AC 2 Given approved administrative or resource information must be exchanged, When the exchange is initiated, Then the solution shall transmit the approved information.; AC 3 Given an administrative exchange is received, When the information is validated, Then the solution shall update the CAD administrative or resource information.; AC 4 Given synchronization or exchange fails, When the failure is detected, Then the solution shall identify the unsuccessful operation.;		
7989	Dynamic Personnel and Resource Scheduling	As a Dispatcher, I want the solution to create, maintain, and adjust personnel and resource rosters, schedules, and pre-assignments during shifts with assignments above normal complements, so that current staffing, resource availability, and assignments reflect operational conditions.	AC 1 Given an Authorized User creates a personnel or resource roster, When the roster is saved, Then the solution shall persist the roster with its assignments and effective period; AC 2 Given an active shift is in progress, When an Authorized User adjusts a roster, schedule, or pre-assignment, Then the solution shall apply the change; AC 3 Given an active shift is in progress, When an Authorized User adjusts a roster, schedule, or pre-assignment, Then the solution shall update current staffing and resource availability accordingly; AC 4 Given a unit is staffed above its normal complement, When an Authorized User records the above-complement assignment, Then the solution shall accept and reflect the assignment without rejecting it as invalid; AC 5 Given a roster change affects resource availability, When the change is saved, Then the solution shall update the affected resources' availability status in real time; AC 6 Given a user without configured permissions attempts to modify a roster or schedule, When the modification is submitted, Then the solution shall prevent the change; AC 7 Given roster or schedule changes are made during a shift, When an Authorized User reviews staffing history, Then the solution shall provide a record of the changes with the user and time of change;		

8045	Statewide Multi-Center CAD Operations	As a Dispatcher at any participating dispatch center, I want to operate within a single statewide CAD capability that maintains center-specific configuration, so that all participating centers share common incident, resource, and location data without requiring a separate solution per center.	AC 1 Given participating dispatch centers operate on a single statewide CAD capability, When a dispatcher at any center operates, Then the solution shall provide access to shared incident, resource, and location data; AC 2 Given center-specific configuration exists, When a dispatcher operates within a center, Then the solution shall apply that center's configuration; AC 3 Given multiple centers share the statewide capability, When they operate concurrently, Then the solution shall support all centers on the shared statewide capability.; AC 4 Given a center-specific configuration change is made, When it is saved, Then the solution shall apply the change to that center without affecting other centers' configurations; AC 5 Given shared data is updated at one center, When another center accesses it, Then the solution shall reflect the current shared incident, resource, and location data; AC 6 Given a dispatcher lacks permission for another center's data, When access is attempted, Then the solution shall enforce the access controls;		
8046	Dispatch Center Onboarding	As a System Administrator, I want to onboard a dispatch center by configuring its agencies, resources, response areas, and operational rules without vendor code changes, so that centers can be brought onto the statewide solution incrementally as the transition proceeds.	AC 1 Given a new dispatch center is being onboarded, When a system administrator configures its agencies, resources, response areas, and operational rules, Then the solution shall persist the center configuration; AC 2 Given a center is configured, When onboarding is completed, Then the solution shall bring the center onto the statewide solution without vendor code changes; AC 3 Given required onboarding configuration is incomplete, When the administrator attempts to activate the center, Then the solution shall identify the missing configuration; AC 4 Given required onboarding configuration is incomplete, When the administrator attempts to activate the center, Then the solution shall prevent activation; AC 5 Given centers are onboarded incrementally, When one center is added, Then the solution shall allow its activation without disrupting existing centers; AC 6 Given a user lacks permission to onboard a center, When the user attempts the configuration, Then the solution shall prevent the action; AC 7 Given center configuration changes are made, When they are saved, Then the solution shall record the change with the user and time;		
8048	Agency Participation and Entitlement Management	As a Program Administrator, I want to maintain each participating agency's participation status, entitlements, and effective dates, so that the solution reflects each agency's current participation and authorized access.	AC 1 Given a program administrator maintains agency participation information, When the administrator sets participation status, entitlements, and effective dates, Then the solution shall persist the agency's participation information; AC 2 Given an agency's effective dates are set, When the current date is within the effective period, Then the solution shall reflect the agency's active participation and authorized access; AC 3 Given an agency's participation lapses or ends, When the effective period ends, Then the solution shall update the agency's participation status accordingly; AC 4 Given required participation information is incomplete, When the administrator attempts to save it, Then the solution shall identify the missing information; AC 5 Given required participation information is incomplete, When the administrator attempts to save it, Then the solution shall prevent saving; AC 6 Given participation information changes, When an Authorized User reviews the history, Then the solution shall provide a record of the change and the user;		
8072	Dynamic Resource Capability Management	As a Dispatcher, I want the solution to allow system supervisors and other authorized users the ability to modify vehicle and resource capabilities without requiring a solution shutdown, so that the capability is available in accordance with approved operational requirements.	AC 1 Given a system supervisor or authorized user has configured permissions, When the user modifies vehicle and resource capabilities, Then the solution shall apply the modification without requiring a solution shutdown; AC 2 Given capability modifications are applied while the solution is running, When the change is saved, Then the solution shall reflect the updated capabilities without impacting operations; AC 3 Given a user lacks permission to modify vehicle or resource capabilities, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given a capability modification is made, When the change is saved, Then the solution shall record the change with the user and time;		
8114	Resource Type Configuration	As a System Administrator, I want the solution to support CAD configuration parameters to include functionality for specifying and modifying the type of resources available in the solution, so that the capability is available in accordance with approved operational requirements.	AC 1 Given CAD configuration parameters, When an authorized administrator specifies or modifies the type of resources available in the solution, Then the solution shall persist the resource type configuration; AC 2 Given resource types are configured, When resources are used in operations, Then the solution shall apply the configured resource types; AC 3 Given a user lacks permission to configure resource types, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given a resource type configuration is changed, When it is saved, Then the solution shall record the change with the user and time;		
8115	Incident Type Configuration	As a System Administrator, I want the solution to support CAD configuration parameters to include functionality for specifying the incident types that will be processed by the solution, so that the capability is available in accordance with approved operational requirements.	AC 1 Given CAD configuration parameters, When an authorized administrator specifies the incident types that will be processed by the solution, Then the solution shall persist the incident type configuration; AC 2 Given incident types are configured, When incidents are processed, Then the solution shall apply the configured incident types; AC 3 Given a user lacks permission to configure incident types, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given an incident type configuration is changed, When it is saved, Then the solution shall record the change with the user and time;		
8116	Agency Case Number Configuration	As a System Administrator, I want the solution to support CAD configuration parameters to include functionality for specifying the starting point and formats of case numbers created by the solution for each agency using the solution, so that the capability is available in accordance with approved operational requirements.	AC 1 Given CAD configuration parameters, When an authorized administrator specifies the starting point and format of case numbers for each agency, Then the solution shall persist the case number configuration per agency; AC 2 Given a case number configuration is defined for an agency, When the solution creates a case number for that agency, Then the solution shall apply the configured starting point and format; AC 3 Given a case number format is invalid, When the administrator attempts to save it, Then the solution shall identify the invalid configuration; AC 4 Given a case number format is invalid, When the administrator attempts to save it, Then the solution shall prevent saving; AC 5 Given the case number configuration is changed, When it is saved, Then the solution shall record the change with the user and time;		
8117	Resource Recommendation Configuration	As a System Administrator, I want the solution to support CAD configuration parameters to include functionality for modifying the display and functional characteristics of the solution's resource recommendations, so that the capability is available in accordance with approved operational requirements.	AC 1 Given CAD configuration parameters, When an authorized administrator modifies the display and functional characteristics of resource recommendations, Then the solution shall persist the recommendation configuration; AC 2 Given resource recommendation characteristics are configured, When recommendations are generated, Then the solution shall apply the configured display and functional characteristics; AC 3 Given a user lacks permission to modify recommendation characteristics, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given the recommendation configuration is changed, When it is saved, Then the solution shall record the change with the user and time;		

8118	Agency-Defined Data Elements	As a System Administrator, I want the solution to allow agencies to define additional data elements based on their operational requirements, so that the capability is available in accordance with approved operational requirements.	AC 1 Given an agency's operational requirements, When an Authorized User defines additional data elements, Then the solution shall allow the agency to define the additional data elements; AC 2 Given additional data elements are defined, When records are created or updated, Then the solution shall support the additional data elements; AC 3 Given a user lacks permission to define additional data elements, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given additional data elements are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8119	CAD Configuration Tables	As a System Administrator, I want the solution to provide configurable tables for defining and maintaining CAD objects with agencies, BOLOs, clearance and disposition codes, hazards, hydrants, incident and event types, fire stations, memos, messages, notifications, personnel, rosters, run cards and response plans, service types, personnel skills, SOPs, units, unit attributes, unit statuses, unit types, and vehicles, so that CAD operational data can be maintained through configurable solution tables without custom development.	AC 1 Given the solution provides configurable CAD tables, When an authorized administrator defines or maintains a CAD object, Then the solution shall retain the configured table values.; AC 2 Given configurable tables support defined CAD objects, When an administrator maintains them, Then the solution shall support agencies, BOLOs, clearance and disposition codes, hazards, hydrants, incident and event types, fire stations, memos, messages, notifications, personnel, rosters, run cards and response plans, service types, personnel skills, SOPs, units, unit attributes, unit statuses, unit types, and vehicles.; AC 3 Given configuration table values are changed, When the changes are saved, Then the solution shall apply the current approved values to CAD operations.; AC 4 Given a configuration change would create invalid or conflicting values, When the administrator attempts to save, Then the solution shall identify the invalid or conflicting information.; AC 5 Given a user is not authorized to maintain configuration tables, When the user attempts a change, Then the solution shall prevent the modification.;		
8175	Configurable Alerts and Timers	As a System Administrator, I want the solution to allow authorized administrators to define, configure, and modify system alerts and timers with alert or timer type, activation status, time interval, triggering conditions, and display behavior, so that alerts and timers reflect agency-defined operational conditions and notification requirements.	AC 1 Given an authorized administrator defines system alerts and timers, When the administrator configures the alert or timer type, activation status, time interval, triggering conditions, and display behavior, Then the solution shall persist the alert and timer configuration; AC 2 Given alerts and timers are configured, When a triggering condition occurs, Then the solution shall apply the configured alert or timer behavior; AC 3 Given a user lacks permission to configure alerts and timers, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given an invalid alert or timer configuration is entered, When the administrator attempts to save it, Then the solution shall identify the invalid configuration; AC 5 Given an invalid alert or timer configuration is entered, When the administrator attempts to save it, Then the solution shall prevent saving; AC 6 Given an alert or timer configuration is changed, When it is saved, Then the solution shall record the change with the user and time;		
8176	Configurable CAD Workstation Parameters	As a System Administrator, I want the solution to allow authorized administrators to configure workstation display settings and other system parameters, so that CAD workstations can be tailored to approved operational and user requirements.	AC 1 Given an authorized administrator configures workstation display settings and other system parameters, When the configuration is saved, Then the solution shall persist the workstation configuration; AC 2 Given workstation settings are configured, When a workstation is used, Then the solution shall apply the configured display settings; AC 3 Given a user lacks permission to configure workstation settings, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given workstation settings are changed, When the change is saved, Then the solution shall record the change with the user and time;		
8180	Emergency Contact Management	As a System Administrator, I want the solution to maintain an emergency contacts list that includes contact name, street address, city, state, ZIP code, telephone numbers, relationship, and configurable user-defined fields, so that emergency contact information can be maintained and accessed when needed.	AC 1 Given an emergency contacts list, When an Authorized User maintains it, Then the solution shall maintain contact name, street address, city, state, ZIP code, telephone numbers, relationship, and configurable user-defined fields; AC 2 Given emergency contact information exists, When it is needed, Then the solution shall make the information accessible; AC 3 Given required emergency contact information is incomplete, When the user attempts to save it, Then the solution shall identify the missing information; AC 4 Given required emergency contact information is incomplete, When the user attempts to save it, Then the solution shall prevent saving; AC 5 Given user-defined fields are configured, When contacts are maintained, Then the solution shall support the user-defined fields;		
8183	Dynamic Dispatcher Assignment	As a Supervisor, I want the solution to allow additional dispatchers to be assigned to one or more services or predefined geographic areas, so that dispatch coverage can be adjusted as operational demands change.	AC 1 Given operational demands change, When a supervisor assigns additional dispatchers to one or more services or predefined geographic areas, Then the solution shall apply the additional dispatcher assignments; AC 2 Given additional dispatchers are assigned, When the assignment is made, Then the solution shall adjust dispatch coverage accordingly; AC 3 Given a user lacks permission to assign dispatchers, When the user attempts it, Then the solution shall prevent the action; AC 4 Given a dispatcher assignment is changed, When it is saved, Then the solution shall record the change with the user and time; AC 5 Given an additional dispatcher is assigned to a service or area, When the assignment is active, Then the solution shall reflect the updated coverage;		
8184	Configurable Messaging Address Book	As a System Administrator, I want the solution to maintain a centralized address book for messaging and allow authorized users to configure recipient device types, default devices, and message delivery by device, day, time, or response mode, so that messages are routed to the communication devices based on configured operational requirements.	AC 1 Given a centralized address book for messaging, When an Authorized User configures recipient device types, default devices, and message delivery by device, day, time, or response mode, Then the solution shall persist the address book configuration; AC 2 Given messaging configuration exists, When a message is sent to a recipient, Then the solution shall route the message to the device based on the configured rules; AC 3 Given a recipient has a default device, When no specific device is selected, Then the solution shall deliver the message to the default device; AC 4 Given a user lacks permission to configure the address book, When the user attempts the change, Then the solution shall prevent the modification; AC 5 Given the messaging configuration is changed, When it is saved, Then the solution shall apply the updated routing to subsequent messages;		
8190	CFS Parameter Configuration	As a System Administrator, I want the solution to allow authorized administrators to configure CFS event parameters with dispositions, priorities, and other event-related values, so that CAD workflows reflect approved operational requirements.	AC 1 Given an authorized administrator configures CFS event parameters with dispositions, priorities, and other event-related values, When the configuration is saved, Then the solution shall persist the CFS event parameters; AC 2 Given CFS event parameters are configured, When events are processed, Then the solution shall apply the configured parameters; AC 3 Given a user lacks permission to configure CFS event parameters, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given CFS event parameters are changed, When the change is saved, Then the solution shall apply the updated parameters to subsequent events;		

8191	CAD Display and Interface Configuration	As a System Administrator, I want the solution to allow authorized administrators to configure the appearance and operational behavior of CAD windows and menus with sort order, layout, colors, and fonts, so that the user interface supports agency-specific operational needs.	AC 1 Given an authorized administrator configures the appearance and operational behavior of CAD windows and menus with sort order, layout, colors, and fonts, When the configuration is saved, Then the solution shall persist the interface configuration; AC 2 Given the interface configuration is applied, When a user operates CAD, Then the solution shall present the windows and menus according to the configured settings; AC 3 Given a user lacks permission to configure the interface, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given the interface configuration is changed, When the change is saved, Then the solution shall apply the updated appearance and behavior;		
8694	Attribute Permission Management	As an Agency Administrator, I need the CAD solution to allow authorized agency representatives to manage unit attributes through delegated permissions that are limited to their agency and assigned responsibilities, so that agencies can maintain unit attribute information while enforcing the principle of least privilege.	AC 1 Given an authorized agency representative has delegated permissions to manage unit attributes, When the representative accesses unit attribute management, Then the CAD solution shall permit access only to the unit attributes within the representative's agency and assigned responsibilities.; AC 2 Given an agency representative attempts to view or modify unit attributes outside their authorized agency or delegated responsibilities, When the representative submits the request, Then the system shall deny the unauthorized access or modification.; AC 3 Given an authorized agency representative creates or updates a unit attribute, When the change is saved, Then the system shall validate the attribute against applicable configuration rules and retain the updated information.; AC 4 Given a unit attribute is managed by an authorized agency representative, When the representative's delegated permissions are changed or revoked, Then the system shall enforce the updated permissions for subsequent access and management actions.; AC 5 Given an authorized agency representative creates, updates, or deletes a unit attribute, When the action is completed, Then the system shall retain the applicable user, agency, action, and date and time in the audit history.		
8695	Mutual Aid Agreement Management Permissions	As a System Administrator, I need the CAD solution to delegate mutual aid agreement configuration and maintenance permissions to authorized representatives of participating agencies, with access restricted to their agency and assigned responsibilities, so that agencies can manage their mutual aid agreements while enforcing the principle of least privilege.	AC 1 Given a System Administrator is authorized to delegate mutual aid agreement management permissions, When the administrator assigns permissions to a participating agency representative, Then the CAD solution shall allow the administrator to define the representative's access based on the agency and assigned responsibilities.; AC 2 Given an authorized agency representative has delegated mutual aid agreement permissions, When the representative accesses agreement configuration and maintenance functions, Then the system shall permit access only to agreements and configuration elements within the representative's agency and assigned responsibilities.; AC 3 Given an agency representative attempts to view or modify mutual aid agreements or configuration elements outside their authorized agency or delegated responsibilities, When the representative submits the request, Then the system shall deny the unauthorized access or modification.; AC 4 Given an authorized agency representative creates or updates mutual aid agreement information, When the changes are saved, Then the system shall validate and retain the changes in accordance with applicable configuration rules and permissions.; AC 5 Given an agency representative's delegated permissions are modified or revoked, When the updated permissions take effect, Then the system shall enforce the revised access restrictions for subsequent agreement management activities.; AC 6 Given an authorized agency representative creates, updates, or deletes mutual aid agreement information, When the action is completed, Then the system shall retain the applicable user, agency, action, and date and time in the audit history.		
8802	Define and Maintain CAD Configuration Tables	As a System Administrator, I want configurable tables for defining and maintaining CAD objects, so that operational data is maintained without custom development.	AC 1 Given configurable tables for CAD objects, When an authorized administrator defines or maintains CAD objects such as agencies, BOLOs, clearance and disposition codes, hazards, hydrants, incident and event types, fire stations, memos, messages, notifications, personnel, rosters, run cards and response plans, service types, personnel skills, SOPs, units, unit attributes, unit statuses, unit types, and vehicles, Then the solution shall persist the configuration through the configurable tables.; AC 2 Given CAD objects are maintained through configurable tables, When the configuration is applied, Then the solution shall use the configured objects in operations without custom development.;		
8803	Validate and Control Configuration Table Changes	As a System Administrator, I want table changes validated and permission-controlled, so that configuration data stays accurate.	AC 1 Given required table information is incomplete, When the administrator attempts to save it, Then the solution shall identify the missing information.; AC 2 Given required table information is incomplete, When the administrator attempts to save it, Then the solution shall prevent saving.; AC 3 Given a user lacks permission to maintain configurable tables, When the user attempts the change, Then the solution shall prevent the modification.; AC 4 Given a configurable table entry is changed, When the change is saved, Then the solution shall record the change with the user and time.;		
8804	Protect Configuration Table Integrity	As a System Administrator, I want in-use table entries protected, so that deletions do not compromise data integrity.	AC 1 Given a configurable table entry is in use, When an administrator attempts to delete it, Then the solution shall identify the dependency.; AC 2 Given a configurable table entry is in use, When an administrator attempts to delete it, Then the solution shall prevent an action that would compromise data integrity.; AC 3 Given configurable table changes are made, When they are applied, Then the solution shall reflect the updated objects in subsequent operations.;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 11: Continuity, Availability & Recovery					
7811	Disconnected Operations	As an Officer, I want to perform defined essential functions when network connectivity is unavailable, so that, when working offline, data is preserved and auto uploaded when service is restored.	AC 1 Given an officer has no network connectivity, When the officer performs a supported essential function, Then the solution shall permit the function using approved offline capabilities.; AC 2 Given information is created while offline, When connectivity is restored, Then the solution shall identify the locally stored information for synchronization.; AC 3 Given locally stored information is synchronized, When the central system receives the information, Then the solution shall update the records.; AC 4 Given an offline transaction cannot be synchronized, When synchronization fails, Then the solution shall identify the transaction requiring attention.; AC 5 Given the same offline information has already been synchronized, When synchronization is attempted again, Then the solution shall prevent unnecessary duplicate records according to configured rules.;		

7819	Connectivity Restoration and Data Synchronization	As an Officer, I want the solution to synchronize locally stored changes when connectivity is restored, so that field information is transferred to the central system without unnecessary re-entry.	AC 1 Given an officer has created or changed supported information while offline, When network connectivity is restored, Then the solution shall identify the locally stored changes for synchronization.; AC 2 Given locally stored changes are eligible for synchronization, When synchronization begins, Then the solution shall transmit the changes to the central system.; AC 3 Given the central system accepts synchronized changes, When synchronization completes, Then the corresponding central records shall reflect the changes.; AC 4 Given a synchronization conflict occurs, When the solution detects the conflict, Then the solution shall identify the conflict according to configured rules.; AC 5 Given synchronization completes successfully, When the officer views the affected record, Then the synchronized information shall be available without unnecessary manual re-entry.;		
7921	Business Continuity and Recovery	As a System Administrator, I want documented business continuity and recovery capabilities for CAD/RMS operations, so that critical services and information can be restored following disruption.	AC 1 Given a disruption affects a critical CAD/RMS service, When the business continuity process is invoked, Then the documented continuity capabilities shall identify the recovery actions.; AC 2 Given a recoverable disruption has occurred, When the recovery process is executed, Then the solution shall restore critical services according to the defined recovery requirements.; AC 3 Given recovery has been completed, When authorized users access the restored system, Then required information and functions shall be available according to the recovery requirements.;		
7922	System Availability	As a System Administrator, I want the production solution to meet the specified availability target, so that public-safety operations remain available for use.	AC 1 Given the production solution is operating during the defined measurement period, When availability is measured, Then the solution shall calculate the measured availability according to the specified availability methodology.; AC 2 Given an unplanned outage occurs, When the outage is recorded, Then the solution shall include the outage duration in availability measurements.; AC 3 Given the defined availability target is evaluated, When the measurement period is complete, Then the solution shall compare the resulting availability with the specified target.;		
7950	PSAP Relocation and Continuity Operations	As a Supervisor, I want the solution to support planned or emergency PSAP relocation and continuity operations, so that essential CAD functions and required integrations can continue during a relocation or operational disruption.	AC 1 Given a PSAP relocation or continuity event has been declared, When the approved continuity process is activated, Then required CAD functions shall be available from the designated operating location.; AC 2 Given required CAD integrations are part of the continuity configuration, When continuity operations begin, Then the integrations shall remain available or operate through the approved continuity method.; AC 3 Given normal PSAP operations are restored, When the recovery process is completed, Then CAD operations shall return to the designated normal operating state.;		
8030	CAD Redundancy and Failover	As a System Administrator, I want the solution to provide redundant system components and automatic failover capabilities, so that CAD operations and critical incident information remain available during solution or component failures and support continuity of dispatch and mutual aid operations.	AC 1 Given CAD redundancy is configured, When a primary system component fails, Then the solution shall continue mutual and automatic aid operations without interruption of dispatch capability; AC 2 Given a failover occurs, When operations continue on the redundant system, Then the solution shall preserve active incident and resource data; AC 3 Given the failed component is restored, When normal operation resumes, Then the solution shall synchronize data so no incident records are lost; AC 4 Given a failover occurs, When the event is processed, Then the solution shall record the failover for administrator review; AC 5 Given redundancy is active, When operations continue during a failure, Then the solution shall maintain mutual and automatic aid dispatching;		
ADO ID	**Epic**	**Title**	**User Story**	**Availability?**	**Vendor Comments**
EPIC 12: Security, Identity & Access Management					
7854	User and Responder Account Management	As a System Administrator, I want to create, update, maintain, and deactivate user and responder accounts and associated attributes, so that authorized access and operational assignments remain current and can be established, maintained, or removed.	AC 1 Given an authorized administrator creates a user account, When the required account information is entered, Then the solution shall create the account according to configured rules.; AC 2 Given an authorized administrator updates account attributes, When the changes are saved, Then the solution shall retain the updated attributes.; AC 3 Given a responder requires operational attributes, When the administrator associates the attributes with the account, Then the solution shall retain the associations.; AC 4 Given an account is no longer authorized for access, When the administrator deactivates the account, Then the solution shall prevent further access according to security rules.; AC 5 Given an account is deactivated, When authorized users review account history, Then the deactivation information shall be available.; AC 6 Given an inactive account is reactivated by an authorized administrator, When the reactivation is completed, Then the account shall be available according to the current access configuration.;		
7902	Single Sign-On and Multi-Factor Authentication	As a System Administrator, I want the solution to integrate with State-approved single sign-on and multi-factor authentication services, so that user authentication meets State security requirements.	AC 1 Given a user attempts to access CAD/RMS, When the user authenticates through the State-approved single sign-on service, Then the solution shall validate the user's identity through the approved authentication service.; AC 2 Given multi-factor authentication is required for the user's access, When the user attempts to authenticate, Then the solution shall require the configured additional authentication factor.; AC 3 Given authentication is unsuccessful, When the authentication service rejects the credentials or required factor, Then the solution shall deny access.; AC 4 Given authentication is successful and the user is authorized, When authentication is completed, Then the solution shall grant access to the functions permitted for that user.;		
7903	User ID Recovery and Password Reset	As an Authorized User, I want to securely retrieve my user ID and reset my password, so that I can regain access to my account without unnecessary administrative intervention.	AC 1 Given an Authorized User has forgotten or needs to retrieve their user ID, When the user initiates the approved recovery process, Then the solution shall provide the user ID using the configured verification process.; AC 2 Given an Authorized User requests a password reset, When the user completes the required identity verification, Then the solution shall allow the user to establish a new password.; AC 3 Given identity verification fails, When the user attempts account recovery, Then the solution shall prevent disclosure or reset of protected account credentials.;		
7906	CJIS and Sensitive Information Protection	As a System Administrator, I want the solution to protect CJIS and other sensitive information using required access, handling, encryption, and monitoring controls, so that protected public-safety information remains secure.	AC 1 Given a user accesses CJIS or other sensitive information, When the user requests access, Then the solution shall enforce the authorization and access controls.; AC 2 Given sensitive information is transmitted or stored, When encryption is required, Then the solution shall protect the information using the required encryption controls.; AC 3 Given a security-sensitive activity occurs, When the activity is subject to monitoring requirements, Then the solution shall record the security event information.; AC 4 Given a user does not have authorization to access protected information, When the user attempts access, Then the solution shall deny the unauthorized access.;		

7934	SIEM Security Event Integration	As a System Administrator, I want required CAD/RMS security events to be forwarded to the State-designated SIEM, so that security activity can be centrally monitored, investigated, and retained for audit purposes.	AC 1 Given a CAD/RMS security event meets the defined forwarding criteria, When the event occurs, Then the solution shall forward the required event information to the State-designated SIEM.; AC 2 Given the SIEM receives a forwarded event, When the event is processed, Then the event shall contain the required information for monitoring and investigation.; AC 3 Given SIEM forwarding fails, When the failure is detected, Then the solution shall identify the unsuccessful forwarding event according to configured monitoring requirements.;		
7939	Security-Sensitive Activity and Configuration Audit	As a System Administrator, I want the solution to record security-sensitive activities and solution modifications with the information required to identify the activity, user or source, date and time, modification performed, and the prior value of modified configuration data, so that security events and system configuration changes can be monitored, investigated, and audited.	AC 1 Given a security-sensitive activity or solution modification occurs, When the activity is processed, Then the solution shall record the event.; AC 2 Given a configuration value is modified, When the modification is recorded, Then the audit information shall identify the user or source, date and time, modification performed, and prior value.; AC 3 Given an Authorized User reviews recorded security activity, When the audit information is retrieved, Then the event history shall be available for monitoring and investigation.; AC 4 Given an unauthorized modification is attempted, When the attempt occurs, Then the solution shall prevent the unauthorized modification.; AC 5 Given an unauthorized modification is attempted, When the attempt occurs, Then the solution shall record the security event where required.;		
7955	Secure Remote Access	As a System Administrator, I want secure remote access to authorized CAD/RMS information and functions from approved devices, networks, or locations, so that authorized personnel can perform required work outside the primary communications center.	AC 1 Given a user is authorized for remote CAD/RMS access, When the user connects from an approved device, network, or location, Then the solution shall authenticate and authorize the user.; AC 2 Given the user's remote access is authorized, When the user accesses CAD/RMS, Then the solution shall provide the functions and information permitted by the user's authorization.; AC 3 Given the device, network, or location is not approved, When remote access is attempted, Then the solution shall prevent access according to configured security controls.;		
7966	Security Roles and Permission Sets	As a System Administrator, I want to create and maintain approved security roles and permission sets, so that access privileges can be defined and maintained according to authorized responsibilities.	AC 1 Given a new security role is required, When a Security Administrator creates the role, Then the solution shall allow the administrator to define the approved permissions for the role.; AC 2 Given an existing role requires modification, When an authorized administrator updates the permission set, Then the solution shall retain the updated permissions.; AC 3 Given a role is no longer approved, When the administrator disables or removes the role according to the approved process, Then the solution shall revoke access to the functions associated with the removed role.;		
7967	User Role Assignment and Authorization	As a System Administrator, I need to assign users to approved roles and enforce the permissions associated with those roles, so that users can access only the functions and information authorized for their specific agency and responsibilities with configuration of response plans, units, and agency-specific configurations.	AC 1 Given an active user requires access to CAD/RMS functions, When a Security Administrator assigns the user to an approved role, Then the solution shall associate the user with that role.; AC 2 Given a user has one or more approved roles, When the user accesses CAD/RMS, Then the solution shall enforce the permissions associated with those roles.; AC 3 Given a user does not have permission for a function or information, When the user attempts access, Then the solution shall deny the unauthorized access.;		
7968	Unique User Identity	As a System Administrator, I want each active user to have a unique system identity, so that user access and activity can be attributed to the individual.	AC 1 Given a new user account is created, When the account is activated, Then the solution shall assign or require a unique system identity.; AC 2 Given an active user identity already exists, When an administrator attempts to create a duplicate identity, Then the solution shall prevent creation of the duplicate active identity.; AC 3 Given a user performs an auditable activity, When the activity is recorded, Then the solution shall attribute the activity to the user's unique identity.;		
7969	User Authentication	As an Authorized User, I want the solution to authenticate my identity before granting access, so that solution functions and protected information are available only to authenticated users with authorization.	AC 1 Given an Authorized User has an active account, When the user submits valid authentication credentials, Then the solution shall authenticate the user's identity before granting access.; AC 2 Given authentication succeeds but the user lacks required authorization, When access is requested, Then the solution shall deny access to the unauthorized function or information.; AC 3 Given authentication fails, When the user attempts access, Then the solution shall deny access to protected CAD/RMS functions and information.;		
8009	Performance Metrics Access and PII Redaction	As a System Administrator, I want role-based access controls and PII redaction in performance and metric views, so that authorized operational metrics can be accessed while sensitive information is protected.	AC 1 Given role-based access controls are configured for performance and metric views, When a user accesses a metric view, Then the solution shall grant or deny access according to the user's role; AC 2 Given a metric view contains PII subject to redaction, When an authorized but restricted user views it, Then the solution shall redact the PII; AC 3 Given a user has full authorization, When the user views performance metrics, Then the solution shall present the authorized operational metrics without redaction; AC 4 Given a user lacks permission for a metric view, When the user attempts access, Then the solution shall deny access; AC 5 Given access to protected metric views occurs, When a user views the data, Then the solution shall log the access for audit purposes; AC 6 Given access control configuration changes, When an administrator saves the change, Then the solution shall apply the updated access controls to subsequent access;		
8047	CJIS Policy Compliance Management	As a System Administrator, I want the solution to identify the CJIS Security Policy version it is assessed against and to accommodate policy revisions without re-architecture, so that CJIS compliance is maintained as the policy is revised through implementation and steady state.	AC 1 Given the solution is assessed against a CJIS Security Policy version, When a security administrator views compliance information, Then the solution shall identify the CJIS Security Policy version it is assessed against; AC 2 Given the CJIS Security Policy is revised, When the revision is adopted, Then the solution shall accommodate the policy revision without re-architecture; AC 3 Given a new CJIS policy version is configured, When it is saved, Then the solution shall reflect the updated assessed version; AC 4 Given a user lacks permission to view or change CJIS compliance settings, When the user attempts access, Then the solution shall prevent the action; AC 5 Given the assessed CJIS version changes, When the change is made, Then the solution shall record the change for audit purposes;		

8112	CAD Transaction and Configuration Audit	As a System Administrator, I want the solution to maintain a protected CAD transaction audit database that records system messages and transactions involving CAD configuration parameters and configuration files with the date and time, sending and receiving user and workstation IDs, message contents, and user actions limited to viewing, printing, adding, editing, or deleting configuration information, so that CAD transactions and configuration changes are traceable and auditable.	AC 1 Given CAD system messages and configuration transactions occur, When the transactions are processed, Then the solution shall record them in a protected CAD transaction audit database.; AC 2 Given a CAD configuration transaction is recorded, When the entry is created, Then the solution shall record the date and time, sending and receiving user and workstation IDs, and message contents.; AC 3 Given a user acts on configuration information, When the action is viewing, printing, adding, editing, or deleting, Then the solution shall record the user action.; AC 4 Given the CAD transaction audit database contains records, When an authorized user accesses the audit information, Then the solution shall make the records available according to configured access rules.; AC 5 Given the audit database is protected, When an unauthorized user attempts to modify audit records, Then the solution shall prevent the modification.;		
8113	External Query Transaction Audit	As a System Administrator, I want the solution to record user- and system-initiated queries to interfaced systems and databases with NCIC and Nlets, in the CAD transaction audit database with associated details limited to the date and time, user ID, workstation ID, query, and response information where available, so that external query activity can be traced, reviewed, and audited for security, operational oversight, and compliance.	AC 1 Given user and system generated queries are sent to interfaced systems and databases limited to NCIC and Nlets, When a query occurs, Then the solution shall capture the query messages in the CAD transaction audit database; AC 2 Given a query is captured in the audit database, When it is recorded, Then the solution shall record associated information with date and time stamp, user ID, and workstation ID; AC 3 Given a response is received from an interfaced system, When it is processed, Then the solution shall capture the associated transaction information; AC 4 Given captured query transactions exist, When an Authorized User reviews them, Then the solution shall provide the recorded query transactions for audit purposes; AC 5 Given an unauthorized user attempts to alter captured query transactions, When the attempt occurs, Then the solution shall prevent the modification;		
8132	Agency and Role-Based Field Access	As a System Administrator, I want the solution to enable CAD users to be configurable by agency and role to the field level, so that the capability is available in accordance with approved operational requirements.	AC 1 Given CAD users are configurable by agency and role, When an administrator configures a user to the field level, Then the solution shall apply the configured agency and role to the user; AC 2 Given a user is configured by agency and role, When the user operates, Then the solution shall enforce access according to the configured agency and role; AC 3 Given a user lacks permission to configure users, When the user attempts the change, Then the solution shall prevent the modification; AC 4 Given a user configuration is changed, When it is saved, Then the solution shall record the change with the user and time; AC 5 Given a user's agency or role configuration changes, When the change is applied, Then the solution shall enforce the updated configuration on subsequent access;		
8174	CAD Transaction Audit Data Protection	As a System Administrator, I want the solution to prevent unauthorized changes to the contents of the CAD/RMS transaction audit database, so that audit records remain protected and reliable for historical and compliance purposes.	AC 1 Given the CAD transaction audit database, When an unauthorized change to its contents is attempted, Then the solution shall prevent the change; AC 2 Given audit records exist, When they are accessed, Then the solution shall allow only authorized access while protecting the records' integrity; AC 3 Given an attempt to alter audit records occurs, When the attempt is made, Then the solution shall record the attempt; AC 4 Given the audit database is maintained, When records are stored, Then the solution shall keep the audit records reliable for historical and compliance purposes;		
8179	Sent Message Audit Logging	As a System Administrator, I want the solution to log all messages sent through the solution, so that message activity is traceable and available for auditing and review.	AC 1 Given messages are sent through the solution, When a message is sent, Then the solution shall log the message; AC 2 Given messages are logged, When an Authorized User reviews message activity, Then the solution shall make the logged messages available for auditing and review; AC 3 Given an unauthorized user attempts to alter the message log, When the attempt occurs, Then the solution shall prevent the modification; AC 4 Given a message is logged, When it is recorded, Then the solution shall capture the message details for traceability;		
8799	Record CAD Configuration Transactions	As a System Administrator, I want the solution to record CAD configuration transactions in a protected audit database, so that configuration changes are traceable.	AC 1 Given CAD configuration parameters and configuration files are changed, When the change occurs, Then the solution shall record the transaction in a protected CAD transaction audit database.; AC 2 Given a CAD configuration transaction is recorded, When it is logged, Then the solution shall capture the date and time, sending and receiving user and workstation IDs, message contents, and the user action.; AC 3 Given configuration information is viewed, printed, added, edited, or deleted, When the action occurs, Then the solution shall record the specific user action in the audit database.; AC 4 Given a configuration change is made, When it is recorded, Then the solution shall associate the audit record with the user and workstation that performed it.;		
8800	Protect and Retain Audit Records	As a System Administrator, I want audit records protected and retained, so that the audit trail stays intact.	AC 1 Given the audit database contains records, When an unauthorized user attempts to modify them, Then the solution shall prevent the modification.; AC 2 Given the audit database is maintained, When transactions are recorded, Then the solution shall retain the records in accordance with the configured retention requirements.;		
8801	Review CAD Audit Records	As a System Administrator, I want to review recorded audit transactions, so that configuration activity is traceable.	AC 1 Given an authorized user reviews the audit database, When the review occurs, Then the solution shall provide the recorded transactions for traceability.; AC 2 Given audit transactions are recorded, When an authorized user searches by user, date, or configuration item, Then the solution shall display the matching audit transactions.; AC 3 Given audit records are presented, When an authorized user reviews them, Then the solution shall present the audit records in read-only form.;		

8835	HIPAA Compliance and Access Controls	As an Authorized User, I want the solution to restrict Health Information (EMS/medical call data, EMD protocol data, 988 and mobile-crisis data, and any patient care or hospital data received) to roles with a defined need, hidden from all other roles by default, so that it is accessed and disclosed only as authorized, and all access can be audited.	AC 1 Given the State provides a role-permission matrix during implementation, When the Contractor configures the solution, Then the matrix shall be configurable by State administrators at the role, record-type and field level without vendor code changes, and the configured matrix shall be delivered as a reviewable report. AC 2 Given a user whose role is not granted Health Information (including all law-enforcement roles by default), When the user opens, searches, prints or exports an incident or person record, Then Health Information fields shall not be displayed, returned in search results, printed or exported, and the record shall indicate that restricted content exists. AC 3 Given a State administrator flags a record or field as restricted (juvenile, victim, sealed/expunged, 42 CFR Part 2), When any user without that specific permission attempts access, Then access shall be denied and logged, including for users who hold general Health Information access. AC 4 Given a user without permission needs emergency access, When the user invokes break-the-glass, Then the solution shall require a reason from a configurable list plus free text, grant time-limited access (configurable, default 60 minutes), and alert the designated administrators within 5 minutes. AC 5 Given any view, create, modify, print, export, disclosure or denied attempt involving Health Information or a restricted record, When the action occurs, Then the audit log shall record user ID, role, date/time, record ID, fields accessed, action, result (allowed/denied), break-the-glass reason if any, and source device/IP.AC 6 Given audit records exist, When an administrator runs an audit report, Then the solution shall produce it by user, by subject person, by record and by date range, exportable to CSV, and audit records shall be tamper-evident and retained per the State retention schedule. AC 7 Given an administrator changes a user's role or permissions, When the change is saved, Then it shall take effect on that user's next request, including in active sessions. AC 8 Given Health Information is sent to another agency or system through an interface, When the transmission occurs, Then only the fields mapped as permitted for that interface in the role-permission matrix shall be sent, and the disclosure shall be logged as in AC 5.AC 9 Given Health Information is stored or transmitted, When it is at rest or in transit, Then it shall be encrypted using FIPS 140-validated cryptography (TLS 1.2 or higher in transit; AES-256 or equivalent at rest), consistent with the CJIS Security Policy.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

PART 4a: NON-FUNCTIONAL REQUIREMENTS

The tables below list the State's Non-Functional Requirements. Indicate if your proposed solution complies in the "Comply" column.	**Yes**	the Solution **complies** with the stated requirement
Describe how the requirement is met in the "Vendor Description of Compliance" column.	**No**	the Solution **does not compy** with the stated requirement
	N/A	Feature is **not** available in the core solution, but can **provided with customization**.

AVAILABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8717	Availability	The solution must achieve a monthly uptime of at least 99.9%, excluding approved maintenance windows.		
8720	Backup and DR testing	The Contractor must perform backup, restore, and disaster recovery testing at least annually, and provide summary results to the State upon request.		
8718	NFR-02 Recovery targets	The Contractor must define and contractually commit to a recovery time objective (RTO) and a recovery point objective (RPO) for each production service, with an RTO of no more than 24 hours from contingency plan activation for each service that supports an essential business function designated by the State.		
8721	NFR-05 Protected backups	The solution must protect backup copies of critical data from alteration and deletion.		
8719	Resilience architecture	The solution must eliminate single points of failure within the provider-controlled boundary.		

COMPATIBILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8744	Bulk import and export	The solution must support bulk import and export for implementation, migration, and transition-out purposes.		
2100	EDGE NFR 3081: CAD RMS Device Compatibility	Mobile applications must support tablets, laptops, smartphones, vehicle-mounted terminals and alternative mobile devices (e.g., land mobile radio (LMR), portable and mobile radios that integrate broadband, cellular, WiFi, satellite access into the LMR radio.)		
8743	Interface specifications and versioning	The Contractor must publish and maintain the interface specifications, versioning rules, backward-compatibility expectations, and deprecation notice periods.		
1904	NFR-3005: Integration Architecture & Platform	The solution must integrate with State-supported enterprise integration platforms and middleware using approved architectural patterns to enable reliable, scalable, and governed data exchange.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1905	NFR-3006: Data Exchange Interfaces	The solution must support standardized, machine-readable interfaces for bidirectional data exchange with internal and external solutions, including real-time and batch-based integrations where appropriate.		
1906	NFR-3007: Data Integration Tooling	The solution must provide integration tooling, including adapters and transformation capabilities, to extract, transform, and load data from heterogeneous source solutions in support of integration requirements.		
1907	NFR-3010: State Network Integration	The solution must integrate with the State of Vermont's network using State-approved connectivity patterns, including DNS-based addressing, secure routing, and approved access paths.		
1908	NFR-3011: Standards-Based Protocols	The solution must use industry-standard networking and communication protocols, including TCP/IP and HTTPS, and must not require proprietary or non-standard networking mechanisms.		
1909	NFR-3014: Data Transfer Without Re-entry	The solution must support the transfer of data between systems without requiring manual re-entry, preserving data accuracy and consistency.		
1910	NFR-3015: Multi-Channel Access	The solution must provide services across approved access channels, including web interfaces, mobile applications, and APIs, to support internal and external stakeholders.		
1911	NFR-3016: Replication Support	The solution database must support data replication to external file formats and other relational database management solutions.		
1912	NFR-3017: Database Isolation	The solution database must accommodate separate database instances.		
1913	NFR-3018: Shared Data Methods	The Contractor must adhere to or establish common enterprise methods and tools for creating, maintaining, and accessing shared data.		
1914	NFR-3019: Flexible Enterprise Data Model	The solution must provide a flexible enterprise data model capable of representing complex relationships among internal solutions, external partners, intermediaries, clients, and providers, including support for complex hierarchies.		
1915	NFR-3020: Transformation Capability Spectrum	The solution must support a full spectrum of data transformations, including simple transformations, moderate complexity transformations, advanced transformations, and custom transformation development.		
1916	NFR-3021: Multi-Platform Operation	The solution must function correctly across supported hardware and software platforms, including approved operating solutions, browsers, and device types.		
1917	NFR-3022: Normalized Data Transformation	The solution must perform data transformations to and from normalized formats to support composability, reduce transformation complexity, and improve interoperability. The solution must support a federated normalization approach; use of a single canonical model is permitted but not required.		
1918	NFR-3023: Third-Party Developer Enablement	The Contractor must assist authorized third-party developers in securely retrieving approved data through documented interfaces in accordance with State requirements.		

1919	NFR-3024: Standards-Based API Design	The solution must implement integration interfaces using industry-standard protocols (e.g., REST over HTTPS) and machine-readable API specifications such as OpenAPI.		
1920	NFR-3025: No Proprietary Integration Mechanisms	The solution must not require proprietary or vendor?locked integration mechanisms that restrict portability or State control.		
1921	NFR-3026: API Gateway Compatibility	The Contractor must design integration services to support proxying, security, and governance through a centralized API gateway (e.g., AWS API Gateway) without requiring architectural redesign.		
1922	NFR-3031: Data Lake	All State data and required reference data must be delivered to the State's S3-compatible data lake at least once every 24 hours in an agreed upon format, schema, and transport mechanism, with failed deliveries logged and retried according to State incident management requirements.		
1923	NFR-3032: Data Lake Incremental / Reconciliation Metadata	Data delivered to the State's S3-compatible data lake must include metadata sufficient to support reconciliation and incremental ingestion, including dataset identifiers, extract timestamps, record counts, and when applicable, change indicators such as insert, update, and delete flags.		
8742	Standards-based integration	The solution must provide secure application programming interfaces (APIs) and documented data exchange formats for standards-based integration.		

MAINTAINABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8746	Advance notice of planned changes	The Contractor must provide advance notice of planned changes that may affect functionality, interfaces, integrations, security, or availability.		
2092	EDGE NFR 7081: Edge Node Scalability 1	The solution must provide modular or microservices-based components for independent scaling and deployment.		
2107	EDGE NFR 7082: Edge Node Updates	The solution must support modular updates and automated deployment to edge nodes.		
8747	Environment separation	The Contractor must maintain separate environments for production and non-production activities.		
8745	Formal change control	The Contractor must maintain formal change management for releases, patches, configuration changes, and emergency fixes.		
2064	NFR-7003: Post-Go-Live Hypercare & Support	The Contractor must provide post go-live Hypercare support, including a defined stabilization period and ongoing support services covering production operations, application maintenance, and enhancements.		
2065	NFR-7004: Modular Architecture Boundaries	The solution must be modular, with components that can be easily added, removed, or replaced.		

2066	NFR-7005: Independent Module Deployment	The solution must support independent deployment of modules to enable more frequent updates and reduce the risk of solution-wide downtime during maintenance activities.		
2067	NFR-7006: Safe Extension & Modification	The solution must support the addition of new functionality, modules, and components without requiring extensive modifications to the existing solution.		
2068	NFR-7007: Automated Testing & Simulation Support	The solution must support automated testing, using clear and well-defined test cases and test data.		
2069	NFR-7011: Managed Shared Components	The solution must support centralized management of shared components and configuration so approved changes can be applied consistently across solutions and environments.		
2070	NFR-7012: Requirements Traceability	The Contractor must deliver and maintain a Requirements Traceability Matrix (RTM) that maps delivered functionality to requirements and associated test evidence.		
2071	NFR-7013: Orphaned Content Detection	The Contractor must address broken links or orphaned documents that are not associated with another object.		
2072	NFR-7014: Third-Party Software Management	The Contractor must install and manage required third-party software.		
2073	NFR-7015: Environment Refresh Governance	The Contractor must develop a State-approved refresh schedule and perform the required refreshes.		
2074	NFR-7018: Centralized Content Management	For document management functions, the solution must use a centralized, shared document management or content management solution.		
2075	NFR-7024: Data Archiving & Protection	The Contractor must assist the State in developing procedures to ensure that specified data is archived and protected from loss, unauthorized access, or destruction.		
2076	NFR-7029: Service Versioning	The solution must support multiple concurrent service versions to accommodate different customer segments, regulatory timelines, and use cases, using controlled versioning mechanisms that prevent breaking changes and support independent upgrade paths.		
2077	NFR-7037: Supported Browser Compatibility	The solution must support the latest three versions of all web browsers with a United States market share greater than 3 percent, as indicated by gs.statcounter.com.		
2078	NFR-7039: Network Configuration Governance	The solution must support controlled management of network configuration changes, including DNS updates and addressing changes, without requiring modifications on the State side during routine upgrades or maintenance.		
2079	NFR-7040: Network Compatibility Testing	The Contractor must perform network compatibility testing across supported environments and configurations to ensure continued operability during upgrades, infrastructure changes, and version transitions.		

2080	NFR-7042: Error Detection and Root Cause Identification	The solution must detect and capture errors, identify their causes where feasible, and notify the State within SLA-defined timeframes for reportable failures.		
2081	NFR-7047: Pre-Release Validation	The Contractor must test and validate new features and updates before releasing them to customers, using automated tools and processes.		
2082	NFR-7049: Continuous Improvement & Iterative Delivery	The Contractor must apply iterative development and continuous improvement practices, incorporating feedback loops and retrospectives to improve solution quality over time.		
2083	NFR-7053: Forward-Compatible Design	The solution must be able to accommodate future changes and updates so that new software versions operate without requiring significant redesign or reimplementation.		
2084	NFR-7075: API Deprecation & Sunset Policy	The solution must maintain a documented API lifecycle policy that includes versioning, deprecation, and sunset procedures. The Contractor must provide advance notice and an approved transition period for breaking changes, maintain backward compatibility for a State-approved minimum period, and provide migration guidance and testing support for impacted integrations.		
8748	Release transparency	The Contractor must provide release notes and regression impact summaries for each update.		

PERFORMANCE

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8723	Capacity management	The Contractor must provide capacity management practices that support forecasted growth in users, transactions, storage, and integrations.		
8725	Capacity threshold notice	The Contractor must notify the State in advance when the solution approaches a capacity threshold that may affect performance.		
2095	EDGE NFR 2081: Edge Node Functionality	Edge nodes must store and serve locally cached datasets including warrants, BOLOs, officer rosters, and vehicle information.		
2096	EDGE NFR 2082: Edge Node Conflict Resolution	The solution must include automated conflict resolution and synchronization between edge nodes and cloud when connection is restored.		
2097	EDGE NFR 2083: Offline First Preference	Mobile applications must support offline-first operation with automatic synchronization when bandwidth is available.		
2103	EDGE NFR 2084: Edge Node Performance	CAD unit status and incident changes must propagate across connected nodes within 1 second.		
2099	EDGE NFR 2084: Locally Stored Geospatial Media	The solution must provide locally cached geospatial tiles for offline mapping.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

2101	EDGE NFR 2085: RPO	The solution must target a maximum data age variance of 1 Hour during active cellular network availability. If a cell link is broken, data mutations must safely buffer locally without bound.		
2102	EDGE NFR 2086: RTO	Upon client re-connection to a cellular network, the outbox synchronization queue must activate within 30 seconds to begin payload offloading.		
2112	EDGE NFR 2087: Granular Audit Log Capturing	The local storage engine must maintain an unalterable, chronological audit log capturing all CJI interaction events (read, write, delete, search history, and failed authentication attempts) along with user IDs and timestamps		
2113	EDGE NFR 2088: Idempotency	The synchronization worker must leverage an incremental transactional versioning protocol to ensure network handshakes cut short by cellular drops do not trigger duplicate database rows upon re-transmission.		
2114	EDGE NFR 2089: Data Security After Device Theft	The application must support programmatic hooks that allow integration with an agency's Mobile Device Management (MDM) platform to initiate an immediate remote wipe of all local encrypted storage files if a device is reported lost or stolen.		
2120	EDGE NFR 2090: Local Storage	The local application layer must utilize a transactional, index-supported database (e.g., IndexedDB or platform equivalent) capable of scaling beyond standard browser local storage limits (up to gigabyte thresholds).		
2121	EDGE NFR 2091: Offline Transaction Latency	Local read and write transactions to the encrypted storage engine must complete within under 100 milliseconds to prevent UI blocking while offline.		
2122	EDGE NFR 2092: Network Payload Management	The synchronization engine must compress data payloads and transmit updates in chunked batches.		
2123	EDGE NFR 2093: Automatically Detect Connectivity	The solution must automatically detect changes in network status (e.g., using navigator.onLine or native network listeners) and transition between online and offline modes without requiring a manual application restart.		
2106	EDGE NFR 2094: Edge Node Scalability	The solution must support multi-agency, multi-jurisdiction scaling across municipalities.		
8724	Elastic scale	The solution must scale to accommodate projected contract-term growth without redesign.		
1895	NFR-2000: Efficient Application Integrations	The solution must meet State-defined performance thresholds for all application-to-application integrations to ensure integration activity does not negatively impact user experience.		
1896	NFR-2001: Scalability & Load Handling	The solution must support large volumes of data and traffic and must scale resources to meet operational demand without service degradation.		
1897	NFR-2002: Network Throughput	The solution must meet State-approved network bandwidth and throughput requirements to ensure timely and accurate data exchange under expected and peak loads.		

1898	NFR-2003: Performance Monitoring & Alerting	The solution must provide monitoring and alerting capabilities that track usage, performance, and availability, and must proactively detect and resolve performance or capacity issues.		
1899	NFR-2004: User Response Time	The solution will meet State-approved response time thresholds for user interactions under normal and peak load conditions, as validated through performance testing.		
1900	NFR-2005: Performance Regression Detection	The solution must detect, analyze, and remediate performance degradation caused by configuration changes, releases, or infrastructure updates.		
1901	NFR-2007: Performance Metrics and Logging	The solution must provide monitoring and logging mechanisms that collect, track, and report performance metrics and error conditions to support performance analysis and operational oversight.		
1902	NFR-2008: Browser-Based Access Performance	The solution must be available directly through a web browser, with no software to download or hardware to install.		
1903	NFR-2009: Application Response Time Commitments	The Contractor must provide expected application response times and the approximated transaction volumes supported by the service.		
8722	Performance targets	The solution must meet the documented response-time targets for interactive transactions, application programming interfaces (APIs), and batch operations under the agreed load conditions.		

PORTABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8758	Configuration without custom code	The solution must support configuration through settings rather than code customization.		
8760	Extensibility	The solution must support extensibility, integration, and future expansion without redevelopment.		
2085	NFR-8000: Platform Portability	The solution must be deployable across supported enterprise infrastructure platforms and operating solutions without functional degradation.		
2086	NFR-8001: Standards-Based Virtualization	For IaaS solutions, the Contractor must use industry-standard virtualization technologies and deploy them in accordance with vendor and industry best practices.		
2087	NFR-8002: Physical and Virtual Component Separation	For IaaS solutions, the Contractor must implement physical and virtual separation of infrastructure components to support isolation, resilience, and operational stability.		
2088	NFR-8003: State Environment Readiness	If the solution requires it, the Contractor must assist the State in preparing desktops, networks, infrastructure, and applications.		

2089	NFR-8006: Source Code Delivery	The Contractor must provide the State with a complete, readable copy of all source code, including build scripts, configuration files, and documentation, for all custom-developed applications deployed to production.		
2090	NFR-8007: Executable Code Delivery	The Contractor must provide the State with built artifacts for deployed releases, including binaries or executable code for all custom-developed applications deployed to production.		
8759	No lock-in for data retrieval	The solution must provide retrieval of State data and basic administrative records without requiring proprietary tooling.		

RELIABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8734	Continuous monitoring	The solution must provide continuous monitoring of service health, security events, and capacity.		
2094	EDGE NFR 5081: Edge Node Continuity of Operations	Edge nodes must manage local CAD operations (e.g., incident creation, incident updates, and unit status changes) during connectivity loss.		
2091	EDGE NFR 5081: Edge Node Reliability 1	The solution must support a cloud architecture with edge nodes capable of autonomous operation.		
2098	EDGE NFR 5082: CAD RMS Store and Forward Preference	The solution must support store-and-forward messaging for incident notes, and media attachments.		
2105	EDGE NFR 5082: Edge Node Reliability	Edge nodes must provide uninterrupted local service.		
8750	Monthly service reporting	The Contractor must provide monthly service reports covering availability, incidents, service-level agreement (SLA) performance, capacity, security events, and open corrective actions.		
8751	Named contacts	The Contractor must identify named service management contacts for operational, security, contractual, and executive escalation.		
8752	NFR-36 Business Continuity and Disaster Recovery	The Contractor must maintain and test business continuity and disaster recovery plans for the in-scope services.		
1943	NFR-5001: Version Control & Rollback	The solution must support version control and rollback capabilities to enable reversions in the event of errors or issues with new updates.		
1944	NFR-5002: Environment Data Refreshes	SaaS and PaaS solutions must perform regular State-approved data refreshes to maintain data accuracy and integrity across environments.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1945	NFR-5003: Network Resilience	The solution's interfaces and integrations must continue to operate during partial network or infrastructure failures through appropriate redundancy, load balancing, and failover mechanisms.		
1946	NFR-5005: High Availability Architecture	The solution must be architected with no single point of failure to support a high-availability enterprise.		
1947	NFR-5006: Zero-Downtime Changes	The solution must support component and data level changes without loss of application availability, enabling maintenance and updates without service disruption.		
1948	NFR-5009: Backup & Recovery Testing	The Contractor must test backup and recovery procedures prior to production launch to validate those procedures and confirm the ability to meet recovery requirements.		
1949	NFR-5012: External Dependency Resilience	The solution must support continuity of operations when dependent external or partner solutions are unavailable, including transaction queuing or deferred processing where appropriate.		
1950	NFR-5018: Alerting and Escalation	The Contractor must generate and send alerts based on monitored solution attributes, with escalation via email and SMS as defined in the operational monitoring framework.		
1951	NFR-5020: Automatic Recovery	The solution must recover automatically from failures and errors without losing data or transactional integrity.		
1952	NFR-5021: Service Quality Controls	The Contractor must ensure service quality and reliability by following defined quality assurance standards and procedures, including testing, defect resolution, and review.		
1953	NFR-5022: Exchange Verification	The solution must perform source-to-destination file integrity checks for exchange data and alert appropriate parties when issues are detected.		
1954	NFR-5023: Inbound Data Processing	The Contractor must load data received from the State of Vermont and make it available to authorized parties within 24 business hours of receipt..		
1955	NFR-5024: Mastered Data Integrity	The solution must employ data de-duplication and cleansing across all mastered subject areas to ensure data accuracy, consistency, and integrity.		
1956	NFR-5025: Application-Level Cleansing	The solution must employ data de-duplication and cleansing to minimize the entry of inaccurate or invalid data into target environments or other solutions.		
1957	NFR-5026: Transaction Integrity & Replay	The solution must ensure that integration transactions are durable, support retry logic, and prevent data loss in the event of partial failures.		
1958	NFR-5027: Idempotent Interfaces	Integration endpoints must support idempotent operations, where applicable, to prevent duplicate transaction processing.		

1959	NFR-5028: Integration Monitoring & Alerting	The solution must provide monitoring and alerting for integration interfaces, including availability, latency, and error rates.		
1960	NFR-5029: Payload Size & Throughput Protection	Integration services must enforce defined payload size limits and support throttling or rate limiting to prevent downstream solution overload.		
1961	NFR-5031: Standardized Observability Export	The solution must generate and export logs, metrics, and traces in structured, machine-readable formats compatible with State-approved monitoring and security tools. Telemetry must include sufficient context to support operational diagnostics (e.g., correlation identifiers, timestamps, environment identifiers, request and transaction identifiers, and error codes) and must be exportable without proprietary tooling lock-in.		
1962	NFR-5032: Architectural Isolation	Each AI component must operate as an independent, non-blocking service that is isolated from the core application stack.		
1963	NFR-5033: Uptime & Availability Protection	Failure or degradation of any approved AI component must not reduce overall solution uptime or availability below established service level thresholds.		
1964	NFR-5034: Workflow Continuity	Failure or degradation of any approved AI component must not prevent the execution of any production workflow.		
1965	NFR-5035: Continuous Monitoring	The Contractor must continuously monitor each AI service for availability, latency, throughput, and error rates.		
1966	NFR-5036: Incident Management Integration	The Contractor must integrate approved AI service monitoring with its incident management processes.		
1967	NFR-5037: State-Controlled AI Disablement	The Contractor must design each approved AI component so that the State can disable it without interrupting core solution functionality, workflows, or business processes.		
8749	Service desk and escalation	The Contractor must provide a service desk with defined severity levels, response times, escalation paths, and restoration targets.		

SECURITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8700	Access agreements	The Contractor must require each covered individual to sign access agreements, nondisclosure agreements, acceptable use agreements, and rules of behavior before the Contractor grants access, and to sign them again when they are updated.		
8707	Assessment, authorization, and continuous monitoring	The Contractor must support control assessments, solution authorization activities, plans of action and milestones, and continuous monitoring for all in-scope services.		
8757	Audit and verification rights	The Contractor must permit the State to exercise audit rights, assessment rights, and evidence-based verification rights.		

8732	Audit logging	The solution must generate tamper-resistant audit logs for authentication, authorization, privileged activity, administrative changes, data access, data export, and security events.		
8705	Audit logging, review, and reporting	The Contractor must generate, protect, retain, review, analyze, and report the audit records needed to support investigations, incident response, and compliance verification.		
8716	CHRI access, use, and dissemination	The Contractor must restrict access to, use of, and dissemination of criminal history record information to authorized purposes, and must capture the justification for each Interstate Identification Index inquiry, in conformance with CJIS Security Policy Section 4.2.		
8696	CJIS compliance obligation	The Contractor must comply with the FBI CJIS Security Policy version 6.0 and its successor versions adopted during the contract term, and with all applicable CJIS Systems Agency, State Identification Bureau, Compact Council, and agency-specific CJIS requirements.		
2115	CJIS NFR 6099.1: User Action Audit 1	The solution must record the specific operation or action executed within the application context (e.g. User Login, Failed Authentication, Record View (Query), Record Modification (Update), Record Deletion, Log Export, Local Encryption Key Purge).		
2116	CJIS NFR 6099.2: User Action Audit 2	For offline client queues, the solution must capture the Local Client Timestamp at the exact millisecond the transaction occurred offline, as well as the Server Ingest Timestamp when the queue is later synchronized.		
2117	CJIS NFR 6099.3: User Identification	The solution must explicitly map to the individual's verified solution username or internal account ID (generic or shared login sessions are prohibited under CJIS identity standards).		
2118	CJIS NFR 6099.4: User Terminal Identification	The solution must record either the Originating Agency Identifier, the local device serial/MDT ID, or the client IP/MAC address.		
2119	CJIS NFR 6099.5: Case Identification	The solution's log must record the internal Database Record ID, Case Number, or National Crime Information Center (NCIC) transaction number to establish a precise data custody trail.		
2109	CJIS SEC 6097: FIPS-Validated Data Encryption	The application must encrypt all Criminal Justice Information (CJI) stored locally at rest using an asymmetric/symmetric algorithm utilizing FIPS 140-3 validated cryptographic modules with a minimum of AES 256-bit strength.		
2108	CJIS SEC NFR 6098: Data Encryption Standard	The solution must encrypt all locally stored data using the AES-GCM (256-bit) cryptographic algorithm prior to writing to the physical disk.		
2104	CJIS SEC NFR 6099: CJIS Compliance	The solution must comply with CJIS authentication, encryption, logging, and access control requirements.		
8761	Cloud security authorization	The Contractor must provide and maintain, throughout the contract term, FedRAMP Moderate or StateRAMP Moderate authorization and continuous monitoring for the specific service offering and deployment proposed.		
8755	Compliance evidence	The Contractor must maintain evidence of compliance with the legal, regulatory, accessibility, security, and privacy obligations applicable to the service.		

8713	Corrective action and remedies	The Contractor must prepare and execute corrective action plans for all CJIS compliance findings, security deficiencies, audit observations, and control failures within the timelines approved by the State.		
8697	Coverage of subcontractors and downstream providers	The Contractor must flow down all CJIS, personnel security, access control, audit, incident, and data protection obligations to every Subcontractor and downstream provider that stores, processes, transmits, administers, or can otherwise access criminal justice information.		
8737	Data classification and handling	The Contractor must classify and handle State data in accordance with State policy, legal requirements, and retention schedules.		
8741	Data residency and subprocessors	The Contractor must disclose all data residency, replication, backup, and subprocessor locations applicable to State data.		
8711	Documentation and evidence of compliance	The Contractor must maintain the latest solution security documentation, architecture documentation, access records, training records, screening records, incident records, audit records, and assessment evidence needed to demonstrate compliance.		
2093	EDGE NFR 6097: Edge Node Interoperability	The solution must expose secure, standards-based APIs for integration with state, federal, and local technology solutions.		
2111	EDGE NFR 6098: Session Inactivity Purge	Local application contexts must execute an automatic timeout sweep after an administrator-defined period of user inactivity in accordance with CJIS standards, securely wiping the encryption keys from memory and locking the application interface.		
8726	Encryption	The solution must encrypt data in transit and at rest using the latest approved cryptographic controls.		
8704	Encryption and key control in cloud environments	When criminal justice information is processed in a cloud environment, the Contractor must document whether that information is decrypted in the provider-managed environment, who holds the encryption keys, and which provider personnel can access that environment.		
8703	Encryption of CJI at rest	The Contractor must implement cryptographic protection that prevents unauthorized disclosure or modification of criminal justice information at rest on the solution and on digital media outside physically secure locations.		
8698	External system services and enforceable service levels	The Contractor must define the external service roles, responsibilities, security functions, ports, protocols, services, measurable outcomes, and remedies for noncompliance in the contract and the service-level documentation.		
8736	Forensics and corrective action	The Contractor must support forensic preservation, root-cause analysis, and corrective action reporting.		
8715	Identity proofing and identity assurance	The Contractor must perform identity proofing and enrollment for each individual granted access to criminal justice information at the identity assurance level required by the CJIS Security Policy, validating the identity evidence and confirming the enrollment address.		
8702	Identity, authentication, and authenticator management	The Contractor must implement CJIS-compliant identity and authentication controls that comprise authenticator management, banned-password controls, and authenticator refresh requirements.		

8735	Incident notification	The Contractor must notify the State of security incidents and service disruptions within the contract-defined time frames.		
8706	Incident reporting and coordination	The Contractor must report security incidents affecting criminal justice information or a CJIS-connected solution through defined and automated mechanisms, coordinate incident information sharing with the State, and support investigation, containment, and recovery.		
8756	Independent assurance reports	The Contractor must provide the latest independent assessment reports, certifications, or control attestations relevant to the service model and scope.		
8712	Inspection and audit rights	The Contractor must permit the State, the CJIS Systems Agency, the State Identification Bureau, a Compact-authorized authority, and authorized auditors to review evidence of compliance, conduct audits or assessments, and require corrective action.		
8733	Log retention and access	The Contractor must retain logs for the period defined by the State, and make the logs available for investigation and compliance review.		
8709	Media protection, sanitization, and destruction	The Contractor must sanitize or destroy media containing criminal justice information before reuse or disposal, using methods commensurate with the sensitivity of the information.		
8714	Mobile device and wireless security	The Contractor must secure mobile and wireless access to criminal justice information through mobile device management, wireless access-point hardening, and mobile authentication controls, in conformance with CJIS Security Policy Section 5.20.		
8728	Multi-factor authentication	The solution must support multi-factor authentication (MFA) for privileged access and for the user populations designated by the State.		
1822	NFR-6000: Data Residency (United States)	Data center facilities must be located within the United States to comply with jurisdictional regulations.		
1823	NFR-6001: FedRAMP & FTI Compliance	Solutions handling Federal Tax Information (FTI) or other sensitive data must comply with FedRamp standards to ensure data security and regulatory compliance.		
1824	NFR-6002: Internal Network Firewall Controls	Access to the environment via the State of Vermont internal network must be controlled by a firewall that validates communications based on recognized protocols and approved source/destination IP address ranges.		
1825	NFR-6003: DMZ Deployment for Public-Facing Applications	Applications accessible from the public internet must be deployed on dedicated Demilitarized Zone (DMZ) servers managed by the Contractor to ensure security and isolation from internal networks.		
1826	NFR-6004: Authorized Personnel Access Control	Contractor personnel must be authorized by the provider for network and system access across all environments to maintain security and control.		
1827	NFR-6005: Secure Network Traffic Routing	Traffic to the State of Vermont must be routed by the Contractor over the appropriate link, either Transaction Link or Management Link, to ensure efficient and secure data transmission.		

1828	NFR-6006: Isolated Support Network Architecture	The Contractor must maintain an isolated support network separate from its intranet, including firewall, VPN, intrusion detection, authentication, reporting, and DNS services, as the standard method for personnel to connect to the environment.		
1829	NFR-6007: Data Center Access Control	The Contractor must manage access control to its data centers and the environment, limiting access to State of Vermont's network connections to authorized personnel only.		
1830	NFR-6008: SSL/TLS Encryption for Web Applications	Secure Socket Layer (SSL) must be deployed for all web-based applications hosted by the Contractor, especially those accessible via the internet or secure networks like hardware VPNs, ensuring secure data transmission.		
1831	NFR-6009: Secure Access for Non-Public Applications	The Contractor must deploy non-Secure Socket Layer (SSL) applications privately, accessible only through secure network connections and not exposed to the public internet, with State of Vermont connections to non-internet applications using SSL and secure network connections.		
1832	NFR-6010: Internal SSL Deployment for Public Access Systems	Secure Socket Layer (SSL) -enabled web applications accessed by the State of Vermont (SOV) via the public internet must be deployed internally by the Contractor over SOV's network, with the hosting provider procuring and maintaining SSL certificates on behalf of the SOV.		
1833	NFR-6011: Site-to-Site VPN Connectivity	The Contractor must utilize VPN devices in a site-to-site (network-to-network) configuration, leveraging either the public internet or dedicated links for secure data transmission.		
1834	NFR-6012: IPsec Encryption Standards	Internet Protocol Security (IPsec) must be implemented within the VPN strategy to secure data using tunneling and encryption (168-bit Triple DES or AES256) for data privacy.		
1835	NFR-6013: VPN Access Provisioning	Access to the environment must be provided via VPN connections, with the Contractor specifying and delivering the required number and type of VPNs for the State of Vermont.		
1836	NFR-6014: Secure Network Transport Design	The Contractor must design and implement network transport (e.g., Transaction Link) to allow personnel access to the environment, with DMZs at hosting provider data centers connecting via VPN tunnels terminating on hosting provider firewalls.		
1837	NFR-6015: Protected Log Access & Integrity	Access to logs must be restricted to authorized personnel based on need-to-know and least privilege principles, with log files protected using FIPS cryptographic hash sums and monitored, and logs accessible via intranet systems relocated daily to non-intranet systems.		
1838	NFR-6016: Enterprise Access Control Policy	Access control policies and procedures must govern resource access within the State of Vermont environment, including physical servers, files, directories, services, database tables, and network protocols.		
1839	NFR-6017: Least Privilege & Separation of Duties	Least Privilege and Separation of Duties (SOD) principles must be applied to all solutions, ensuring user permissions and system functionality align with specific roles based on access needs.		
1840	NFR-6018: Security Review for New Deployments	New deployments within Contractor data centers must undergo security technical reviews by a cross-organization team, including dedicated security experts, and technologies or tools not meeting security policies or standards must not be deployed.		
1841	NFR-6019: Consistent Security Across Environments	Security and compliance standards for deployment environments must remain consistent whether in production or non-production settings.		

1842	NFR-6020: Security Awareness & Privacy Training	All permanent or contract employees handling data must complete data privacy awareness and corporate ethics training, including understanding data privacy, recognizing risks related to personal data, understanding their data responsibilities, and reporting privacy violations.		
1843	NFR-6021: Firewall-Based Server Isolation	Server instances within deployment environments must be isolated via firewalls based on their application role.		
1844	NFR-6022: Secure Remote Access via VPN	Remote access for Contractor employees and subcontractors must require IPsec or SSL-encrypted VPN connections from non-hosting service provider locations to access the network.		
1845	NFR-6023: MFA for Support Access	Contractor support engineers accessing the State of Vermont's (SOV's) environment via VPN through the SOV internal network must use two-factor authentication.		
1846	NFR-6024: Role-Based Access Provisioning	Access provisioning must be centralized and based on job roles, requiring management approval to ensure appropriate access levels are maintained.		
1847	NFR-6025: Secure OS Authentication Controls	Access to operating systems must require secure login procedures with unique user IDs and strong passwords to protect system integrity.		
1994	NFR-6026: Privileged Credential Rotation (30-Day)	Root passwords for hosts and facilities must be changed every 30 days to enhance security and prevent unauthorized access.		
1849	NFR-6027: Confidentiality & Data Protection Agreements	Employees must maintain confidentiality of state data by signing confidentiality agreements and complying with company policies on the protection of confidential information.		
1850	NFR-6028: Secure Data Transmission Controls	Network controls must protect and control State of Vermont data during transmission, ensuring all connected devices comply with security standards and policies.		
1851	NFR-6029: Removable Media Handling & Protection	Designated personnel must handle removable digital media according to defined procedures, with media securely transported, logged, and vaulted by a third-party service provider under contractual obligations to comply with hosting provider-defined media protection terms.		
1852	NFR-6030: Intrusion Detection & Threat Monitoring	Intrusion Detection Systems (IDS) must provide continuous surveillance to intercept and respond to security events, ensuring timely detection and mitigation of threats.		
1853	NFR-6031: Encrypted Storage for Removable Media	State of Vermont data must not be stored on removable drives or mediums unless encrypted to safeguard sensitive information.		
1854	NFR-6032: Restricted Distribution of Sensitive Media	Strict restrictions must be maintained over the distribution of media containing state health information, complying with information protection, media sanitization, privacy, and records retention policies.		
1855	NFR-6033: NIST 800-53 Compliance (Go-Live)	The Contractor must ensure that the solution achieves compliance with applicable State and Federal regulations and standards as outlined in the National Institute of Standards and Technology (NIST) Publication 800-53, current revision, upon Operational Go-Live. Compliance must be verified through an independent third-party production security controls assessment.		

1856	NFR-6034: Annual Independent Security Assessment	The Contractor must ensure an independent third-party production security controls assessment is conducted at least annually, at no additional cost to the State, and performed by a State-approved third party that has no financial or controlling relationship with the Contractor.		
1857	NFR-6035: Continuous Compliance Remediation	The Contractor must be responsible for implementing modifications to maintain compliance with applicable State and Federal regulations and standards as outlined in the National Institute of Standards and Technology (NIST) Publication 800-53, current revision, including the application of compensating controls to address any identified gaps.		
1858	NFR-6036: Security Assessment Reporting & CAP	The Contractor must provide documented results of the independent third-party production security controls assessment and develop corrective action plans for any deficiencies identified during the assessment.		
1859	NFR-6037: Ongoing Compliance Maintenance	The Contractor must ensure all modifications necessary to maintain compliance with applicable State and Federal regulations and standards as outlined in the National Institute of Standards and Technology (NIST) Publication 800-53, current revision, are executed in accordance with the terms and conditions of the Contract.		
2006	NFR-6038: Database Credential Rotation (180-Day)	Database passwords must be changed every 180 days to ensure ongoing security and prevent unauthorized access.		
1861	NFR-6039: Encryption of Data in Transit	Data integrity during transmission must be protected using strong encryption protocols such as TLS/SSL or IPsec on VPN networks, and validated with FIPS 140-3 certificate.		
1862	NFR-6040: SIEM Monitoring & 24/7 Alerting	The Contractor must implement a Security Information and Event Management (SIEM) system to correlate and alert on security events from Intrusion Detection Systems (IDS), firewall logs, and network flow events, with monitoring conducted 24/7 throughout the year.		
1863	NFR-6041: Email Security (AV/Anti-Spam/TLS)	Third-party anti-virus and anti-spam products must scan all State of Vermont and employee emails and attachments traversing Contractor data centers, with the email infrastructure enforcing TLS encryption for both inbound and outbound emails.		
1864	NFR-6042: Operating System Hardening	Server operating systems must be hardened by eliminating unnecessary services, accounts, and network access rights to enhance security and reduce vulnerabilities.		
1865	NFR-6043: Security Incident Response & Coordination	The Contractor must evaluate and respond promptly to incidents of unauthorized access or handling of State of Vermont (SOV) data, collaborating with relevant teams and law enforcement to restore the confidentiality, integrity, and availability of SOV's environment.		
1866	NFR-6045: Administrative User & Role Management	Solution administrators must have the capability to create, manage, and assign user accounts with role-based access, including configurations for user groups, locations, and organizational hierarchy.		
1867	NFR-6046: Critical Patch Management (24-Hour SLA)	Critical security patches must be applied within 24 hours of their release, with support for automated patch deployment to ensure timely protection against vulnerabilities.		
1868	NFR-6047: Transaction Logging & Monitoring	The solution must provide transaction tracking and log consolidation capabilities across the application's data tier to facilitate comprehensive monitoring and analysis.		
1869	NFR-6048: Data Change Audit & Traceability	The solution must maintain records of all data additions, changes, and deletions, which must be searchable by user/client ID, date/time, location, and other relevant details to ensure traceability and accountability.		

1870	NFR-6049: Audit Log Integrity Protection	Audit records must be protected from unauthorized modifications and require formal approval for any changes to maintain integrity and compliance.		
1871	NFR-6050: SaaS Compliance Attestation	SaaS service providers must provide evidence of attestation that meets federal and state compliance regulations to ensure adherence to legal and regulatory standards.		
1872	NFR-6051: Single Sign-On (SSO) Support	The solution must utilize Single Sign-On (SSO) components for authentication and authorization to streamline user access and enhance security.		
1873	NFR-6052: Message Integrity & Digital Signatures	The solution must employ digital signatures or secure mechanisms to authenticate senders of messages or transactions, ensuring the authenticity and integrity of communications.		
1874	NFR-6053: PII Protection (Encryption/De-Identification)	The solution must support the protection of Personally Identifiable Information (PII) through encryption or de-identification techniques to safeguard sensitive data.		
1875	NFR-6054: OWASP & Secure Coding Compliance	The Contractor must certify code against OWASP Application Development Security Standards and mitigate risks outlined in CWE/SANS Top 25 Most Dangerous Software Errors.		
1876	NFR-6055: SOC 2 Type II Compliance Report	The Contractor must submit a Statement on Standards for Attestation Engagements (SSAE) 18, Service Organization Control (SOC) 2 Type II Compliance Report from hosting providers.		
1877	NFR-6056: Information Security Policy	The Contractor must maintain organizational information security policies to ensure comprehensive protection of data.		
1878	NFR-6057: Ongoing Security & Privacy Compliance Obligations	The Contractor must ensure the system(s) maintains compliance with current and future security, privacy, accessibility, and certification laws (State and Federal), regulations, policies, and guidelines relevant to system security, confidentiality, integrity, availability, and safeguarding of information. Where any of these overlap, the Contractor must ensure that the system(s) must always strive to attain the more stringent policy. The Contractor retains responsibility for all modifications to the system(s) to maintain compliance according to the terms and conditions of the resulting Contract.		
1879	NFR-6058: 24/7 Breach Response Team (5-Minute SLA)	The Contractor must maintain a Security Breach Response Team available 24 hours a day, 7 days a week, and within 5 minutes of notification of an incident to respond to security violations and breaches (physical and electronic). This includes communications to a defined list of personnel at the State tied to the State's Continuity of Operations/Disaster Recovery. State staff must be informed of response plan, including specific steps and time frames for resolution.		
1880	NFR-6059: Security Administration Interface (508-Compliant)	The Contractor must provide a State-approved, 508-compliant user-centered designed and intuitive interface for Security Administrators to grant, track, manage, and revoke access for individuals. System must also provide auditing capabilities for approved audit resources.		
1881	NFR-6060: Annual Independent Security Testing	The Contractor must ensure all systems undergo Industry Standard security testing (e.g., penetration, physical security, web application, social engineering) minimally on an annual basis, as mutually agreed upon between the Contractor and the State, when there has been a significant infrastructure change or resulting from Federal requirements. This security testing must be conducted at no cost to the State and by a State-approved third party that maintains no financial or controlling relationship with the Contractor. Additionally, the Contractor must provide documented testing results and generate corrective action plans for any deficiencies identified as well as be responsible for modifications to remain compliant based on the terms and conditions of the Contract.		

1882	NFR-6061: Quarterly Security Testing & Reporting	The Contractor must design and execute security testing to prevent unauthorized access to the system (intrusion detection and vulnerability testing) on a quarterly basis and provide a report of all findings to the State within 10 business days. Any issues identified and reported to the State are to be resolved according to their respective SLA.		
1883	NFR-6062: Strict Data Residency & Access Restrictions	The Contractor must ensure State of Vermont (SOV) data is not stored, transmitted to, or accessed from outside the United States except as authorized in writing by SOV.		
1884	NFR-6063: Privacy Impact Analysis	The Contractor must conduct a Privacy Impact Analysis that identifies data elements of the system exposing Vermont beneficiaries to potential privacy threats and outlines system controls to mitigate risks of private data disclosure.		
1885	NFR-6064: Security Incident Response	The Contractor must establish a security event notification process, event evaluation and escalation procedures, and security event response procedures to ensure timely and effective handling of security incidents.		
1886	NFR-6065: Network Architecture Documentation	The Contractor must provide a complete network diagram detailing servers, printers, workstations, firewalls, intrusion prevention systems, network security device internet connections, and any other network-connected devices. This diagram must show sufficient detail of data flows in and out of security boundaries, including VPNs, subnets, ports, and protocols.		
1887	NFR-6066: Log Collection and Monitoring	The Contractor must establish a detailed strategy for system log collection and monitoring to ensure ongoing oversight and security.		
1888	NFR-6067: Anti-Malware Protection	The Contractor must establish an antivirus deployment and maintenance plan to protect against malware and other security threats.		
1889	NFR-6068: Software Maintenance Strategy	The Contractor must establish a software maintenance strategy, including updates for operating systems and third-party software, to ensure systems remain secure and functional.		
1890	NFR-6069: Access Control	The Contractor must establish procedures to limit access to information to individuals who need it for their job functions, ensuring access is restricted to the minimum necessary information.		
1891	NFR-6070: Physical Security	The Contractor must ensure that data under its control is physically protected using appropriate devices and methods, such as alarm systems, locked file cabinets, security guards, or other measures to prevent loss or unauthorized access.		
1892	NFR-6071: Credential and Access Control Management	The Contractor must establish procedures to prevent unauthorized use of passwords, access logs, badges, or other methods designed to prevent loss or unauthorized access to electronically or mechanically held data.		
2040	NFR-6073: Central IDP Routing	Login is routed through the State-determined central identity provider external users, and MS Entra for internal users ensuring state-approved authenticators and user experience.		
2041	NFR-6074: SAML 2.0 / OIDC enforcement	Authentication for both internal and external users is handled via SAML 2.0 or OIDC only, and in conformance with their respective standards.		
2042	NFR-6075: Auth Validated in DEV/TEST/PROD	Authentication is validated in DEV and TEST environments, in addition to PROD, when directed by the State.		

2043	NFR-6076: Dual IDP / Routing Logic	Applications serving both internal and external users support two identity providers with separate URLs. Where an application cannot support two providers, the State may agree to handle routing through a single IDP upon request.		
2044	NFR-6077: Internal vs External Status via Claims	Applications dependent on internal/external user status can reliably determine that status from OIDC claims or SAML attributes.		
2045	NFR-6078: Block Incomplete Profiles	Users with incomplete profiles are blocked from application functionality until profile requirements are met.		
2046	NFR-6079: Profile Sourced from IDP	User profile data is sourced from the State's identity provider at each login and kept current. Upon State request, the application provides a real-time update endpoint keyed to the user's persistent subject identifier.		
2047	NFR-6080: Persistent Subject Identifier (Sub)	User identity is anchored to a persistent subject identifier issued by the State's identity provider, not a mutable attribute such as email.		
2048	NFR-6081: Identity Proofing Redirect (id.vermont.gov)	Where OIDC claims or SAML attributes indicate insufficient identity proofing for the application's requirements as defined by the State, users are redirected to id.vermont.gov with State-specified parameters.		
2049	NFR-6082: Configurable Session Length	Application session length is configurable per agency requirements. Identity provider session length is determined by the State.		
2050	NFR-6083: Federated Logout (App + SSO)	Logout terminates both the application session and the SSO session simultaneously.		
2051	NFR-6084: Least Privilege Provisioning	New users are provisioned under least privilege by default, with access elevated only after administrator approval within the application. Where approved by the State, permissions may be tied to identity provider security groups.		
2052	NFR-6085: Self-Service with Restricted Access	The application supports self-service entry, where users can log in and are informed they require elevated access if any access is restricted to a subset of the IDP.		
2053	NFR-6086: Open-Source Model Deployment Environment	Where an open-source AI model is used, the contractor must deploy it within a State-approved, network-restricted environment on State-controlled cloud or infrastructure.		
2054	NFR-6087: Dedicated Hosting & Access Controls	Each open-source AI model must be hosted on dedicated infrastructure with access restricted to approved networks through firewall rules, network segmentation controls, and identity-based access restrictions.		
2055	NFR-6088: External Endpoint Restriction	The solution must not use any unmanaged model endpoints unless explicitly approved by the State.		
2056	NFR-6089: Secure Interfaces	Integration mechanisms, including APIs and web services, must not compromise end-to-end security and must adhere to State approved security standards and protocols.		

2057	NFR-6090: Controlled De-Identified Data Sharing	The solution must support controlled sharing of designated data sets with authorized State and local agencies, ensuring full anonymization and de-identification in accordance with applicable privacy regulations.		
1894	NFR-6091: Multi-Tenant Security Controls (If SaaS)	For multi-tenant environments, the solution must enforce strict tenant isolation at the data, application, and infrastructure levels to prevent cross-tenant access.		
2059	NFR-6092: Secure Transport	All integration traffic must use encrypted transport protocols (TLS 1.3 or a State-approved successor).		
2060	NFR-6093: Token-Based Authentication	Integration authentication must use token-based mechanisms (e.g., OAuth2, signed JWT) unless otherwise approved by the State.		
2061	NFR-6094: Least Privilege Service Accounts	Service accounts used for integration must be restricted to the minimum necessary permissions.		
2062	NFR-6095: Endpoint Abstraction & Configuration Security	Integration endpoints, credentials, and configuration values must be externalized and must not be hardcoded within application logic.		
2063	NFR-6096: Edge Protection for Public-Facing Endpoints (WAF/DDoS/Rate Limiting)	Public-facing endpoints must be protected using State-approved edge security controls, including web application firewall (WAF) protections, DDoS mitigation, and rate limiting or throttling. The solution must support configurable protection policies (e.g., allow/deny lists, request size limits, bot mitigation where applicable) and must log enforcement actions for operational and security review.		
8837	NFR-6097 Software Allowlisting	The solution must permit only authorized software programs to execute, using a deny-all, permit-by-exception policy.		
8838	NFR-6098 Authorized Software List Review	The Contractor must review and update the list of authorized software programs at least annually.		
8839	NFR-6099 Unauthorized Component Detection	The solution must detect unauthorized hardware, software, and firmware components using automated mechanisms at least weekly.		
8840	NFR-6100 Unauthorized Component Response	When the solution detects an unauthorized component, the Contractor must disable or isolate that component and notify the State's designated security contact within the State-defined time frame.		
8841	NFR-6101 Software Installation Enforcement	The solution must enforce software installation policies through automated methods.		
8842	NFR-6102 Software Installation Monitoring	The Contractor must monitor compliance with software installation policies through automated methods at least weekly.		
8699	Personnel screening	The Contractor must screen each individual before granting that individual unescorted physical or logical access to unencrypted criminal justice information or to a solution that could expose unencrypted criminal justice information.		

8710	Personnel transfer and termination	The Contractor must remove badges, credentials, access rights, and privileged access upon the transfer or termination of an individual, and notify the State of affected external personnel within the required time frame.		
8740	Portable data export	The Contractor must provide a complete data export on demand and at contract termination in non-proprietary or openly documented formats.		
8738	Retention and defensible deletion	The solution must support data retention, legal hold, export, archival, and defensible deletion requirements.		
8727	Role-based access and least privilege	The solution must enforce role-based access control and least-privilege administration.		
8731	Secure baselines	The Contractor must maintain documented secure configuration baselines for the infrastructure, platform components, and application components under provider control.		
8701	Security awareness and role-based training	The Contractor must provide and document initial and recurring security awareness training and role-based security training for each individual with access to criminal justice information or a CJIS-connected solution.		
8739	State ownership of data	The Contractor must ensure that the State retains ownership of its data, metadata, configurations, and transaction history.		
8708	Supply chain risk management	The Contractor must maintain a supply chain risk management plan for the solutions, components, and services used to process, store, or transmit criminal justice information, review that plan at least annually, and protect it from unauthorized disclosure and modification.		
8730	Tenant isolation	The solution must segregate State data from other tenants' data using logical and technical controls.		
8729	Vulnerability and malware management	The Contractor must maintain vulnerability management, patch management, malware protection, and security event monitoring.		

TRANSFERABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance
8753	Exit and transition plan	The Contractor must provide an exit and transition plan that includes data return, knowledge transfer, interface disposition, and secure data destruction.		
8754	Transition-period obligations	The Contractor must continue to meet security and retention obligations through the transition-out period.		

USABILITY

ADO ID	Title	Description	Comply ?	Vendor's Description of Compliance

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1924	NFR-4000: User Guidance & Help	The Contractor must provide user-facing guidance, including context-sensitive help and user documentation, available online and in printable formats to support effective and efficient use of the solution.		
1925	NFR-4001: Action Status Visibility	The solution must provide a feedback mechanism that informs users about the status and progress of their actions.		
1926	NFR-4002: Continuous Usability Assessment	The solution must provide an unmoderated usability testing and evaluation mechanism that measures and improves user satisfaction and user experience.		
1927	NFR-4005: Browser-Based Access	The solution must be accessible to customers and State workers using iOS and Android smartphones, as defined during joint application development (JAD) sessions.		
1928	NFR-4011: Efficient Non-Linear Navigation	The solution must support non-linear navigation that enables users to move easily among available functions without requiring sequential traversal of menus or screens.		
1929	NFR-4012: Plain-Language Error Messaging	The solution must present error messages in plain language that clearly describe the issue and constructively suggest corrective actions.		
1930	NFR-4013: Data Entry Validation and Correction	The solution must suggest or automatically correct entries that do not conform to data entry standards.		
1931	NFR-4014: Required Field Identification	The solution must highlight and flag required and incomplete data fields.		
1932	NFR-4015: Document Availability Status	The solution must provide user notifications for document availability events, including files that are checked out, overdue, or otherwise unavailable.		
1933	NFR-4017: Policy & Procedure Document Access	The solution must provide secure, scalable, and accessible storage and retrieval of policy and procedure documents, enabling users to quickly find and access the information they need. The solution must include robust search capabilities, support version control, and enable collaboration among multiple stakeholders.		
1934	NFR-4018: Multi-Device and Browser Support	The solution must function consistently across supported browsers, operating solutions, and device types, including varying screen sizes and resolutions, without degradation of usability or functionality.		
1935	NFR-4020: Standardized & Ad Hoc Analytics	The solution must provide access to standardized reporting, ad hoc queries, and data visualization.		
1936	NFR-4021: Multi-Channel Report Delivery	The solution must provide reports to users in online and offline formats agreed upon during joint application development (JAD) sessions.		
1937	NFR-4025: User-Customizable Analytics	The solution must support creation and customization of reports, queries, and dashboards without requiring technical intervention.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

1938	NFR-4026: Automated Report Distribution	The solution must notify users and distribute reports based on user-specified criteria.		
1939	NFR-4027: Roll-Up and Drill-Down	The solution must provide roll-up, drill-down, and drill-through functionality for online reports.		
1940	NFR-4028: Scheduled Report Generation	The solution must support scheduling of report generation at specific times based on user-defined options.		
1941	NFR-4029: User Interaction Analytics	The solution must capture and report user analytics.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

PART 4b: GENERAL ADMINISTRATIVE REQUIREMENTS

The tables below list the State's General Administrative Requirements. Indicate if your company complies in the "Comply" column.	**Yes**	the vendor **complies** with the stated requirement
Describe how the requirement is met in the "Vendor Description of Compliance" column.	**No**	the vendor **does not compy** with the stated requirement

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2508	GR-00213: Service Management Reporting	The Contractor must deliver a service management report quarterly, including at minimum: incident resolution times (MTTR) by severity, change success rate (percentage of changes implemented without rollback or unplanned service disruption), and problem management outcomes (number of problems opened, closed, and root-caused), using definitions consistent with the Contractor's Service Management Plan.		
2509	GR-00212: Continual Service Improvement Register	The Contractor must conduct a Continual Service Improvement review no less than quarterly and must maintain a CSI register documenting each identified improvement opportunity and its disposition (accepted, rejected, or in progress).		
2510	GR-00211: Service Request Fulfillment	The Contractor must track and report service request fulfillment times monthly, measured against documented target fulfillment times by request category.		
2511	GR-00210: Problem Management Records	The Contractor must maintain a Problem Management log that records, for each identified problem: linked incidents, root cause analysis status, and resolution or workaround status.		
2512	GR-00209: Incident Management Metrics	The Contractor must report incident management metrics monthly, including Mean Time to Acknowledge (MTTA), Mean Time to Resolve (MTTR), and SLA compliance percentage, using definitions consistent with the Contractor's documented Service Management Plan.		
2513	GR-00208: Configuration Management Database Accuracy	The Contractor must maintain a Configuration Management Database (CMDB) and must achieve and sustain a CMDB accuracy rate of at least 95%, as measured by quarterly reconciliation audit.		
2514	GR-00207: Release and Deployment Records	The Contractor must maintain a release log recording, for each production release: release date, scope of change, and post-release validation outcome.		
2515	GR-00206: Change Management Process	The Contractor must use a documented change management process requiring, for every production change: a documented risk assessment, a named approver, and a documented rollback plan.		
2516	GR-00205: Capacity and Availability Records	The Contractor must maintain capacity and availability records for each in-scope service and must report capacity utilization and availability percentage monthly.		
2517	GR-00204: Service Level Agreements	For each service in the Service Catalog, the Contractor must define and document a Service Level Agreement (SLA) specifying availability, performance, and support response targets.		
2518	GR-00203: Service Catalog	The Contractor must maintain a Service Catalog listing all in-scope services, including service owner, description, and supported business capability, and must update it within 10 business days of any service addition, retirement, or material change.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2519	GR-00201: Service Management Plan	The Contractor must develop, manage, and maintain a State-approved Service Management Plan, that includes all in-scope ITSM processes mapped to their corresponding ITIL 4 practice, including for the core processes of Incident Management, Problem Management, Change Enablement, and Service Request Management: process owner, process steps, and applicable performance targets. The Service Management Plan must be submitted for State review and approval prior to contract go-live, reviewed with the State no less than annually, and updated and re-submitted for approval within 30 days of any material process change.		
2521	GR-00200: Accessibility Issue Reporting and Accommodations	The solution and associated support processes must provide a clearly identified mechanism for users to report accessibility issues and request accommodations. The Contractor must capture, track, and remediate such reports within the same service levels that apply to other critical defects.		
2522	GR-00199: Periodic Accessibility Reviews and Updated ACRs	The Contractor must participate in periodic accessibility reviews with the State at least annually and after any major release affecting the user interface, and must provide updated accessibility test results and Accessibility Conformance Reports as part of these reviews.		
2523	GR-00198: Accessibility Defect Mitigation/Remediation SLAs	The Contractor must classify and remediate accessibility defects in accordance with the agreed service levels, at minimum as follows: critical defects that block users with disabilities from completing primary tasks must be mitigated within five business days and fully remediated within 30 calendar days; high-severity defects that significantly degrade usability must be mitigated within 10 business days and fully remediated within 60 calendar days.		
2524	GR-00197: User-Involved Accessibility/Usability Testing	For solutions identified by the State as high-impact, usability and accessibility testing must include participation by users with disabilities and assistive technologies. The Contractor must document findings from this testing and incorporate them into design and implementation decisions.		
2525	GR-00196: Release Gate for Critical/High Accessibility Defects	The Contractor must not promote a release to production until critical and high-severity accessibility defects identified by the State have been remediated or are covered by an approved exception and interim alternate access method.		
2526	GR-00195: Accessibility Testing: Automated, Manual, AT, Reporting	The Contractor must conduct accessibility testing using automated tools, manual expert review, and assistive technologies, and must provide test plans and results to the State. The Contractor must review accessibility testing results to determine defect severity.		
2527	GR-00194: Semantic Structure for Assistive Navigation	The solution must expose a meaningful semantic structure, including headings, landmarks, labels, and status messages, to enable efficient navigation by users of assistive technologies.		
2528	GR-00193: Keyboard Navigation and Visible Focus	All interactive elements in the solution must be fully usable with keyboard-only input, with visible focus indicators and a logical tab order.		
2529	GR-00192: Full Functionality with Assistive Technologies	The solution must support effective use with common assistive technologies on supported platforms and browsers, including screen readers, screen magnifiers, and speech input tools, without loss of functionality compared to non-assisted use.		
2530	GR-00191: Post-Release VPAT/ACR Update	The Contractor must provide an Accessibility Conformance Report, using the appropriate Voluntary Product Accessibility Template (VPAT) , within 14 business days of any major release that affects the user interface.		
2531	GR-00190: Pre-Go-Live VPAT/ACR Submission	The Contractor must provide a current Accessibility Conformance Report, using the appropriate Voluntary Product Accessibility Template (VPAT) , for each product or major module with a user interface prior to contract award or prior to solution go-live.		
2532	GR-00189: Accessibility Across All User-Facing Components	The solution must meet accessibility requirements across all user-facing components, including portals, mobile applications, administrative interfaces used by staff, generated documents, forms, and embedded widgets or third-party components that affect the user experience.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2533	GR-00188: WCAG AA/508 Compliance and AT Testing	The solution must conform to the most recent version of the Web Content Accessibility Guidelines (WCAG) Level AA for all web and mobile user interfaces, Section 508 requirements for electronic and information technology, and any applicable provisions of the DOJ Web and Mobile App Accessibility Final Rules for public services. The solution must accommodate a wide range of assistive technologies and must be tested to ensure accessibility compliance.		
2534	GR-00187: TTY/TDD Communication Support	Where applicable to the solution's communication channels, the solution must support communication via Teletypewriter (TTY) or Telecommunications Display Device (TDD) for individuals who are deaf, hard of hearing, or have a speech disability.		
2535	GR-00186: Language Services, Disability Aids, and LEP Services	The Contractor must provide language access services for individuals with limited English proficiency, including interpretation, translation, and non-English taglines indicating the availability of language services.		
2536	GR-00185: Plain Language Compliance	The solution must provide information to users in plain language and must provide auxiliary aids and services at no cost to individuals with disabilities.		
2537	GR-00184: Section 504/508 and State Accessibility Compliance	The solution must adhere to all Federal and Vermont accessibility requirements, including Section 504 and Section 508 of the Rehabilitation Act, for web-based intranet and internet information and applications.		
2538	GR-00183: Secure, Searchable Policy Repository with Versioning	The solution must provide secure, scalable, and accessible storage and retrieval of policy and procedure content, with search capabilities, version control, and collaboration support for multiple stakeholders, enabling users to quickly find and access information.		
2539	GR-00182: Scalable CMS with Workflow Management	The solution must include a web content management capability that is scalable and supports workflow management.		
2540	GR-00181: Survey Engine: Create, Distribute, Analyze	If the solution requires a survey engine, the survey engine must provide configuration options to create, distribute, and analyze surveys.		
2541	GR-00180: Browser-Accessible Web URL Access	The solution must be accessible through a URL entered in a web browser.		
2543	GR-00170: Infrastructure Transition and Training	The Contractor must transition and train, as requested and negotiated, any or all infrastructure responsibilities necessary to fulfill the Contractor's contractual obligations to the State or another party upon notification from the State. This includes but is not limited to transference of: The Cloud Service Provider's (CSP) member accounts using the appropriate mechanisms; Complete system inventory for all Contractor services; Contractor cloud boundary access control policies; Network ACLs; Security Groups; Roles; Users; 2FA/Multi-Factor Authentication tooling; Infrastructure as Code programs and scripts; Security and compliance monitoring tools and processes; Audit logs; System monitoring; SIEM tooling and logs; Vulnerability Management; Plan of Action and Milestones; Compliance scans; Data backups; Configuration Management Database items; Disaster Recovery fail-over and recovery routines.		
2544	GR-00169: Turnover and Closeout Plan Development	The Contractor must develop a State-approved Turnover and Closeout Plan that includes a documented process for assessing the fitness of any organization seeking to assume Maintenance and Operations & responsibilities under an extended or transferred licensing arrangement, as authorized by the State.		
2546	GR-00178: Backup RPO and RTO	The Contractor's backup and recovery environment(s) must support mutually agreed Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO), and must include secure backup, recovery, and periodic disaster recovery testing capabilities.		
2547	GR-00168: Air Gap Backup Strategies	The solution must employ backup strategies that include air gap measures.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2548	GR-00167: Immutable Backups	The solution must ensure that all backups are immutable (unchangeable).		
2549	GR-00166: Backup Services for All Environments	Backup and Recovery Services must be in place for Production Environment and Non-Production Environments.		
2550	GR-00165: Backup and Recovery System Compliance	The Contractor must provide a backup and recovery/failover system(s) in compliance with State and Federal rules and regulations to ensure full backup.		
2551	GR-00164: Backup Capabilities at Remote Sites	The Contractor must provide backup and recovery/failover system(s) that ensure full backup of State data and comply with the FBI CJIS Security Policy (current version), NIST SP 800-53 (current revision) controls CP-9 and CP-10, and applicable State of Vermont ADS security and records retention policies, and that meet the recovery targets defined in GR-00178 and NFR-02.		
2552	GR-00163: Training for Recovery and Incident Response Personnel	The Contractor must ensure that personnel who are responsible for systems recovery and cyber incident response are trained in accordance with NIST Publication 800-53 current revision and tested in their ability to execute the contingency and incident response procedures.		
2553	GR-00162: Review of New Business Processes	The Contractor must review any new applicable Contractor provided business processes, including systems and operations under the scope of Subcontractors, for impact on mission critical functionality and update Business Continuity/Disaster Recovery/Cyber Incident Response Plans prior to new business process implementation.		
2554	GR-00161: Training on BC/DR/CIR Plans	In coordination with the State, the Contractor must provide training to Contractor staff and State-identified stakeholders on the execution of the Business Continuity/Disaster Recovery/Cyber Incident Response Plans a minimum of 20 business days prior to implementation of the Contractor's module components, with the implementation of major changes, and annually thereafter.		
2555	GR-00160: Alert Process Implementation	The Contractor must implement a State-approved alert process to handle system-related issues, including notifying State-identified contacts in accordance with the Business Continuity/Disaster Recovery/Cyber Incident Response Plans.		
2556	GR-00159: Update of Key Personnel Contact Information	The Contractor must update key personnel contact information as it relates to the Business Continuity/Disaster Recovery/Cyber Incident Response Plans within one business day of notification of the change.		
2557	GR-00158: Evaluation of Systems and Processes	The Contractor must evaluate systems and business processes in collaboration with the State for criticality and necessity to determine appropriate return to operations time frames during development of both the initial and ongoing Business Continuity/Disaster Recovery/Cyber Incident Response Plans.		
2558	GR-00157: BC/DR/CIR Test and Incident Reports	The Contractor must provide annual test reports to the State within 10 business days of exercise, Business Continuity (BC)/Disaster Recovery (DR) and Cyber Incident Response (CIR) Plan reports within one business day of incident, and BC/DR/CIR Plan updates within one business day of identified deficiency.		
2559	GR-00156: Contingency and Training Plan Adjustments	The Contractor must adjust contingency and training plans to correct deficiencies identified through Business Continuity, Disaster Recovery, and Cyber Incident Response exercises and present updates to the State for approval.		
2560	GR-00155: Documentation of BC/DR/CIR Activities	The Contractor must document all Business Continuity, Disaster Recovery, and Cyber Incident Response activities and report to the State instances where appropriately trained personnel were unable to complete the necessary recovery procedures.		
2561	GR-00154: BC/DR/CIR Exercises After System Changes	The Contractor must perform Business Continuity, Disaster Recovery, and Cyber Incident Response exercises after major system changes as required by the State.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2562	GR-00153: BC/DR/CIR Exercise Activities	Business Continuity (BC), Disaster Recovery (DR), and Cyber Incident Response (CIR) exercises must include activities selected from the BC/DR/CIR Plans to verify the viability of each plan in accordance with NIST CP-4 and IR-8 standards.		
2563	GR-00152: Annual BC/DR/CIR Exercises	The Contractor must perform annual Business Continuity, Disaster Recovery, and Cyber Incident Response exercises, including pre-go-live activities.		
2564	GR-00151: BC/DR/CIR Plan Submission	The Contractor must submit the Business Continuity, Cyber Incident Response, and Disaster Recovery Plan annually or more frequently as directed by the State, such as after a major system change that materially affects the plan.		
2565	GR-00150: BC/DR/CIR Plan Accessibility	The Contractor must provide an up-to-date copy of the Business Continuity/Disaster Recovery/Cyber Incident Response Plan in a secure, highly accessible, centralized online location and at an offsite location approved by the State.		
2566	GR-00149: BC/DR/CIR Plan Standards Compliance	The Contractor must ensure the Business Continuity/Disaster Recovery/Cyber Incident Response Plan's operational and system functions, including systems and operations under the scope of Subcontractors, adhere to Health Insurance Portability and Accountability Act and National Institute of Standards and Technology standards.		
2567	GR-00148: BC/DR/CIR Plan Compliance and Framework	The Contractor must ensure the Business Continuity/Disaster Recovery/Cyber Incident Response Plan: (a) provides a framework for reconstructing vital operations to ensure the safety of employees (b) provides for the resumption of time sensitive operations and services in the event of an emergency (c) provides for initial and ongoing notification procedures (d) complies with all NIST CP-2, NIST 800-61, and IR-8, NIST-800-53 standards.		
2568	GR-00147: Business Continuity, Cyber Incident Response, and Disaster Recovery Plan Development	The Contractor must develop, maintain, and manage a State-approved Business Continuity, Cyber Incident Response, and Disaster Recovery (BC/DR/CIR) Plan.		
2570	GR-00146: Lessons-Learned Report	The Contractor must transcribe the lessons-learned repository to a lessons-learned report within 60 business days after the project is completed.		
2571	GR-00145: Exception Handling Mechanisms	The solution must include exception handling mechanisms to facilitate error correction and/or auditing across all components of the solution without impacting concurrent, overall operations, as well as reporting of exceptions to the State.		
2572	GR-00144: Operating Procedures Guide Development	The Contractor must develop, maintain, and manage a State-approved Operating Procedures Guide.		
2573	GR-00143: Participation in User Groups	The Contractor must invite a State representative to participate in any Contractor-facilitated user group that is associated with any part of the solution.		
2574	GR-00142: Performance Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Performance Management Plan.		
2575	GR-00141: Stakeholder Notification for Maintenance	The Contractor must notify affected State stakeholders of scheduled and emergency maintenance windows and system outages.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2576	GR-00139: Maintenance Approval Protocol	The Contractor must obtain State approval at least ten (10) business days in advance of any scheduled maintenance window or planned system outage. Requests for approval must include sufficient details regarding the anticipated maintenance activities, duration, and potential service impacts. In the event of emergency maintenance or an unplanned system outage, the Contractor must notify the State immediately upon discovery and provide ongoing updates regarding the issue, anticipated impacts, and remediation efforts.		
2577	GR-00138: Maintenance Windows Documentation	The Contractor must document and maintain State-approved standard maintenance windows for system maintenance and downtime that are coordinated across solutions and minimize stakeholder disruption.		
2578	GR-00137: Configuration Management Summary Report	The Contractor must provide a quarterly Configuration Management Summary report providing a high-level overview of any changes to the system baseline configuration and operational usage.		
2579	GR-00136: Change Management Metadata Maintenance	The Contractor must maintain, as part of the Release Management Plan, change management metadata regarding all system application release and operational performance and behavior.		
2580	GR-00135: Configuration Management Process	The Contractor must implement a configuration management process with established promotion and version control procedures for the implementation of a multi-Contractor, integrated system-wide enterprise.		
2581	GR-00134: Network Design and Monitoring Plan	The Contractor must provide, as part of the Release Management Plan, a Network Design and Monitoring Plan for an optimally performing computing and data transporting environment.		
2582	GR-00133: Implementation of Improvements and Changes	The Contractor must implement improvements, changes, or enhancements following a State-approved approach that must enable all other environments to update and mirror the "new" production functionality.		
2583	GR-00132: Modification and Release Flexibility	The Contractor must have the ability to selectively move modifications on a release schedule with State approval, with the flexibility to selectively back out system changes prior to a release (last minute) without significant resources or impact (point in time restore).		
2584	GR-00131: Release Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Release Management Plan.		
2585	GR-00130: Data Quality Review Process	The Contractor must maintain a data quality review process for the identification and resolution of corrupt or bad data.		
2586	GR-00129: Collaboration for Data Resolution	The Contractor must collaborate with the source system Contractor to resolve bad or otherwise corrupt data in accordance with the data quality review process timelines.		
2587	GR-00128: Error and Exception Management	The Contractor must detect, log, notify, and respond appropriately to errors and exceptions in both system and data processing.		
2588	GR-00127: Lessons-Learned Repository Maintenance	The Contractor must, in coordination with the State, maintain a comprehensive lessons-learned repository in the State's Azure DevOps tenant that is a knowledge base of all lessons learned.		
2589	GR-00126: Development Walk-Throughs	The Contractor must conduct development walk-throughs as appropriate to demonstrate to the State that all functions have been completely and accurately planned, developed, and unit tested.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2590	GR-00125: Azure DevOps for Defect Management	The Contractor must utilize Microsoft Azure DevOps, the State-approved online Defect Management tool, for the identification, impact assessment, definition, traceability, verification, and reporting of all defects and resolutions.		
2591	GR-00124: Defect Resolution	The Contractor must perform and complete all work necessary to correct and resolve each defect identified in the solution.		
2592	GR-00123: Maintenance Support Activities	The Contractor must provide Maintenance Support activities during transition to all State parties and/or third parties responsible for maintenance and operations, including making changes to existing functionality and features that are necessary to continue proper system and/or operational services.		
2593	GR-00122: System Maintenance Support Plan Development	The Contractor must develop, maintain, and manage a State-approved System Maintenance Support Plan.		
2595	GR-00120: Phone Help Desk Support	The Contractor must maintain a State-approved help desk support function that enables users to submit requests by phone during State business days, 7 a.m. ET to 7 p.m. ET.		
2596	GR-00119: Web Portal Help Desk Support	The Contractor must maintain a State-approved help desk support function that enables users to submit requests through a web portal during State business days, 7 a.m. ET to 7 p.m. ET.		
2597	GR-00118: Help Desk Plan Development	The Contractor must develop, maintain, and manage a State-approved Help Desk Plan. The Help Desk function must be capable of receiving and accepting submissions and document uploads through the designated portal 24 hours per day, seven (7) days per week, including outside of normal business hours.		
2598	GR-00117: Training Provision	The Contractor must provide training to the State, its agents, and Successor Contractor(s).		
2599	GR-00116: ADA Compliance for Training Materials	The Contractor must develop, maintain, and manage training materials in compliance with Americans with Disabilities Act of 1990 (ADA) standards. Any identified changes to training materials to comply with this requirement must be addressed at no cost to the State.		
2600	GR-00115: User Guide for Training	The User Guide must be used as part of the basis for user training, unless otherwise specified by the State.		
2601	GR-00114: User Guide Development	The Contractor must develop, maintain, and manage a searchable, web-based State-approved User Guide.		
2602	GR-00113: User Training Plan Development	The Contractor must develop, maintain, and manage a State-approved User Training Plan.		
2604	GR-00222: Defect Management in Azure DevOps	The Contractor must document, track, update, remediate, retest, and maintain all defects resulting from testing activities within the State's Azure DevOps tenant in accordance with the State's direction and governance standards.		
2605	GR-00221: Test Case Management in Azure DevOps	The Contractor must manage and maintain all test cases, including those provided by the State, within the State's Azure DevOps tenant in accordance with the State's direction and governance standards.		
2606	GR-00220: State-Authored User Acceptance Test Cases	The Contractor must incorporate into user acceptance testing any test cases, test scenarios, workflows, datasets, or acceptance criteria provided by the State.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2607	GR-00177: User Acceptance Test Case Development	The Contractor must develop and document user acceptance test cases sufficient to validate that the solution satisfies all contractual, general, business, functional, and nonfunctional requirements.		
2608	GR-00112: Quality of Draft Deliverables	The Contractor must ensure that all draft deliverables meet the State's minimum expectations for grammar, spelling, formatting, and overall quality, with revisions made at no additional cost and without impacting the project schedule.		
2609	GR-00111: Time and Resources for Testing	The Contractor must provide sufficient time and resources for all testing performed by the Contractor, and to support testing done by entities other than the Contractor.		
2610	GR-00110: Resources for System Tests	The Contractor must provide resources to assist, complete, and submit results, in a State-approved format, of all comprehensive system(s) tests as documented in the State-approved Test Management Plan.		
2611	GR-00109: Test Case Development for System Changes	The Contractor must develop, maintain, and manage, for each system change, a State-approved suite of test cases that includes the test scope, approach, and tools, and is used to complete testing and provide the documented test results to the State.		
2612	GR-00108: Standards for Data Loading into Non-Production Environments	The solution must adhere to established and mutually agreed-upon standards, procedures, and protocols for data loading into non-production environments.		
2613	GR-00107: User Acceptance Test Environment Implementation	The Contractor must implement a User Acceptance Test (UAT) environment so there is a dedicated environment for UAT activities.		
2614	GR-00106: Device and Resource Access in Test Environments	The Contractor must ensure development and test environments enable access to appropriate devices and resources required to connect to the State environment.		
2615	GR-00104: Data Loading into Non-Production Environments	The solution must enable State-approved users to load data into development, testing, training, and other non-production environments.		
2616	GR-00103: Compliance with ISO/IEC/IEEE 29119-3:2021 Standards	The Test Management Plan must comply with ISO/IEC/IEEE 29119-3:2021 standards.		
2617	GR-00102: Collaboration on Test Management Plan	The Contractor must collaborate with other project Contractors to ensure the Test Management Plan establishes test frameworks and test objectives, supporting all Contractors and partners involved in the solution.		
2618	GR-00101: Test Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Test Management Plan.		
2619	GR-00100: Proactive Quality Control	The Contractor must take a proactive role in identifying and addressing quality control issues within the solution in the effort to meet or exceed performance benchmarks/metrics for the State.		
2620	GR-00099: Quality Assurance Staff Provision	The Contractor must provide adequate and dedicated staff to implement, monitor, and address all quality assurance and improvement activities required under the Quality Management Plan.		
2621	GR-00098: Dedicated Quality Assurance Resource	The Contractor must assign a dedicated resource to lead the quality assurance staff during the design, development, and implementation phases.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2622	GR-00097: Quality Assurance Management	The Contractor must lead, coordinate, and be responsible for all project quality assurance management, documentation quality assurance, and quality assurance testing meetings as requested and required under the Quality Management Plan and/or by the State.		
2623	GR-00094: Quality Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Quality Management Plan that is consistent with ISO 9001:2015, Quality Management System (QMS), Total Quality Management (TQM), SSAE18 SOC 2 Type 2, and Continuous Quality Improvement principles and standards.		
2625	GR-00219: SSA Electronic Information Exchange	Where the solution exchanges electronic information with the Social Security Administration (SSA), the Contractor must comply with the SSA's Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies.		
2626	GR-00215: FIPS 140-2 Validated Cryptographic Modules	All cryptographic modules used to protect State data at rest and in transit must be FIPS 140-2 (or successor) validated.		
2627	GR-00214: Compliance Matrix	The Contractor must include, as an appendix to the System Security and Privacy Plan, a Compliance Cross-Reference Matrix that demonstrates traceability between each applicable law, regulation, standard, and guideline and the specific plan section(s), control(s), or process(es) that address it. At minimum, the matrix must: List each applicable authority separately (NIST SP 800-53, FIPS 200, ARRA, Title XIX of the Social Security Act, HIPAA, HITECH, and any other State or Federal requirement identified as applicable). For each authority, identify the specific requirement or provision being addressed. Map each requirement to the corresponding SSP section, NIST 800-53 control ID(s), policy, or procedure that implements or satisfies it. Distinguish between requirements satisfied through technical/security controls (mapped to the NIST 800-53 Moderate baseline) and those satisfied through privacy, programmatic, or administrative provisions not captured in the control baseline. Identify any gaps where an applicable requirement is not yet fully addressed, along with a remediation plan and target completion date. Be reviewed and updated on the same cycle as the SSP (at least annually and whenever significant system changes occur), and whenever a new or amended law, regulation, or standard becomes applicable.		
2628	GR-00092: Compliance with 42 CFR 434.6(a)(5)	The Contractor must, throughout all phases of this Contract, adhere to 42 CFR 434.6(a)(5), which allows evaluation by Federal Partners through inspection or other means, of the quality, appropriateness, and timeliness of services performed under this Contract.		
2629	GR-00091: System Access for Audits	The Contractor must provide appropriate system access and/or a walk-through of any Contractor facilities and operations as directed by the State to facilitate external and internal audits.		
2630	GR-00089: Security Compliance in Test Environments	The Contractor must ensure that test environments must adhere to the same level of security compliance as required in a production environment, including deidentification of sensitive data,& unless authorized otherwise in writing by the State.		
2631	GR-00088: Security Controls in Development and Test Environments	The Contractor must ensure development and test environments have sufficient security controls in place to prevent unauthorized access.		
2632	GR-00085: System Security and Privacy Plan Development	The Contractor must develop, maintain, and manage a State-approved System Security and Privacy Planthat complies with applicable State and Federal laws, rules, regulations, standards, and guidelines [including NIST SP 800-53 (current revision), FIPS 200, the American Recovery and Reinvestment Act (ARRA), Title XIX of the Social Security Act, HIPAA (1996), and HITECH (2009)] and that: (1) Maps all applicable security controls to the NIST SP 800-53 Moderate baseline. (2) Documents the implementation status of each control. (3) Identifies responsible parties for control ownership and maintenance. (4) Documents inherited, shared, and system-specific controls. (5) Is reviewed and updated at least annually and whenever significant system changes occur. (6) Supports security authorization, assessment, and continuous monitoring activities.		
2634	GR-00084: Tools and Infrastructure for Access	The Contractor must provide the tools and infrastructure to support required access to all systems and data under their scope to all State?authorized stakeholders.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2635	GR-00083: Upgrade/Replacement Plan Implementation	The Contractor must implement each approved upgrade/replacement plan for all software and infrastructure upgrades in accordance with a State-approved schedule.		
2636	GR-00082: Upgrade/Replacement Plan Notification	The Contractor must notify the State and present the upgrade/replacement plan within 20 business days of awareness of a software or infrastructure upgrade notice received from a software/infrastructure contractor, unless the change is categorized as an Emergency Upgrade, in which case notification must be given five days prior to the upgrade date.		
2637	GR-00081: Infrastructure Monitoring	The Contractor must continuously monitor, track, and report monthly to the State infrastructure space and storage trends over the term of the Contract.		
2638	GR-00080: Response Time Requirements Documentation	The Contractor must document and maintain State?approved application?specific response time requirements, measurements, and reporting.		
2639	GR-00079: Infrastructure Optimization Reporting	The Contractor must provide reporting of all infrastructure optimizations annually, or after any major system change, to meet or exceed performance requirements or as requested by the State.		
2640	GR-00078: Infrastructure Optimization	The Contractor must provide the base infrastructure and optimization of all systems under the scope of this Contract to meet required application-specific uptime/response time requirements related to performance requirements, deliverable due dates, and Service Level Agreements.		
2641	GR-00077: Asset Management Plan Development	The Contractor must collaborate with the State to provide, as a subsidiary plan to the Business Design/System Design Document, an Asset Management Plan that describes the process the Contractor must use to manage applicable technology assets for the duration of the Contract within a multi-Contractor, integrated system-wide enterprise solution. This plan must include: (a) Hardware/software inventory (including location) (b) Procurement information (c) Contract information (d) License management.		
2642	GR-00076: Maintenance and Operations Responsibility	The Contractor must retain all responsibility and costs for all software, hardware, and infrastructure necessary to fulfill their obligations of this Contract.		
2643	GR-00075: Network Connectivity Responsibility	The Contractor must retain the responsibility and costs for providing network connectivity and access to all systems and data under their scope to all State authorized stakeholders.		
2644	GR-00074: Environment Management Responsibility	The Contractor must be solely responsible for the end-to-end oversight and management of all environments during implementation, transition, and maintenance and operations such that performance metrics and service level agreements are met.		
2645	GR-00073: Infrastructure Management	The Contractor must implement, host (or arrange for third-party hosting), operate, maintain, and manage all infrastructure, including all hardware, software, middleware, and licenses necessary for successful operation of all systems and services under the Contract.		
2647	GR-00071: Database Documentation	The Contractor must provide documentation that describes the contents, format, and structure of all databases and the relationships among all database objects.		
2648	GR-00070: Database Models Update Protocol	The Contractor must complete all conceptual, logical, and physical models to reflect the most current updates or changes based on approval by the State 10 business days prior to implementation of the planned change. Updates must be published to users at the time of implementation.		
2649	GR-00069: Repository Storage for Database Models	The Contractor must store all conceptual, logical, and physical models in a State-approved repository.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2650	GR-00068: Database Models Documentation	The Contractor must document and keep current all conceptual, logical, and physical models for all database service layers and supporting data stores and make the models available online to the State.		
2651	GR-00067: Interface Control Document Development	The Contractor must develop, maintain, and manage a State-approved Interface Control Document that documents all data elements, processes, methodologies, mechanisms, protocols, and other related information for each data source.		
2652	GR-00066: Operational, System, and Technical Process Documentation	The Contractor must create and keep current documentation of all operational, system, and technical processes as they relate to the solution.		
2653	GR-00065: Business Design/System Design Document Development	The Contractor must develop, maintain, and manage a State-approved Business Design/System Design Document.		
2655	GR-00064: Presentation Approval Protocol	The Contractor must secure State approval prior to any representation or presentation of documentation related to this project, including any local, State, national conferences, or other public or private forums.		
2656	GR-00063: Meeting Records Maintenance	The Contractor must maintain complete and detailed records of all Contractor-facilitated meetings with the State related to the Contract, software development lifecycle documents, presentations, project artifacts, and any other interaction and post and maintain these artifacts in the Project Management Repository within five business days of the meeting or interaction.		
2657	GR-00062: Documentation Revision Protocol	The Contractor must revise any required documentation deliverable if requested to do so by the State.		
2658	GR-00061: Documentation Standards Alignment	The Contractor must maintain a documentation standard that aligns with the standards and templates set forth by the State and other contracted Contractors and utilize the approved standard throughout the life of the Contract.		
2659	GR-00058: Documentation Software Compliance	The Contractor must ensure all documentation is prepared and accessible using current State standard/approved software packages.		
2660	GR-00057: Documentation Availability and Retention	The Contractor must ensure all documentation is maintained electronically and readily accessible online in Microsoft-compatible formats or Adobe PDF format. All documentation must be electronically maintained, retained, archived, and restored in accordance with applicable document and data retention laws, regulations, and requirements, including compliance with any applicable litigation hold.		
2661	GR-00056: Document Repository Usage	The Contractor must utilize the State-approved Project Management Repository as well as any other State-required document repository to maintain system?related business, technical, and operational documentation.		
2662	GR-00055: Documentation Standards Compliance	System and technical documentation must utilize State approved language, diagrams, and structure.		
2663	GR-00054: System and Technical Documentation Maintenance	The Contractor must create and maintain all system and technical documentation for the solution.		
2664	GR-00053: Documentation Preparation and Submission	The Contractor must prepare, update, revise, and submit to the State for approval all operational, systems, or reporting-based documentation (in all original forms/media) as they relate to system changes, maintenance, or modification work requests.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2665	GR-00052: Project Deliverables Maintenance	The Contractor must update and maintain all Project Deliverables on a mutually agreed upon cadence as approved by the State.		
2666	GR-00051: Deliverables Management Plan Development	The Contractor must review, provide feedback on, sign-off, and conform to the project's State-authored Deliverables Management Plan.		
2667	GR-00050: Public-Facing Communication Restrictions	The Contractor must ensure that the Contractor's own name, logo, or any reference to the Contractor are not included in any public-facing communications with respect to this project, unless approved by the State.		
2668	GR-00049: Brand Standards Compliance	The Contractor must ensure all communications conform to State of Vermont brand standards as issued by the Chief Marketing Office.		
2669	GR-00048: Inquiry Response Protocol	The Contractor must not respond to legislative, executive level, or media inquiries regarding the project unless directed by the State, except where required by law.		
2670	GR-00047: Inquiry Notification	The Contractor must notify the State of all legislative, executive level, and media inquiries with respect to this project and forward any such inquiries to the State within one business day of the Contractor's awareness of said inquiry.		
2671	GR-00046: Communication Management Plan Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Communication Management Plan.		
2673	GR-00045: Forum Material Preparation Assistance	Upon State request, the Contractor must provide staff and resources to assist the State with preparing and reviewing materials planned to be shared at forum(s), such as national organizations and conferences, on efforts related to this Contract.		
2674	GR-00044: Legal Information Provision	The Contractor must provide, at no cost to the State, information and data as requested by the State to fulfill requests for litigation, subpoenas, open record requests, or other legal actions.		
2675	GR-00043: Subcontractor Contact Identification	For any Subcontract, the Contractor must identify a designated Subcontractor contact who is accessible to the State.		
2676	GR-00042: Subcontractor Work Responsibility	The Contractor must be responsible/accountable for all subcontracted work assigned, including responsibility for enforcement and oversight of subcontractors and their compliance with all State and Federal contractual terms/provisions as included within this Contract.		
2677	GR-00041: Subcontractor Agreements Availability	The Contractor must make all Subcontractor agreements available to the State upon request.		
2678	GR-00040: Invoice Correction and Reissue	The Contractor must correct and reissue invoices within five business days of State notification.		
2680	GR-00218: FTI Annual Certification	The Contractor may be required to obtain an initial certification, and subsequent annual recertification's, via a signed confidentiality statement, for each officer or employee authorized to access Federal Tax Information. The Contractor may be required to retain these signed statements and provide them to the State or IRS upon request.		
2681	GR-00216: FTI Personnel Background Screening	Contractor personnel granted access to Federal Tax Information (FTI) may be required to first meet the background-check requirements defined in IRS Publication 1075. The Contractor may be required to maintain, and provide upon request to the State or IRS, a current list of personnel authorized to access FTI.		

Docusign Envelope ID: C9152619-EB96-8131-8263-FCB6338A1607

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2682	GR-00179: Criminal Background Check Follow Up	The Contractor must conduct a follow-up criminal investigation every two years for any staff supporting this contract, if requested by the State.		
2683	GR-00038: Onboarding and Training Processes	The Contractor must develop and apply onboarding and training processes for new staff and turnover in staff.		
2684	GR-00037: Costs for Personnel Changes	The Contractor must bear the costs of changes, hires, or reassignment of Contractor personnel.		
2685	GR-00036: Resource Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Resource Management Plan.		
2686	GR-00035: Access Removal Process	The Contractor must keep current a State-approved process for immediate removal, with just cause or reason, physical and remote access to systems and facilities for Contractor or Subcontractor employees deemed unfit to continue employment.		
2687	GR-00034: Cross-Training Staff	The Contractor must cross train its staff to prevent loss of knowledge and expertise when staff leave, as well as to minimize negative impacts to project timelines due to resource availability.		
2688	GR-00033: Licensure Maintenance	The Contractor must ensure that all licensed Contractor staff maintain current licensure required for their role on the project, with no State or Federal sanctions.		
2689	GR-00031: Criminal Background Check	The Contractor must ensure that any employee accessing State systems or data has passed a criminal background check prior to accessing the State system or data, at no cost to the State.		
2690	GR-00030: Personnel Replacement for Cause	The Contractor must replace or reassign personnel supporting this Contract for cause (i.e., where the State can demonstrate a reason) at the State's request. The State shall report to Contractor any concerns regarding Contractor Personnel that may lead the State to make such a request with sufficient detail and time for Contractor to take corrective measures.		
2691	GR-00029: Personnel Replacement Notification	The Contractor must notify the State within one business day of the replacement, reassignment, resignation, or termination of any personnel directly supporting this Contract.		
2692	GR-00028: Personnel Change Notification	The Contractor must provide the State 20 business days or more advance notice of any plans to change, hire, or reassign personnel supporting this Contract.		
2693	GR-00027: Vacant Position Management	The Contractor must ensure vacant positions supporting this Contract are filled within 60 calendar days of date of vacancy or obtain written approval by the State for extended vacancies.		
2694	GR-00026: Resume Submission	The Contractor must provide the State with resumes for Contractor and Subcontractor staff working on the project.		
2695	GR-00025: Organizational Chart Development	The Contractor must develop, maintain, and manage a State-approved Organizational Chart of all Contractor and Subcontractor personnel working on the project.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2696	GR-00024: Personnel Table Maintenance	The Contractor must keep current, on the State's SharePoint site, a Personnel Table of all Contractor staff and Subcontractor staff associated with the project. The Personnel Table must provide: (a) Full name (b) Business phone number (c) Business email address (d) Project role (e) Project responsibilities.		
2698	GR-00223: ADO License Costs	The Contractor must ensure all personnel have the Azure DevOps (ADO) licenses required by the State and maintain such licenses for the duration of the Contract at no cost to the State; if the State provisions any ADO licenses for Contractor personnel, the Contractor must reimburse the State for the actual cost of those licenses.		
2699	GR-00023: Deliverables Matrix Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Deliverables Matrix.		
2700	GR-00022: Schedule Management Plan Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Schedule Management Plan.		
2701	GR-00021: Project Kickoff Deck Development	The Contractor must develop a State-approved Project Kickoff Deck.		
2702	GR-00020: Scope Management Plan Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Scope Management Plan.		
2703	GR-00019: Monitoring Industry Changes	The Contractor must monitor and inform the State of industry changes that may have an impact on business processes or on systems covered by the Contract, so that the State can prepare for and implement any necessary updates and stay aligned with industry changes and best practices.		
2704	GR-00018: Impact of Data Source Changes	The Contractor must identify the impact of data source changes to all solution components and capabilities, so that the changes may be verified to be in accordance with the approved Change Management Plan.		
2705	GR-00017: Collaboration in Change Management	The Contractor must collaborate with all State-approved Contractors and Subcontractors under the direction of the State Change Control Board to manage change within a multi-Contractor, integrated systems solution as it relates to any system- or non-system-based changes, modifications, or maintenance activities, efforts, tasks, or projects		
2706	GR-00016: Change Management Plan Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Change Management Plan.		
2707	GR-00015: Participation in Project Steering Committee	The Contractor must, upon Contract execution, participate in the project Steering Committee, which will govern and steer the project.		
2708	GR-00014: Implementation Plan Development	The Contractor must develop, maintain, and manage a State-approved Implementation Plan that outlines the approach for the design, development, and implementation of all technology and services in accordance with the solution scope.		
2709	GR-00013: Risk Management Plan Development	The Contractor must develop, maintain, and manage a State-approved Risk Management Plan.		
2710	GR-00012: Requirements Management in Azure DevOps	The Contractor must maintain and manage all requirements, user stories, and business rules in the State's Azure DevOps (ADO) tenant per the direction of the State.		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2711	GR-00011: Elicitation of User Stories and Requirements	The Contractor must collaborate with the State to elicit user stories and requirements at sufficient detail to ensure the solution meets the needs of the State.		
2712	GR-00010: Business Analysis Methodologies Compliance	The Contractor must follow business analysis methodologies that are consistent with the International Institute for Business Analysis (IIBA) Guide to Business Analysis Body of Knowledge (BABOK) v3.		
2713	GR-00009: Business Analysis Plan Review	The Contractor must review, provide feedback on, signoff, and conform to the project's State-authored Business Analysis Plan.		
2714	GR-00008: Conflict Escalation Protocol	If an inter-vendor conflict cannot be resolved collaboratively within five business days, the Contractor must escalate the issue to the State no later than one business day thereafter.		
2715	GR-00007: Participation in Cross-Vendor Forums	The Contractor must participate in State-facilitated cross-vendor forums, and align to shared standards, environments, calendars, and schedules as directed by the State.		
2716	GR-00006: Collaboration with Contractors and Subcontractors	The Contractor must actively collaborate with all State-approved Contractors and Subcontractors, sharing information, designs, and schedules necessary to achieve an integrated solution.		
2717	GR-00005: Decision, Risk, and Issue Log Maintenance	The Contractor must maintain a decision log, risk log, and issue log (in State-approved tools), updated at least weekly, with clear owners and due dates.		
2718	GR-00004: Weekly Project Schedule Submission	The Contractor must provide, on a weekly basis, a current project schedule in Microsoft Project format (v2013 or later).		
2719	GR-00003: EPMO Project Lifecycle Activities	The Contractor must complete the activities specified in the Enterprise Project Management Office (EPMO) Project Lifecycle as published on the EPMO public-facing website.		
2720	GR-00002: SharePoint Online Repository Usage	The Contractor must use the State-managed SharePoint Online Project Management Repository in accordance with State standards and expectations.		
2721	GR-00001: Project Management Methodologies Compliance	The Contractor must follow project management methodologies as directed by the State that are consistent with the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) Guide v7 and Agile project management.		
2723	CJIS Security Policy: Performance Management Plan	Per CJIS Security Policy: A Performance Management Plan must contain the following sections - Performance Management Framework, Service Catalog & Service SLAs, Technical Performance Monitoring, Response Time Requirements, Incident & Problem Management Performance, Reporting & Transparency, User Satisfaction Measurement, SLA Breach Management & Remediation, Performance Review Governance		
2724	CJIS Security Policy: Business Continuity, Disaster Recovery & Critical Incident Response Plan (BC/DR/CIRP)	Per CJIS Security Policy: The following sections must appear in the BC/DR/CIRP - Disaster Classification & Triggering Events, Infrastructure Inventory & Dependencies, Backup Architecture & Validation, Alernate Site Technical Configuration, RPO and RTO Targets, Continuity Strategy, Resource Requirements, Plan Activation Criteria and Authority, Notification and Communication Processes, Backup and Recovery Procedures, Continuity of Operations Procedures, System Validation & Integrity Verification, Return to Normal Operations Criteria, Training & Awareness, Exercise Program, Plan Maintenance & Continuous Improvement,		

ADO ID	Title	Requirement	Comply ?	Vendor's Description of Compliance
2725	CJIS Security Policy: System Maintenance Plan (SMP)	Per CJIS Security Policy the following sections must be reflected in a System Maintenance Plan (SMP) - Maintenance Philosophy & Objectives, Maintenance Windows, Authorized Maintenance Personnel, Nonlocal (Remote) Maintenance Controls, Maintenance Tools & Management, Security Patch Management, Software & Firmware Integrity, Controlled Maintenance Records, Maintenance Impact on System Security, Timely Maintenance & SLA Compliance.		
2726	CJIS Security Policy: Release Management Plan (RMP)	Per CJIS Security Policy: The following sections must appear in the RMP - Release Types & Approval Authority, Environment Management, Change Management Process, Security Impact Assessment, Security Patch Management & Flaw Remediation, Software Integrity Verification, Release Testing Requirements, Network Design & Monitoring, Configuration Management, Maintenance Windows, Release Records & Reporting		
2727	CJIS Security Policy: Data Interface Design & Control Document (DIDCD)	Per CJIS Security Policy: The following sections must appear in the Data Interface Design & Control Document (DIDCD) - Interface Inventory, Data Classification by Interface, Information Exchange Agreements, Interface Security Controls, Ports Protocols & Services, API Specifications, Data Validation & Error Handling, Audit & Monitoring Controls, Third-Party & Subprocessor Interface Controls, Interface Testing & Validation, Interface Change Control.		
2728	CJIS Security Policy: Supply Chain Risk Management Plan	CJIS Security Policy considers this a Supply Chain Risk Management Plan and requires the following sections - Supply Chain Risk Tolerance & Policy, Supply Chain Inventory & Mapping, Supply Chain Risk Assessment, CJIS Compliance Assessment for Key Suppliers, Preferred Supplier Standards & Acquisition Controls, Supply Chain Risk Mitigations, Supply Chain Monitoring, Supply Chain Notification Agreements, Component Disposal & End-of-Life, SCRM Plan Governance & Maintenance		
2729	CJIS Security Policy: System Design Document	Per CJIS Security Policy: The following sections must appear in the System Design Document - System Overview & Architecture, Technology Stack, Data Architecture, Security Architecture, Authentication & Authorization Architecture, Network Architecture, Integration Architecture, High Availability & Scalability Architecture, Audit & Logging Architecture, Development & Deployment Architecture		
2730	GR-00217: FTI System Controls	A system that receives, processes, stores, or transmits Federal Tax Information may be required to implement the managerial, operational, and technical controls required by IRS Publication 1075.		