



Department of Administration  
Purchasing Division  
2019 Washington Street East  
Post Office Box 50130  
Charleston, WV 25305-0130

# State of West Virginia Master Agreement

Order Date: 05-13-2025

CORRECT ORDER NUMBER MUST  
APPEAR ON ALL PACKAGES, INVOICE  
AND SHIPPING PAPERS. QUESTIONS  
CONCERNING THIS ORDER SHOULD BE  
DIRECTED TO THE DEPARTMENT  
CONTACT.

Order Number:	CMA 0511 3245 BSS2500000003 1	Procurement Folder:	1574748
Document Name:	CHILD WELFARE MOBILE APPLICATION COMMUNICATION SOFTWARE	Reason for Modification:	
Document Description:	CHILD WELFARE MOBILE APPLICATION COMMUNICATION SOFTWARE		
Procurement Type:	Central Master Agreement		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way		
Free on Board:	FOB Dest, Freight Prepaid		

Effective Start Date: 2025-06-01  
Effective End Date: 2030-05-31

## VENDOR

Vendor Customer Code: VS0000019201  
ELIXIR LAB USA INC  
267 KENTLANDS BLVD STE 5092  
GAITHERSBURG MD 20878  
US  
Vendor Contact Phone: 3123423776 Extension:

### Discount Details:

	Discount Allowed	Discount Percentage	Discount Days
#1	No	0.0000	0
#2	No		
#3	No		
#4	No		

## DEPARTMENT CONTACT

Requestor Name: Anthony J Walizer  
Requestor Phone: (304) 356-2915  
Requestor Email: anthony.j.walizer@wv.gov

**2025**  
FILE LOCATION

## INVOICE TO

ADMINISTRATIVE SERVICES ASSISTANT - 304-356-4528  
HEALTH AND HUMAN RESOURCES  
BSS - COMMISSIONER'S OFFICE  
350 CAPITOL ST, RM 730  
CHARLESTON WV 25301-3711  
US

## SHIP TO

ADMINISTRATIVE SERVICES ASSISTANT - 304-356-4528  
HEALTH AND HUMAN RESOURCES  
BSS - COMMISSIONERS OFFICE  
350 CAPITOL ST, RM 730  
CHARLESTON WV 25301-3711  
US

CR 5-22-25

Purchasing Division's File Copy

Total Order Amount:

Open End

PURCHASING DIVISION AUTHORIZATION

DATE: 5/13/25  
ELECTRONIC SIGNATURE ON FILE

ATTORNEY GENERAL APPROVAL AS TO FORM

DATE: 5/23/25  
ELECTRONIC SIGNATURE ON FILE

ENCUMBRANCE CERTIFICATION

DATE: 5-23-25  
ELECTRONIC SIGNATURE ON FILE

**Extended Description:**

THE VENDOR, ELIXIR LAB USA INC, (D/B/A) CARDINALITY.AI., AGREES TO ENTER WITH THE AGENCY, WEST VIRGINIA DEPARTMENT OF HUMAN SERVICES, INTO AN OPEN-END CONTRACT TO PROVIDE A CHILD WELFARE MOBILE APPLICATION COMMUNICATION SOFTWARE SOLUTION, MAINTENANCE, AND SUPPORT PER THE TERMS AND CONDITIONS, SPECIFICATIONS, BID REQUIREMENTS, ADDENDUM 1 ISSUED 12/19/2024, AND THE VENDOR'S PROPOSAL DATED 02/06/2025, INCORPORATED HEREIN BY REFERENCE, AND MADE A PART OF HEREOF.

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	83121700				0.000000
	<b>Service From</b>	<b>Service To</b>			
	2025-06-01	2030-05-31		<b>Service Contract Amount</b>	
Commodity Line Description: Child Welfare mobile application					3597414.40

**Extended Description:**

Years 1-2 Total Cost: \$1,792,840.00  
Year 3 Total Cost: \$593,610.00  
Year 4 Total Cost: \$593,610.00  
Year 5 Total Cost: \$617,354.40

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
2	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>			
	2025-06-01	2030-05-31		<b>Service Contract Amount</b>	
Commodity Line Description: Account Manager					0.00

**Extended Description:**

Account Manager  
Year 1-2 Hourly Rate: \$150.00  
Year 3-5 Hourly Rate: \$156.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
3	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>			
	2025-06-01	2030-05-31		<b>Service Contract Amount</b>	
Commodity Line Description: Project Manager					0.00

**Extended Description:**

Project Manager  
Year 1-2 Hourly Rate: \$125.00  
Year 3-5 Hourly Rate: \$130.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
4	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>			
	2025-06-01	2030-05-31		<b>Service Contract Amount</b>	
Commodity Line Description: Business Lead					0.00

**Extended Description:**

Business Lead  
Year 1-2 Hourly Rate: \$120.00  
Year 3-5 Hourly Rate: \$125.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
5.	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Technical Lead

**Extended Description:**

Technical Lead

Year 1-2 Hourly Rate: \$120.00

Year 3-5 Hourly Rate: \$125.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
6	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Implementation Manager

**Extended Description:**

Implementation Manager

Year 1-2 Hourly Rate: \$125.00

Year 3-5 Hourly Rate: \$130.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
7	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Operations Manager

**Extended Description:**

Operations Manager

Year 1-2 Hourly Rate: \$120.00

Year 3-5 Hourly Rate: \$125.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
8	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Quality Assurance Manager

**Extended Description:**

Quality Assurance Manager

Year 1-2 Hourly Rate: \$110.00

Year 3-5 Hourly Rate: \$114.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
9	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Testing Manager

**Extended Description:**

Testing Manager

Year 1-2 Hourly Rate: \$110.00

Year 3-5 Hourly Rate: \$114.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
10	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Info Security Architect/Privacy Data Protection Officer

**Extended Description:**

Information Security Architect/Privacy Data Protection Officer

Year 1-2 Hourly Rate: \$140.00

Year 3-5 Hourly Rate: \$145.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
11	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Developer

**Extended Description:**

Developer

Year 1-2 Hourly Rate: \$110.00

Year 3-5 Hourly Rate: \$115.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
12	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Tester

**Extended Description:**

Tester

Year 1-2 Hourly Rate: \$100.00

Year 3-5 Hourly Rate: \$104.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
13	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Integration Lead

**Extended Description:**

Integration Lead

Year 1-2 Hourly Rate: \$120.00

Year 3-5 Hourly Rate: \$125.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
14	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Solution Architect

**Extended Description:**

Solution Architect

Year 1-2 Hourly Rate: \$120.00

Year 3-5 Hourly Rate: \$125.00



Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
15	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** UI/UX Designer

**Extended Description:**

UI/UX Designer

Year 1-2 Hourly Rate: \$100.00

Year 3-5 Hourly Rate: \$104.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
16	80000000				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		0.00	

**Commodity Line Description:** Support Engineer

**Extended Description:**

Support Engineer

Year 1-2 Hourly Rate: \$100.00

Year 3-5 Hourly Rate: \$104.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
18	83121700				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		755000.00	

**Commodity Line Description:** Digital Signing Tools

**Extended Description:**

Digital Signing Tools

Annual Cost: \$151,000.00

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
19	83121700				0.000000
	<b>Service From</b>	<b>Service To</b>		<b>Service Contract Amount</b>	
	2025-06-01	2030-05-31		400000.00	

**Commodity Line Description:** Mobile Responsive Solution

**Extended Description:**

Mobile Responsive Solution

Cost: \$400,000.00

**STATE OF WEST VIRGINIA**  
**ORDER OF PRECEDENCE AND ADDITIONAL TERMS AGREEMENT**

**THIS ORDER OF PRECEDENCE AND ADDITIONAL TERMS AGREEMENT**, by and between Cardinality ("Vendor") and the State of West Virginia ("State"), collectively referred to herein as (the "Parties"), is intended to provide an order of priority for the various documents that comprise the contract resulting from CRFP 0511 BSS2500000001 ("Contract") and to add certain required terms to the Contract.

The Parties Agree as follows:

1. **Order of Precedence:** The Contract is comprised of the documents listed in this section. The terms and conditions contained in the various documents shall be interpreted according to the priority given to the Contract document in this section.

**Contract Documents:**

- a. This Document - First in priority.
- b. West Virginia General Terms and Conditions - Second Priority
- c. Cardinality Terms and Conditions - Third Priority.
- d. Additional Vendor Documents - Fourth Priority.

2. **Additional Contract Terms.** The following additional terms are added to the Contract:

a. **VOID CONTRACT CLAUSES** - This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

b. **CONFIDENTIALITY** - The State/Agency acknowledges that during the performance of this Agreement, it may be provided with or otherwise gain access to confidential and proprietary information, data, materials, and intellectual property owned or controlled by the Vendor (collectively "Vendor Confidential Information" or "Exempt Information"). Such Vendor Confidential information includes, but is not limited to, trade secrets, proprietary information or financial information, including any formulae, plan, pattern, process, tools, 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 agrees that it shall treat all such Vendor Confidential Information as strictly confidential and shall not disclose, distribute, or use it for any purpose other than as explicitly necessary for the performance of its obligations under this agreement. The State shall not, directly or indirectly use Vendor Confidential Information for any purpose other than as expressly permitted under this Agreement, and shall not reverse-engineer, decompile, or disassemble any proprietary materials provided by the Vendor. The Vendor acknowledges that State contracts are public records under the West Virginia Freedom of information Act ("FOIA") (W. Va. Code §29B-a-1, et seq.) and public procurement laws. This Contract and other public records may be disclosed without notice to the vendor at the State's sole discretion. Any "Vendor Confidential Information" which requires the confidential treatment by the State described above or which is exempt from FOIA disclosure shall be identified by the Vendor as such in order to receive such confidential treatment. The State shall not be responsible for evaluating Vendor Information to identify if it falls into the categories described above, but shall treat information

identified as confidential with the above-described care. These provisions shall be construed to be consistent with FOIA.

**c. FORCE MAJEURE:** Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, any act of war, hostile foreign action, nuclear explosion, riot, strikes, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God. In the event of any such occurrence, the affected party shall promptly notify the other party in writing of the nature of the event, the anticipated duration, and the effect it has on the performance of its obligations. The affected party shall take reasonable steps to mitigate the impact of the event and to resume performance as soon as possible after the event has concluded or circumstances have improved.

**d. INTELLECTUAL PROPERTY:** The Vendor acknowledges and agrees that any intellectual property developed, created, or conceived by the Vendor in the performance of this Contract, including but not limited to software, inventions, designs, documents, data, or other works, which are based on or derived from State-owned resources, funding, or materials, shall be considered the exclusive property of the State. The Vendor agrees to assign and hereby assigns all rights, title, and interest in such intellectual property to the State.

**e. PREEXISTING INTELLECTUAL PROPERTY:** The Vendor retains all rights, title, and interest in any intellectual property that is owned or developed by the Vendor prior to the effective date of this Contract ("Preexisting IP"). The State acknowledges and agrees that the Vendor's Preexisting IP is and shall remain the sole property of the Vendor. The State shall not modify, distribute, or sublicense any Preexisting IP.

**f. ISRAEL BOYCOTT:** Vendor understands and agrees that pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**g. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

The Parties are signing this Agreement on the date stated below the signature.

**VENDOR:**

Cardinality, Inc.

By: Anna Harper

It's: Chief Administrative Officer

Signed:



Date: 05/02/2025

**STATE AGENCY:**

West Virginia, Department of  
Human Services

By: BRYAN D. ROSEN

It's: INTERIM EDO

Signed:



Date: 5/5/25

## **GENERAL TERMS AND CONDITIONS:**

**1. CONTRACTUAL AGREEMENT:** Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

**2.1. "Agency" or "Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

**2.2. "Bid" or "Proposal"** means the vendors submitted response to this solicitation.

**2.3. "Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

**2.4. "Director"** means the Director of the West Virginia Department of Administration, Purchasing Division.

**2.5. "Purchasing Division"** means the West Virginia Department of Administration, Purchasing Division.

**2.6. "Award Document"** means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

**2.7. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

**2.8. "State"** means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

**2.9. "Vendor" or "Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**3. CONTRACT TERM; RENEWAL; EXTENSION:** The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☒ **Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of five (5) years. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within \_\_\_\_\_ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within \_\_\_\_\_ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for \_\_\_\_\_ years;

☐ the contract may be renewed for \_\_\_\_\_ successive \_\_\_\_\_ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as \_\_\_\_\_), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in \_\_\_\_\_

**4. AUTHORITY TO PROCEED:** Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

**5. QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☐ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☐ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☒ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.



☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

**6. EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

**7. REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐☐☐☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

**8. INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☒ **Commercial General Liability Insurance** in at least an amount of: \$1,000,000.00 per occurrence.

☒ **Automobile Liability Insurance** in at least an amount of: \$1,000,000.00 per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: \_\_\_\_\_ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: \_\_\_\_\_ per occurrence.

☒ **Cyber Liability Insurance** in an amount of: \$1,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: \_\_\_\_\_ per occurrence.

☐ **Aircraft Liability** in an amount of: \_\_\_\_\_ per occurrence.

☐

☐

☐

☐

**9. WORKERS' COMPENSATION INSURANCE:** Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**10. VENUE:** All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

**11. LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ \_\_\_\_\_ for \_\_\_\_\_.

☐ Liquidated Damages Contained in the Specifications.

☒ Liquidated Damages Are Not Included in this Contract.

**12. ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

**14. PAYMENT IN ARREARS:** Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**17. ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**18. FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

**19. CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

**20. TIME:** Time is of the essence regarding all matters of time and performance in this Contract.

**21. APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

**22. COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**23. ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

**24. MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

**25. WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

**26. SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**28. WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in [www.state.wv.us/admin/purchase/privacy](http://www.state.wv.us/admin/purchase/privacy).

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

**DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.**

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**32. LICENSING:** In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**34. VENDOR NON-CONFLICT:** Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.



**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**37. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

**38. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

**39. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☒ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at [purchasing.division@wv.gov](mailto:purchasing.division@wv.gov).

**40. BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

**41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS:** Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open hearth, basic oxygen, electric furnace, Bessemer or other steel making process.
- c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
  1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
  2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**44. PROHIBITION AGAINST USED OR REFURBISHED:** Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**DESIGNATED CONTACT:** Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) : Anna Harper, Chief Administrative Officer

(Address): 267 Kentlands Boulevard Suite #5092, Gaithersburg, MD 20878

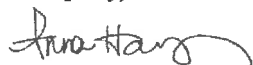
(Phone Number) I (Fax Number): (513) 907-1068

(email address): sales@cardyai.com

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code s SA-3-62, which automatically voids certain contract clauses that violate State law, and that pursuant to W. Va. Code SA-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Elixir Lab USA Inc. d/b/a Cardinality.ai  
(Company)



(Signature of Authorized Representative)

Anna Harper, Chief Administrative Officer (06-Feb-2025)  
(Printed Name and Title of Authorized Representative) (Date)

(513) 907-1068  
(Phone Number) (Fax Number)

sales@cardyai.com  
(Email Address)

Revised 10/17/2024

Request for Proposal

## General Terms and Conditions

### Team Cardinality's Exceptions

ATTACHMENT/S EC/PG.NO	Exception or Addition	Reason	PROPOSED VERBIAGE
General Terms and conditions – RFP Sec 30, Privacy, Security and Confidentiality	Additional language	The purpose of the clause is to protect the Vendor's confidential and proprietary information from being disclosed, used, or misused during the performance of the agreement and to clarify the confidentiality obligations of the State/Agency and to provide a legal framework for the protection of Vendor Confidential Information in alignment with applicable laws governing trade secrets, intellectual property, and business privacy.	<b>Vendor Confidential Information.</b> The State/Agency acknowledges that during the performance of this Agreement, it may be provided with or otherwise gain access to confidential and proprietary information, data, materials, and intellectual property owned or controlled by the Vendor (collectively, " <b>Vendor Confidential Information</b> " or " <b>Exempt Information</b> "). Such Vendor Confidential Information includes, but is 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 agrees that it shall treat all such Vendor Confidential Information as strictly confidential and shall not disclose, distribute, or use it for any purpose other than as explicitly necessary for the performance of its obligations under this Agreement. The State shall not, directly or indirectly, use Vendor Confidential Information for any purpose other than as expressly permitted under this Agreement, and shall not reverse-engineer, decompile, or disassemble any proprietary materials provided by the Vendor.
General Terms and conditions – RFP	Additional language	Force Majeure clause is being added to protect both parties from unforeseen events, clarifies expectations for handling these situations, and aims to prevent conflicts related to uncontrollable circumstances.	<b>FORCE MAJEURE:</b> Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God. In





			the event of any such occurrence, the affected party shall promptly notify the other party in writing of the nature of the event, the anticipated duration, and the effect it has on the performance of its obligations. The affected party shall take reasonable steps to mitigate the impact of the event and to resume performance as soon as possible after the event has concluded or circumstances have improved.
General Terms and conditions -- RFP	Additional language	Requesting the inclusion of an Intellectual Property (IP) clause to clarify the ownership and use of intellectual property developed, created, or conceived during the performance of the contract and also safeguarding the Vendor's rights to any intellectual property developed prior to or independent of the contract.	<p><b>INTELLECTUAL PROPERTY.</b> The Vendor acknowledges and agrees that any intellectual property developed, created, or conceived by the Vendor in the performance of this Contract, including but not limited to software, inventions, designs, documents, data, or other works, which are based on or derived from State-owned resources, funding, or materials, shall be considered the exclusive property of the State/Agency. The Vendor agrees to assign and hereby assigns all rights, title, and interest in such intellectual property to the State/Agency.</p> <p><b>PREEXISTING INTELLECTUAL PROPERTY.</b> The Vendor retains all rights, title, and interest in any intellectual property that is owned or developed by the Vendor prior to the effective date of this Contract, or independently of the services provided under this Contract ("Preexisting IP"). The State acknowledges and agrees that the Vendor's Preexisting IP is and shall remain the sole property of the Vendor. The State shall not modify, distribute, or sublicense any Preexisting IP.</p>

### 3. Response to Project Goals and Objectives (§ 4.2.1)

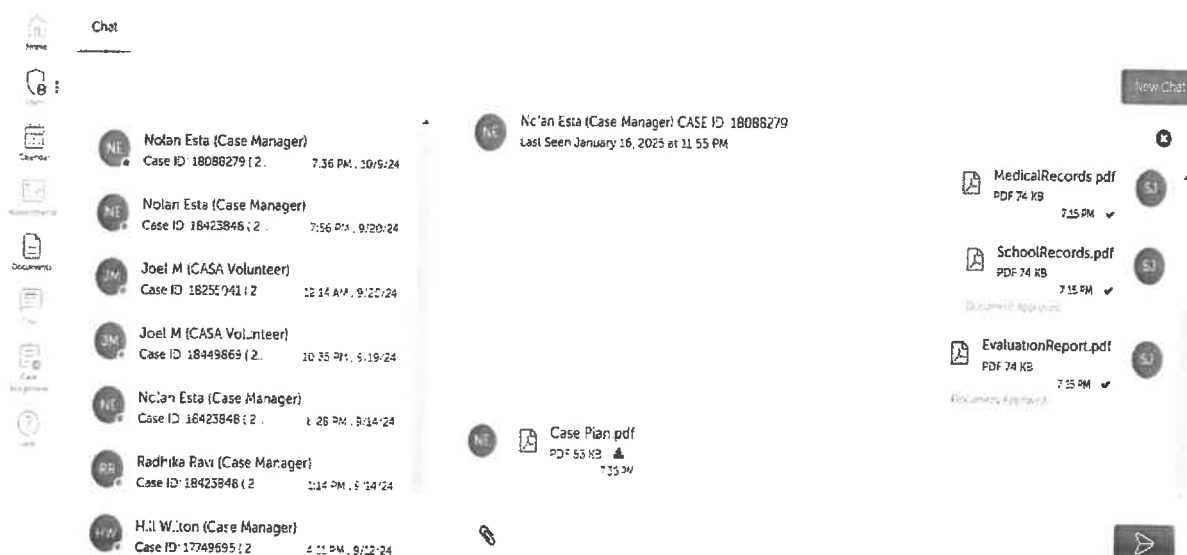
**3.1 Authorized users to use the Solution to access information and documents and communicate through a secure connection. The intent of the portal is to allow authorized users of a foster child's case to see court documents, case plans, and other case related documents; and electronically sign forms (e.g., release forms) (RFP section 4.2.1.1.1)**

Cardinality's WV-MACS solution provides a secure, role-based web portal that is optimized for mobile browsers, allowing authorized users to access case-specific information and documents. This solution is designed to interact with the PATH CCWIS system via secure APIs—preferably using WS02—to fetch the necessary child information in real time.

#### Key features include:

##### Secure Access and Document Viewing:

Authorized users—including caseworkers, foster parents, biological parents, service providers, and legal partners—can log in through a protected connection to view approved court documents, case plans, and other critical records. An advanced Electronic Document Management System (EDMS) organizes these documents by tagging them with relevant metadata (e.g., case ID, document type, timestamps) for efficient retrieval as shown in **Figure 6**.



**Figure 6: Communication module for real time collaboration**

#### Robust Communication Module:

The platform includes a communication module that supports real-time collaboration among stakeholders. This module not only facilitates secure messaging and data sharing but also provides detailed contact information for responsible parties, ensuring coordinated decision-making across the child welfare process as shown in **Figure 7**.

View Person Involved




Andrew Smith Case ID: 17749695

Back

[Child Overview](#) [Evaluations](#) [Assessments](#) [Reports](#) [Forms](#) [Staff Contact Information](#) [Document](#) [Appointments](#) [Chat](#)

Staff Contact Information



Job Description	Staff Name	Action
Social Services Supervisor	James Cray	
County Director	Drake Malfroy	
Social Services Specialist	Jane Sood	

10

1 of 1 items

1 of 1

**Figure 7: Contact information associated with the communication module**

### Electronic Form Management and Digital Signatures:

A configurable form builder is integrated into the solution, allowing users to create, manage, and electronically sign forms (e.g., release forms). Secure electronic signature frameworks and APIs are employed to simplify workflows and reduce paperwork while complying with regulatory standards.

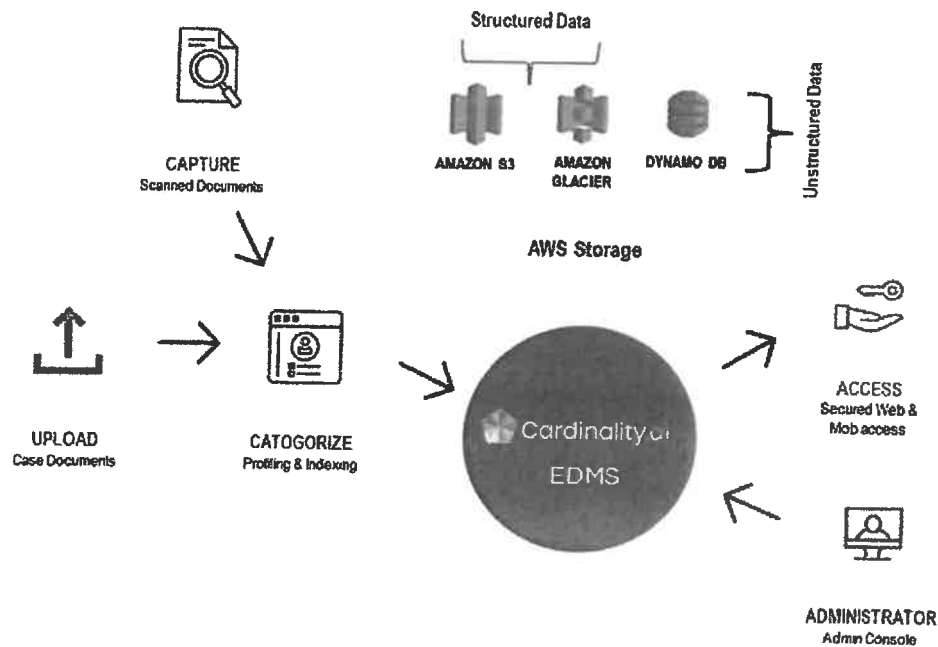
### Integration with PATH CCWIS:

The solution establishes a secure connection with the PATH CCWIS system using robust, API-based integration—preferably through WS02—allowing the portal to fetch up-to-date child information as required. This integration minimizes redundant data entry and streamlines the process for accessing critical case details.

Cardinality's WV-MACS solution delivers a user-friendly, secure web portal accessible via mobile browsers, with strong integration capabilities with the PATH system. This approach effectively supports the safe access, management, and sharing of foster care case information while enhancing collaboration among all stakeholders.

**3.2 Authorized users to utilize the Solution to upload and download information. The intent is for the portal to allow collaboration and access to case records, appointments, and communication. ((RFP section 4.2.1.1.2))**

The WV-MACS solution provides comprehensive capabilities for authorized users to upload, download, and manage case-specific information securely. At its core is an embedded **Enterprise Document Management System (EDMS)**, which allows tagging and packaging all related documentation for both current and future use. The EDMS includes archival, retrieval, and expunging capabilities and can integrate effortlessly with any Document Management System (DMS) chosen by the agency, either immediately or in the future. Utilizing AI-based document classification powered by Natural Language Processing (NLP) and Machine Learning (ML), the system automates the categorization of documents, reading both structured and unstructured data to assign accurate tags. This intelligent classification process addresses challenges such as scalability and manual errors, streamlining the document management process in case management applications. The EDMS lifecycle is depicted in **Figure 8**.

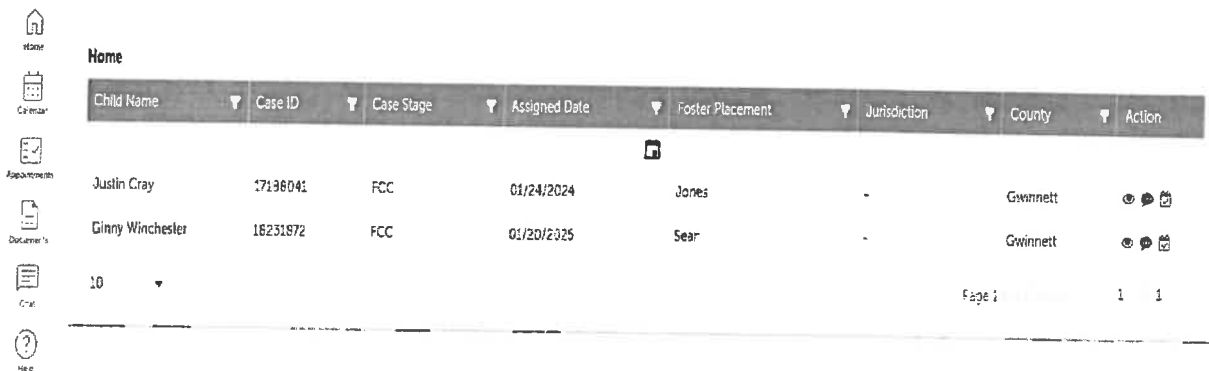








**Figure 8: EDMS entire life cycle**

The system supports document uploads in a variety of formats, including PDF, TIF, JPG, PNG, WAV, WMA, AAC, WMV, M4V, and Microsoft Office formats. Each uploaded document is enriched with customizable metadata fields such as title, category, sub-category, description, document type, author, and timestamp, facilitating efficient organization and searchability. The modular document upload component can be smoothly integrated with any business function or module, providing flexibility across the solution. Metadata provides additional context, enabling users to locate documents using keywords, chronology, or topic-based searches. The EDMS also supports secure digital storage, indexing documents by unique identifiers, creation time, author, and document thumbprints, facilitating traceability and accessibility.

In addition to document management, the case management module enhances collaboration by enabling authorized users to access case records and related documentation efficiently. The case management module will provide secure and efficient access to case records and related documentation, enabling the child welfare stakeholders to view, update, and share information as needed. This capability streamlines workflows and promotes smooth communication, enabling users to collaborate on case-related activities in real-time. By centralizing case records and integrating them with the existing CCWIS/PATH system, the module minimizes delays, reduces redundancies, and supports informed decision-making, ultimately enhancing the overall efficiency and effectiveness of case management in child welfare processes. **Figure 9** depicts the "Upload Screen" where case workers can upload the documents and **Figure 10** depicts how the cases are assigned to a case worker.

**Figure 9: List of uploaded documents**




Child Name	Case ID	Case Stage	Assigned Date	Foster Placement	Jurisdiction	County	Action
Justin Gray	17198041	FCC	01/24/2024	Jones	-	Gwinnett	  
Ginny Winchester	18231872	FCC	01/20/2025	Sear	-	Gwinnett	  

Page 1 of 1

**Figure 10: Assigned cases**

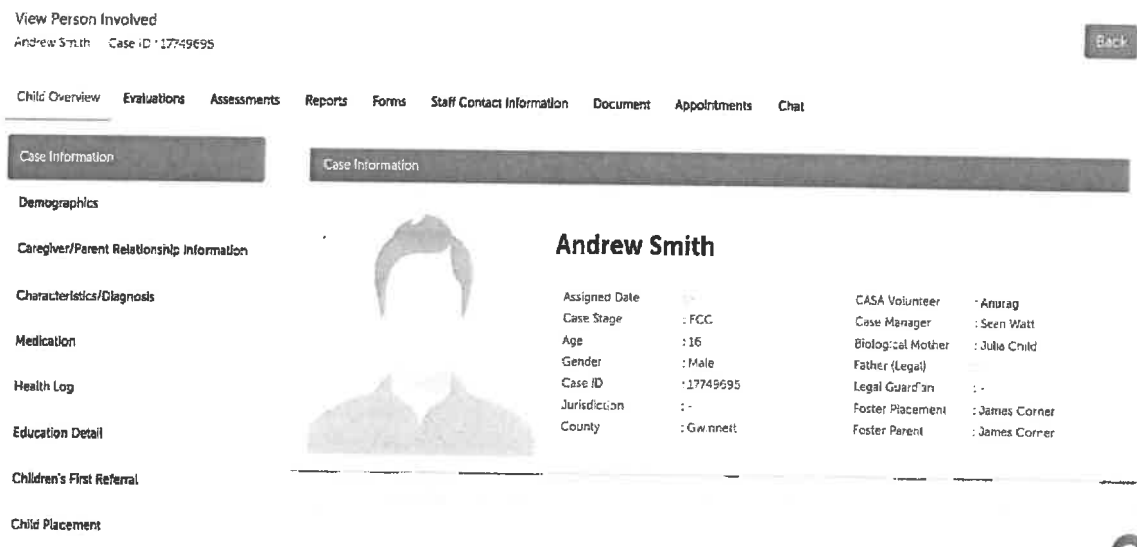
The case management module of our solution includes a powerful Case Search feature designed to streamline the process of finding specific cases. Users can input search criteria such as case ID, client name, or other relevant parameters to quickly locate the desired case. The search results are displayed in a clear and organized format, enabling users to efficiently identify and access the relevant case records as shown in **Figure 11**. This functionality will save time, enhance productivity, and make sure that only authorized users can retrieve the necessary information promptly to support case-related activities and decision-making.



First Name	Last Name	DOB	Child's Legal County	Jurisdiction	Assign/Unassign
Martha	Jones	11/05/2004	Gwinnett		Assign To
Salomon	Cruise	08/18/2014	Gwinnett		Assign To
Amari	Winchester	01/27/2004	Gwinnett		Assign To
Andre	James	11/21/2008	Gwinnett		Assign To

**Figure 11: Case search feature**

This enables caseworkers, foster parents, biological parents, multidisciplinary team (MDT) members, and other users to have a unified view of critical case details as shown in **Figure 12**. The scheduling module facilitates the management of appointments, such as court hearings, visitations, and team meetings, providing a centralized calendar for better coordination. Furthermore, the communication module allows secure, real-time collaboration between case participants, supporting smooth interaction.



View Person Involved  
Andrew Smith Case ID : 17749695

Child Overview Evaluations Assessments Reports Forms Staff Contact Information Document Appointments Chat

Case Information

Demographics

Caregiver/Parent Relationship Information

Characteristics/Diagnosis

Medication

Health Log

Education Detail

Children's First Referral

Child Placement

**Andrew Smith**

Assigned Date		CASA Volunteer	Amrags
Case Stage	: FCC	Case Manager	: Seen Watt
Age	: 16	Biological Mother	: Julia Child
Gender	: Male	Father (Legal)	
Case ID	: 17749695	Legal Guardian	: -
Jurisdiction	: -	Foster Placement	: James Corner
County	: Gwinnett	Foster Parent	: James Corner

**Figure 12: Case details screen**

**3.3 The Solution should help prevent user error with document uploading to any case. For example, a user uploads the wrong psychiatric evaluation to a case, and the Solution asks the user to confirm the correct file and/or case before completing the transaction. (RFP section 4.2.1.1.3)**

The WV-MACS solution will incorporate an Enterprise Document Management System (EDMS) and Cardy AI, which uses Natural Language Processing and Machine Learning to minimize errors during document uploads. The EDMS will be able to validate documents by checking metadata such as case ID, document type, and timestamps to enable them to be correctly linked to the appropriate case. With Cardy AI, the solution will be able to further analyze document content in real-time, classify and verify it to identify any mismatches. For example, if a psychiatric evaluation is uploaded to the wrong case, the system reviews the content and metadata, flags the issue, and prompts the user to confirm or correct the upload before proceeding.

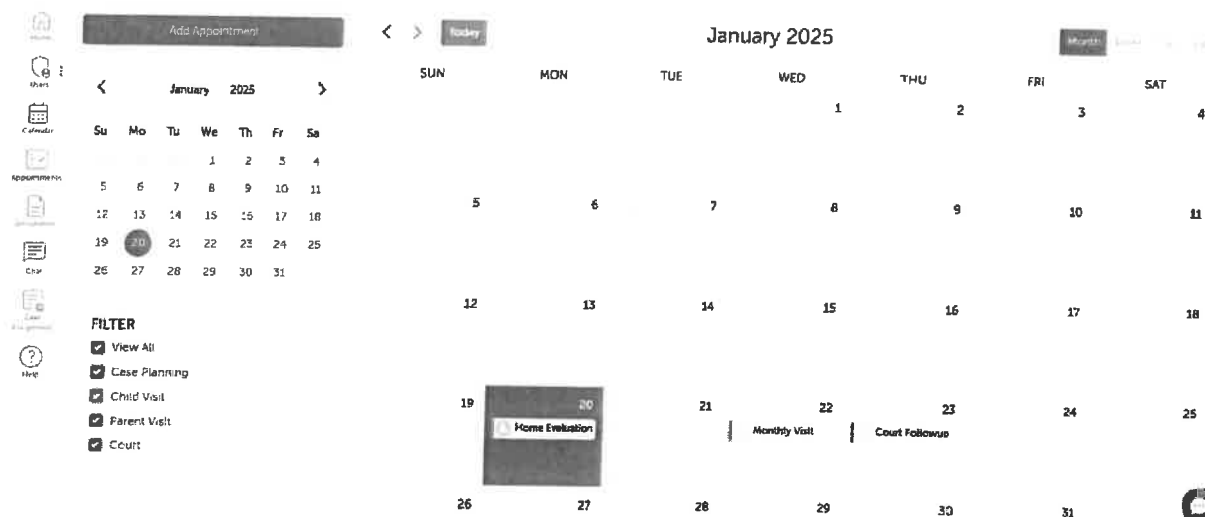
The solution also uses a workflow and business rules engine powered by Drools to apply validation rules and conduct automated checks throughout the upload process. The user interface includes tooltips to provide contextual guidance and prompts to help users verify their file selection and its association with the intended case. If the system detects an issue, it sends alerts via our notifications and alerts module, providing clear instructions for resolving that problem. Access to upload functionality is controlled by Role-Based Access Control (RBAC), which enables only authorized users to perform these actions, further reducing the likelihood of errors.

In the example scenario, if a psychiatric evaluation is uploaded to the wrong case, Cardy AI's real-time content checks and metadata validations will be able to detect the error and flag it immediately. The user will be prompted to confirm the upload and correct any discrepancies. If the issue remains unresolved, a notification can be sent to enable it to be addressed. This process helps maintain accurate record-keeping, prevents user errors, and supports the integrity of case management operations.

**3.4 Authorized users to utilize calendar functionality that allows users to schedule visitation sessions for children and parents, SNS appointments, meetings with GALs, court dates, and MDT meetings. (RFP section 4.2.1.1.4)**

Cardinality's WV-MACS solution includes a highly configurable scheduling module that supports the scheduling of critical events such as visitation sessions for children and parents, Socially Necessary Services (SNS) appointments, meetings with Guardians ad Litem (GALs), court dates, and Multidisciplinary Team (MDT) meetings. By leveraging an integrated calendar system, our solution enables smooth scheduling, documentation, and tracking of action items within the case plan.

The solution features a shared calendar for collaborative scheduling, which enhances communication and coordination between foster parents, DHS staff, and other stakeholders. The Calendar View displays all appointments, allowing users to view events by day, week, or month for clarity and accessibility. Additionally, the module integrates with external systems such as Microsoft Office 365 Outlook, enabling automatic synchronization of court dates and other key events into users' calendars. This facilitates real-time updates, efficient time management, and reduced manual errors. Stakeholders can propose, view, and confirm hearing dates directly within the system, streamlining the scheduling process for appeals and court sessions, which is critical for improving the efficiency and timeliness of foster care operations in West Virginia.



**Figure 13: Calendar screen**

The user-centric design of the scheduling module as shown in **Figure 13** allows for intuitive interaction, with continuous user interfaces enabling all scheduling-related functions to be performed without losing the context of the workflow. This design supports creating, assigning, and tracking tasks linked to scheduled events, fostering a collaborative and progressive approach to case management. By automating scheduling processes and supporting group decision-making through templates and indicators, the solution enables every stakeholder to remain informed and engaged. The integration of robust tools for task scheduling, workload balancing, resource allocation, and performance monitoring further empowers the DHS to enhance agency efficiency and enable optimal resource utilization. With its ability to synchronize across platforms, document actions, and maintain shared calendars, the WV-MACS solution delivers a comprehensive, user-friendly scheduling solution tailored to the needs of West Virginia's child welfare system.

**3.5 All authorized users are able to make non-medical related requests, including but not limited to vacation requests or haircut requests. (RFP section 4.2.1.1.5)**

Cardinality's WV-MACS solution enables authorized users to make non-medical requests, such as vacation or haircut requests, through its integrated Case Management Module. For instance, a foster parent can log a non-medical request via the portal, which is automatically tagged as a non-medical request and assigned as a task in the Task Management Module. Notifications will be sent to the caseworker for review and approval through the Notification and Alerts Module. Upon approval, the Scheduling Module helps plan the appointment, while the Provider Management Module coordinates with Socially Necessary Services (SNS) providers for required resources.

The solution leverages advanced technology for smooth processing. The solution's UI enables foster parents to submit requests through an interactive portal. Our solution will be using AWS Lambda to process the submission, categorize it as a non-medical request, and trigger the next steps. The Drools Rules Engine applies predefined approval workflows, determining whether caseworker or administrative review is required. Notifications are managed through our Notifications and Alerts module, enabling all





relevant parties to be informed of request statuses. Request details, including metadata, are securely stored in Amazon RDS, while any uploaded supporting documents are stored in Amazon S3 for easy access and compliance. This integrated approach facilitates efficient handling of non-medical requests, improving coordination and user experience.

**3.6 The Agency to utilize Solution-generated reports to understand the responsiveness of team members to questions or requests and the average time it takes for authorized Agency users to update the information. (RFP section 4.2.1.1.6)**

Cardinality's WV-MACS solution includes a robust Reporting Module (**MicroStrategy**) designed to provide actionable insights into the responsiveness of team members to questions or requests and the average time it takes for authorized users to update information. Standard reports, including key performance indicators (KPIs), can be generated to assess team performance and operational efficiency, leveraging our OEM partnership with MicroStrategy and the capability of the solution to integrate smoothly with advanced business intelligence tools such as Power BI, Tableau. This flexible reporting capability enables the generation of both pre-built and adhoc reports to meet diverse business needs, with advanced charting and visualization tools that are intuitive and require minimal training.

The Reporting Module supports pre-built reports aligned with current West Virginia DHS report outputs, providing users with readily available templates that can be exported into multiple formats, including Microsoft Excel and Adobe PDF. Team members' actions, such as responses to questions or requests, will be captured through the Case Management Module or Task Management Module, with timestamps recorded for every action. Notifications and acknowledgments are tracked via the Notification and Alerts Module, and AWS Lambda will be used to process this data to calculate KPIs like response times and update frequencies. This processed data is stored securely in Amazon RDS and visualized using tools like MicroStrategy for insightful analytics.

Reports can be accessed through the portals, offering interactive filters and configurable views, enabling users to drill down into specific details. The solution's flexibility enables the agency to generate comprehensive reports tailored to operational needs, combining pre-built/standard reports with adhoc configuration to enhance decision-making and streamline team responsiveness. These capabilities empower the agency to monitor performance effectively, improve service delivery, and align with the state's child welfare operational goals.

## 4. Project Phases

**4.1 Project Phases:** The Agency's objective is to implement the Solution in phases. Table 2 below outlines high-level project phases, the major efforts and deliverables involved during those phases, and the outcomes the Agency anticipates that the Vendor will achieve during these phases. ((RFP section 4.2.1.2)

**4.2 Project Deliverables:** The Agency anticipates that the Vendor will supply the deliverables listed in Table 2 below. Vendors should provide a narrative describing their approach to the major efforts and deliverables in their technical proposal. As part of the response, Vendors should include a draft Implementation Plan, including a project timeline that aligns with the Vendor information submitted in the Appendix C: Cost Proposal Form, Project Deliverables worksheet.

Vendors should also include a copy of their project management plan outline, including at a minimum, sections for Scope, Quality, Resource, and Risk and Issue Management that will be finalized during project planning. (RFP section 4.2.1.3)

### Implementation Approach

Cardinality's **work plan** for the implementation of the **WV-MACS** will ensure that both **Phase 1 (Messaging and Other Communication Capability)** and **Phase 2 (Visitation Appointments, Travel and other services, Court hearings, meetings with GALs, MDT meetings, File Upload, Calendaring, Reporting)** are completed within the designated contract periods. This work plan will include a detailed timeline that displays each major activity, task, and corresponding deadlines. Cardinality will assign clear responsibilities for each task and highlight any work delegated to subcontractors. ***Cardinality is pleased to submit a sample Project Management plan as a separate attachment for the agency's review.***

#### 1. Work Plan Overview

The work plan is divided into two major phases:

- **Phase 1:** Development and Go-Live of Messaging and Other Communication Capability
- **Phase 2:** Development and Go-Live of the Visitation Appointments, Travel and other services, Court hearings, meetings with GALs, MDT meetings, File Upload, Calendaring, Reporting

#### **Phase 1: Development and Go-Live of Messaging and Other Communication Capability (Months 1-5)**

Phase 1 will focus on the development, testing, and deployment of **Messaging and Other Communication Capability**. The work plan follows a clear sequence of discovery, design, development, testing, training, and Go-Live activities, ensuring that the portal is functional by the **5<sup>th</sup> month**. Post-Go-Live, the post implementation support will begin as per contract terms.

**Phase 2: Development and Go-Live of the Visitation Appointments, Travel and other services, Court hearings, meetings with GALs, MDT meetings, File Upload, Calendaring, Reporting (Months 6-9)**

**Phase 2** will commence immediately after **Phase 1 Go-Live** and will be developed and rolled out over **9 months**. During this time, the same rigorous steps of discovery, development, testing, and training will be followed.

**2. Work Plan Timeline and Activities**

**Exhibit 1** gives a detailed breakdown of the major activities, their timelines, and the positions responsible for executing each task:

Task	Timeline	Responsible Position	Details
<b>Discovery and Planning</b>	Month 1	Project Manager, Business Analyst	Gather and analyze requirements, create detailed project roadmap.
<b>Design</b>	Month 1	Technical Architect, UX/UI Designers	Develop architectural designs, wireframes, and user experience guidelines.
<b>Development &amp; System Integration</b>	Month 2 - 3	Development Lead, Developers, Integration Lead, DB Lead	Develop the Messaging & communication features, database, and integrations. Integrate with PATH CCWIS system, databases and other systems.
<b>Testing</b>	Month 2 - 4	Testing Lead, Testers	Conduct functional, security, and user acceptance testing.
<b>Training Development</b>	Month 3-5	Training Lead, Training Material Developer, Trainer	Develop training materials for end users and administrators. Conduct training for WV administrators on the new portal.

<b>Phase 1 Rollout/Go-Live</b>	End of Month 5	Project Manager, Technical Team	Go-Live for the Messaging & communication module, followed by Post implementation support.
<b>Maintenance &amp; Operations</b>	Month 6 onwards	Support Engineers, Help Desk	Ongoing system maintenance, monitoring, and user support post-Go-Live.

**Exhibit 1: Phase 1 Development timeline****3. Phase 2: Public Portal Timeline**

After the Go-Live of **Phase 1**, **Phase 2** development will begin and will take **4 months**, from Month 6 to 9. **Exhibit 2** gives a detailed breakdown of activities:

Task	Timeline	Responsible Position	Details
<b>Discovery and Planning &amp; Design</b>	Month 6	Project Manager, Business Analyst, Technical Architect, UX/UI designers	Requirements gathering and planning for Phase 2. Technical design and UX for the public portal
<b>Development</b>	Month 6 - 7	Development Lead, Developers	Build the remaining features of the Mobile Application Communication Software
<b>Testing</b>	Month 6 - 8	Testing Lead, Testers	Perform functional, security, and UAT testing on the Public Portal.
<b>Training Development</b>	Month 7 – 9	Training Lead, Training Material Developer	Develop training materials for the Public Portal users.
<b>Phase 2 Rollout/Go-Live</b>	End of Month 9	Project Manager, Technical Team	Go-Live for the Public Portal, followed by ongoing M&O support.

**Exhibit 2: Phase 2 Development timeline**

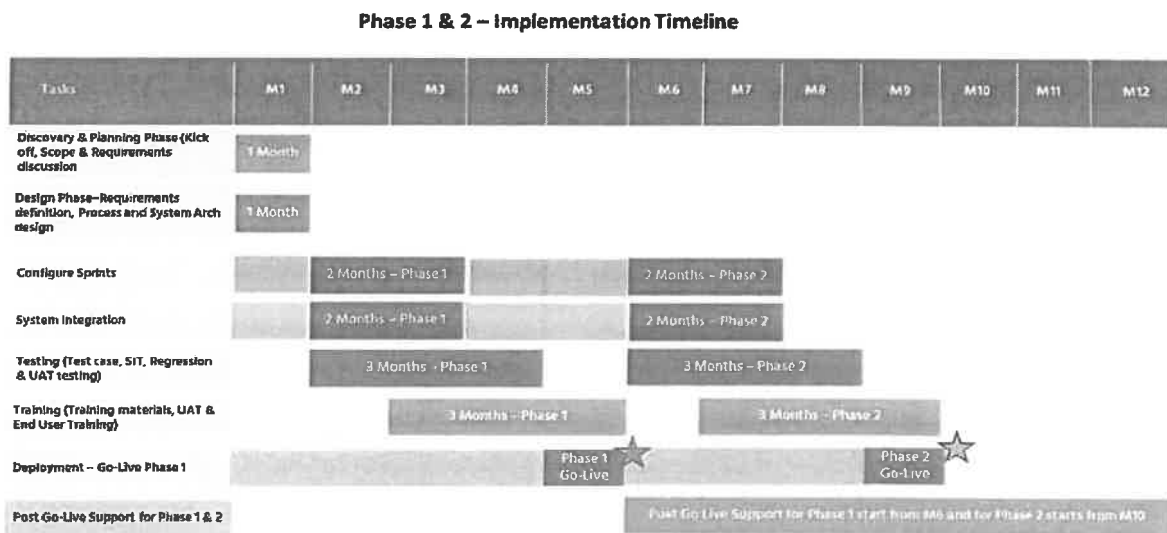
#### 4. Responsibilities and Task Delegation

**Cardinality's team** will handle most of the project execution. The **Project Manager** will oversee all phases and ensure that tasks are delivered on time, while **Business Analysts, Developers, and Testers** will play key roles in executing their respective tasks.

For **System Integration, Testing and Post-Implementation support** Cardinality's partner, **Cyquent, Inc.**, will oversee and manage these tasks in coordination with Cardinality's Project Manager to confirm successful completion.

#### Proposed Project Schedule:

Please find below **Figure 14** the project implementation timelines of both phase 1 and phase 2 which provide a clear, visual representation of the project flow, ensuring that stakeholders have visibility in the entire implementation process.

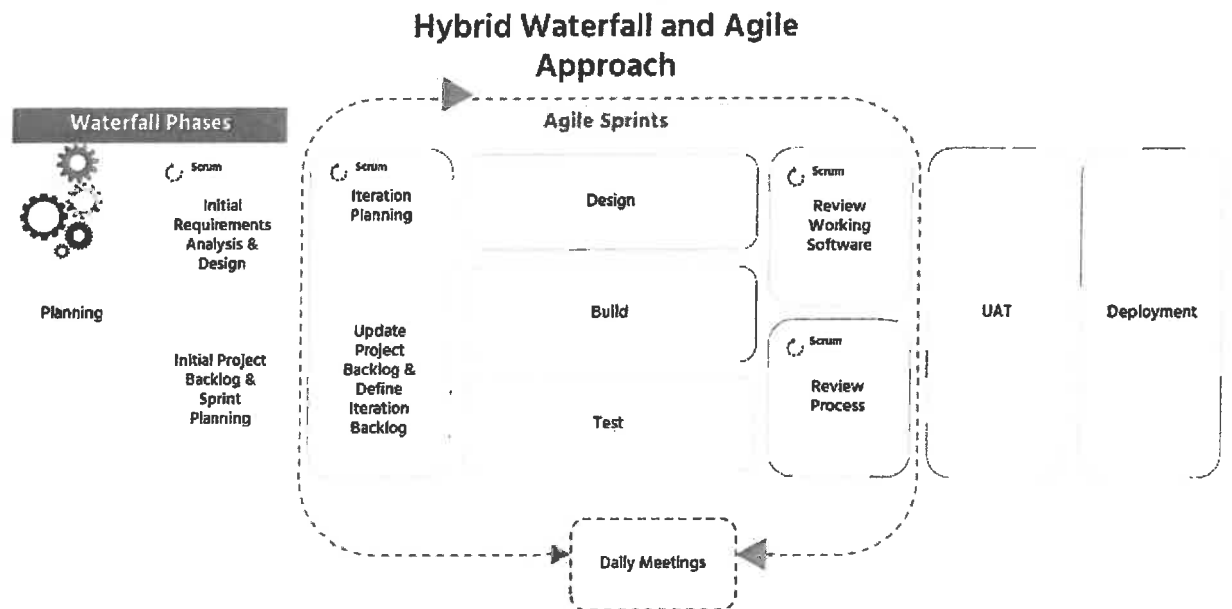


**Figure 14: Implementation Timeline**

#### Project Management Approach

Cardinality employs a robust Hybrid Agile project methodology that integrates Joint Application Development (JAD) sessions as a central component of the requirements gathering and validation process. These sessions allow us to capture detailed functional requirements directly from the users, ensuring that all perspectives and needs are considered from the outset. **Figure 15** illustrates the Hybrid-Agile approach:

## Implementation Approach - Hybrid Agile



**Figure 15: Hybrid Agile Implementation Methodology**

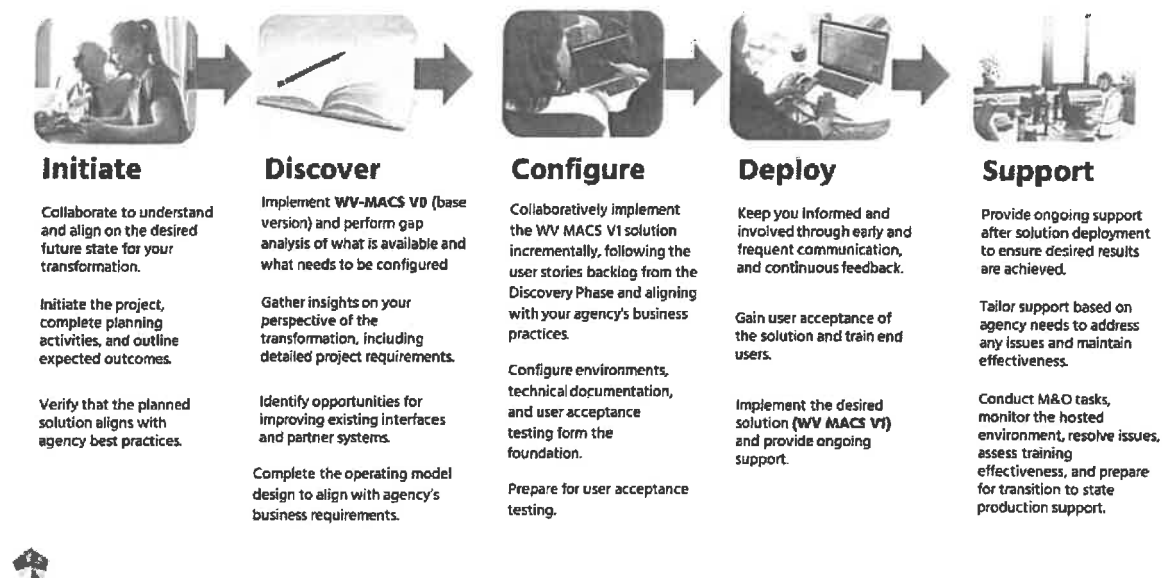
For the **WV-MACS** implementation, by day 30, we will deploy version 0 (**EF-CW V2025.4.1 v0**) of the solution, which serves as the baseline for conducting discovery sessions and then incrementally enhance using our gap-based implementation model. This v0 is pre-built based on the requirements outlined in the RFP documents.

During sprint 1, we update this v0 addressing gaps and deploy v0.1, with incremental progress towards version 1 (v1), the planned go-live version. We follow this process for each sprint, resulting in intermediate versions of the solution, such as v0.2, v0.3, and so on. Throughout the DDI phase, we maintain a continuous feedback loop, ensuring that any discrepancies or changes in requirements are addressed promptly.

Cardinality emphasizes rigorous documentation of all functional requirements, ensuring that they are traceable throughout the project lifecycle. This traceability ensures that each requirement is accounted for and fully implemented by the end of the DDI phase.

For the implementation of WV-MACS, Cardinality deploys the above hybrid-agile methodology comprising of 5 phases as given below (**Figure 16**):

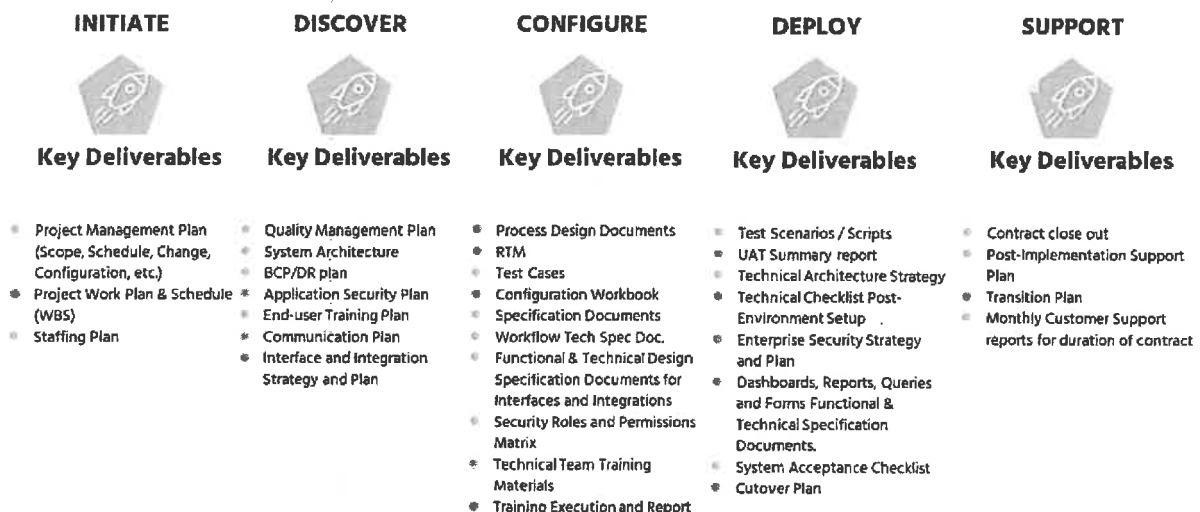
## Project Phases



**Figure 16: Cardinality's Project Management Phases**

The following list of deliverables (Figure 17) will be submitted with the agency against each phase of the project:

## Key Project Deliverables



**Figure 17: Project deliverables**

## 5. Functional and Technical Requirements

**Functional and Technical Requirements:** The Vendor should submit a completed Appendix B: Functional and Technical Requirements that indicates Vendor's level of fit for each requirement. (RFP section 4.2.1.4)

Team Cardinality has thoroughly reviewed the requirements outlined in **Appendix B** and has filled in our responses for each of the requirements and attached it separately. Additionally, we are pleased to highlight some of the key features of our solution along with sample screen shots demonstrating our successful implementation of this exact solution in Georgia DHS (Communicare Project).

### 5.1 Functional Requirements:

1. **Communication module will be used for messaging functionality:** Cardinality's WV-MACS solution features secure messaging capabilities that enable authorized users to communicate and exchange messages within the system as shown in **Figure 18**. The messaging functionality includes a comprehensive message history feature, allowing users to access and review past communications while enabling data privacy and security through role-based access controls and encryption protocols. This messaging will support all stakeholders involved in a foster child's case, including case workers, foster parents, biological parents or guardians, Child Placing Agencies (CPAs), Socially Necessary Services (SNS) providers, Multidisciplinary Team (MDT) members, and other legal community representatives (GALs and Probationary officers). This capability will promote efficient collaboration and streamlined workflows among authorized personnel, enhancing overall system effectiveness. Leveraging the communication module, it supports real-time messaging via email, SMS, or in-app notifications, facilitating timely and reliable updates.



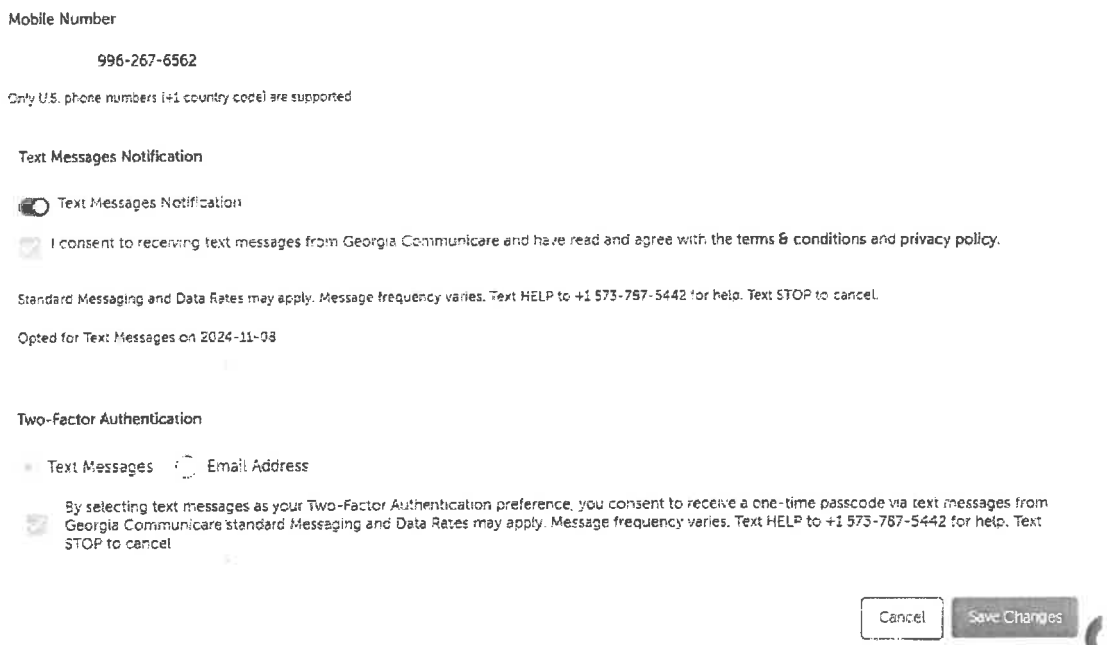
**Figure 18: Messaging functionality**

The solution incorporates a dedicated communication module that supports real-time collaboration among stakeholders, such as caseworkers and foster parents, facilitating coordinated decision-making in the child welfare process. This functionality is included in the current WV-MACS solution release and will be implemented by the planned phase go-live date, aligned with the State's agreed-upon configuration planning. The communication module enables effective communication across roles, with



the ability to securely send messages and view message history, fostering better coordination and outcomes in child welfare services. This module will improve communication and collaboration among all the interested parties involved in the welfare of children to help enhance the state's foster care system.

- 2. Alerts and Notifications module:** Cardinality's WV-MACS solution incorporates a robust notification and alert module that enables authorized users to be informed of new information, task deadlines, and critical actions requiring attention. The system dynamically generates alerts for key events, such as changes to a child's case, including updates to placement location. Notifications are both event-based (triggered by specific actions or changes in the system) and time-based (triggered by approaching deadlines), enabling comprehensive and timely user engagement to support effective case management. This feature is included in the current software release and will be implemented by the planned phase go-live date in accordance with agreed-upon configuration planning with the State as illustrated in **Figure 19**. This functionality enables authorized users to remain responsive to time-sensitive tasks and case developments, enhancing collaboration and operational efficiency.



**Figure 19: Alerts and Notifications module**

- 3. Communication Archiving:** Our solution smoothly supports communication archiving into the CCWIS/PATH system by capturing and securely storing text, email, and chat records in compatible formats such as json, xml, csv, database formats, or as log files. The proposed solution will integrate smoothly with the existing CCWIS/PATH system using WSO2 Enterprise integrator, leveraging standard interfaces such as RESTful or batch APIs, SFTP, SOAP, and web-based services. This approach maintains a comprehensive and accessible archive of communications, supporting compliance, reference, and reporting while promoting effective case documentation and



efficient system operations. The archived data remains secure, retrievable by authorized users, and aligned with federal, state, and agency-specific retention policies.

Communication records are securely processed using AWS Lambda and stored in AWS S3 or RDS for PostgreSQL, facilitating tamper-proof data retention. AWS WAF and CloudFront protect data during transmission and retrieval, while AWS CloudTrail logs all archival actions, maintaining compliance and traceability. Elastic Kubernetes Service (EKS) further enhances scalability, managing communication workflows efficiently and facilitating smooth operation under variable workloads.

By creating a centralized repository within the PATH system, our solution will have the capability to link communication records to relevant case files, facilitating complete traceability and accountability. Real-time access to archived communication supports informed decision-making and compliance with reporting requirements, ultimately improving case management in child welfare processes.

4. **WV-MACS: Secure Messaging Across Multiple Platforms:** The communication module allows authorized users to securely send and receive messages, access a comprehensive message history (archiving functionality) within the PATH system, and receive real-time updates through email, SMS, chat, text, or in-app notifications. This enables timely and reliable communication, enhancing decision-making and workflows in child welfare processes. By improving communication among all parties, the module strengthens the foster care system and promotes better outcomes for children.

The workflow for secure messaging begins with users initiating a message through the Angular-based UI interface, which sends data securely to the Node.js back-end for processing. AWS Lambda will be used for encrypting messages, formats them for delivery (JSON for chat, plain text for SMS), and triggers event-based notifications for tasks or updates. Messages are delivered through appropriate channels—email via AWS Simple E-mail Services (SES), chat through APIs, and SMS via AWS Simple Notification Services (SNS)—enabling reliable and timely communication.

To maintain data integrity, message metadata is stored in Amazon RDS for PostgreSQL for structured querying and retrieval, while attachments or logs are securely stored in Amazon S3. Notifications will be facilitated by AWS CloudFront, facilitating efficient delivery with low latency. AWS CloudWatch will be used to monitor system performance, and AWS CloudTrail logs all activities for auditing and compliance purposes.

This secure and scalable messaging capability is included in the current WV-MACS solution release and will be implemented by the planned phase go-live date, in alignment with the State's agreed-upon configuration planning. By enabling real-time collaboration and secure communication, the WV-MACS solution enhances coordination among stakeholders and enables the welfare of children to remain a top priority.

5. **File-Sharing Capability within Messaging Functionality:** The WV-MACS solution integrates a robust file-sharing feature within its messaging functionality, allowing authorized users to securely upload, share, and manage documents and files. This capability facilitates smooth collaboration and efficient information exchange among stakeholders, protecting data integrity and confidentiality through strict access controls. By embedding this feature into the messaging

platform, the WV-MACS solution supports real-time, secure communication, enhancing operational efficiency, and improving Child Welfare case management outcomes.

At the heart of this functionality lies the Communication module and Enterprise Document Management System (EDMS), which enable secure sharing, tagging, packaging, and management of case-specific documents for both immediate and future use. The EDMS provides advanced document handling capabilities, including archival, retrieval, and expungement. Enhanced by AI-based document classification using Natural Language Processing (NLP) and Machine Learning (ML), the system automates the categorization of structured and unstructured data. This intelligent classification reduces manual errors, improves scalability, and streamlines the overall document management and sharing process, facilitating accurate tagging and quick retrieval of critical information.

File metadata, such as file name, sender, recipient(s), timestamp, and case information, is simultaneously stored in Amazon RDS for PostgreSQL, linking the file to its corresponding messaging thread for efficient retrieval and organization. Recipients can be notified through the messaging platform via email, chat, or SMS, enabling them to securely access and download the file through the UI interface. APIs will be used to validate recipient access rights, maintaining adherence to role-based security protocols.

The WV-MACS solution leverages AWS CloudTrail to log all file-sharing and document upload activities, creating a comprehensive audit trail that captures detailed information about uploads, downloads, and permission checks. AWS CloudWatch will continuously monitor the system's performance, tracking metrics like upload speed and storage utilization to maintain reliable operation. Alerts are generated for administrators in the event of potential issues, maintaining smooth system performance.

The solution's technology stack enables a secure, scalable, and user-friendly file-sharing and document management system. Amazon S3 safeguards uploaded files with encryption and access controls, while Node.js facilitates smooth communication between front-end and back-end systems. AWS Lambda enhances compliance through encryption and validation, and Elastic Kubernetes Service (EKS) supports scalability to handle growing volumes of files without performance degradation. The Angular UI interface provides an intuitive user experience, allowing stakeholders to interact with the system efficiently while maintaining compliance with regulatory standards.

- 6. Bidirectional Integration with CCWIS:** Cardinality's WV-MACS solution is designed to interface bidirectionally with the CCWIS/PATH system, enabling smooth push and pull of information to maintain data consistency and support operational efficiency. The CCWIS serves as the single source of truth for all foster case information and documentation. The solution captures, synchronizes, and archives data in alignment with this structure, enabling accurate data exchange and comprehensive case management within the CCWIS framework.

Leveraging advanced integration technologies such as the WSO2 API Integrator, the solution facilitates secure connectivity through RESTful APIs, Batch APIs, SOAP services, and SFTP protocols. This enables real-time data updates for critical activities such as placement changes and case updates, while asynchronous methods (e.g., scheduled batch processing) optimize performance for non-urgent tasks. The solution enables both systems to remain updated and consistent, allowing all stakeholders to access accurate and up-to-date information.

The WV-MACS solution uses an advanced technology stack to fulfill the bidirectional integration requirement. Node.js serves as the back-end middleware, managing WSO2 API calls and enabling data exchanged with CCWIS to adhere to required formats such as JSON or XML. AWS Lambda processes data dynamically, enabling real-time updates and event-driven synchronization for both push and pull operations. For large-scale or archival data exchanges, Amazon S3 handles secure storage and bulk file management, while Amazon RDS for PostgreSQL provides transitional storage for metadata or intermediary data during synchronization. The integration framework will be secured with AWS WAF, protecting endpoints from unauthorized access and malicious activities, while AWS CloudTrail provides a detailed audit trail for all data exchange activities, supporting compliance and accountability.

This approach enables the CCWIS/PATH system to remain the authoritative repository for all foster care data, with the WV-MACS solution acting as a robust interface to enhance communication functionality and user experience. By synchronizing with CCWIS, the solution centralizes the archiving of foster care records, promotes operational efficiency, and maintains data integrity and compliance with child welfare regulations.

7. **Role-Based Access Control (RBAC) module:** Cardinality's solution incorporates an advanced Role-Based Access Control (RBAC) module as shown in **Figure 20** to securely manage access to sensitive case record information stored in the existing CCWIS.



Page Name	Create	Read	Update	Delete	Download	None	Data Access	Custom Actions
Complaints List	<input checked="" type="checkbox"/>						All	
Incident Violation Ticketing List	<input checked="" type="checkbox"/>						All	
Incident Violation Ticketing page	<input checked="" type="checkbox"/>							

**Figure 20: RBAC access section**

This functionality enables only authorized users to access specific records, such as education, medical, dental, mental health, psychological evaluations, and visitation records, based on their predefined roles and responsibilities. By implementing RBAC, the solution safeguards sensitive

information, maintains compliance with data privacy regulations, and supports efficient and secure case management.

The RBAC module framework dynamically assigns permissions based on user roles, enabling granular access control for various categories of case information. Permissions are configurable, accommodating changes in organizational roles or temporary assignments, facilitating operational flexibility without compromising security.

To protect sensitive data, the RBAC module enforces strict security measures, including encryption during data transmission and secure authentication protocols, such as multi-factor authentication (MFA). Comprehensive audit logs, powered by AWS CloudTrail, capture all RBAC-related actions, including access attempts and role assignments, promoting transparency and accountability. These logs maintain compliance with regulatory standards like HIPAA and FERPA while providing a clear audit trail for oversight and reporting.

- 8. Online/Offline Messaging and Video/Audio Conferencing Capability:** Cardinality's WV-MACS solution provides authorized users with the capability to enter messages via SMS, email, or in-app channels, which are immediately uploaded to the CCWIS when online or queued for upload once connectivity is restored. Additionally, the solution supports video and audio conferencing among authorized users, complete with a recording feature for documentation and future reference, enhancing collaboration and communication efficiency. These features facilitate efficient collaboration using its communication module and comprehensive documentation, all integrated with the Comprehensive Child Welfare Information System (CCWIS)/PATH system.

**Online/Offline Messaging:** The WV-MACS solution provides robust online and offline messaging capabilities, enabling authorized users, such as caseworkers, supervisors, and service providers, to securely communicate through SMS, email, or in-app notifications as illustrated in **Figure 21**. The solution will make sure that all case-related communications are securely documented and integrated into the CCWIS for comprehensive case management and compliance.



Date & Time	Priority	Alert Type	Description	Triggered by
01/03/2025, 07:26 PM	high	Attachment	Document Approved by Nolan Esta case# 18423846	Nolan Esta
01/03/2025, 07:18 PM	high	Attachment	Document Approved by Nolan Esta case# 18088275	Nolan Esta
12/20/2024, 01:54 PM	high	Attachment	Document Approved by Nolan Esta case# 18423846	Nolan Esta
12/20/2024, 01:38 PM	high	Attachment	Document Approved by Nolan Esta case# 18088275	Nolan Esta
11/05/2024, 01:02 PM	high	Appointment	Appointment "Child Visit", planned for Thu September 12, 2024 8:00 AM, has been canceled by P.J. Wilton.	P.J. Wilton

**Figure 21: In-app notifications**

For online messaging, messages are immediately uploaded to the CCWIS, leveraging smooth integration with the WSO2 API Integrator using its RESTful API functionality. This enables real-time documentation of case-related communication, keeping all relevant parties informed and maintaining data accuracy in critical child welfare processes, such as case updates and service coordination.

In offline scenarios, users can compose messages that are automatically queued and securely stored. Upon restoration of connectivity, these messages, regardless of the medium (SMS, email, or in-app notifications), are uploaded to the CCWIS/PATH system using batch APIs facilitated by the WSO2 API Integrator. This approach enables no loss of communication records, even in areas with limited or intermittent connectivity, meeting the operational needs of DHS for continuous documentation and communication.

**Video/Audio Conferencing Capability:** The WV-MACS solution will enable authorized users, to conduct secure video and audio conferencing. These capabilities will be tailored to support child welfare processes, including interactive discussions, case planning meetings, stakeholder interviews, and collaborative decision-making. By facilitating real-time communication, the solution will help stakeholders in sharing critical information and is documented efficiently and effectively.

To meet the requirements of West Virginia DHS, all conferencing sessions are encrypted during transmission to protect sensitive information, leveraging AWS WAF to secure endpoints against unauthorized access. System performance, including connection stability and resource utilization, can be continuously monitored through AWS CloudWatch, facilitating a smooth user experience for high-stakes interactions such as multidisciplinary team meetings and family case discussions.

The solution includes a robust recording feature, allowing sessions to be documented for compliance, future reference, or accountability purposes. Recordings are temporarily stored in Amazon S3, enriched with metadata such as participant details, timestamps, and session duration, and subsequently can be uploaded to the CCWIS/PATH system for secure archival. This integration enables all case-related conferencing data to become part of the centralized repository, supporting comprehensive case documentation and audit readiness.

Comprehensive logging of all conferencing activities is managed through AWS CloudTrail, capturing session initiation, duration, and recording uploads. This maintains adherence to regulatory requirements, including HIPAA, while providing a transparent audit trail to address privacy, accountability, and compliance requirements/standards outlined by DHS. The WV-MACS solution will support the operational and regulatory framework of child welfare by enhancing collaboration, data integrity, and secure information sharing.

9. **Capture and Securely Store Media:** Cardinality's WV-MACS solution enables authorized users to capture photos, videos, and audio recordings directly within the system. This functionality supports critical child welfare processes by enabling real-time documentation of case-related activities such as home condition assessments, interviews, and evidence collection for compliance with care plans. These capabilities enable media documentation to be smoothly integrated into the Comprehensive Child Welfare Information System (CCWIS), supporting accurate case management and adherence to regulatory standards.

The solution allows users to utilize device hardware, including smartphones, tablets, or webcams, to capture media. Leveraging the Angular front-end, the solution provides an intuitive interface for media capture and metadata input, such as date, time, location, and case association. Captured media files are securely transmitted via the backend, which validates user permissions and routes the files for storage. Files are encrypted and stored in Amazon S3, a centralized repository, enabling data security at rest and during motion. Metadata, such as timestamps and user associations, is automatically enriched through AWS Lambda, which also processes media files for efficient storage, such as compressing images or generating video thumbnails.

All media-related actions, including file uploads and metadata updates, are logged by AWS CloudTrail, maintaining compliance with privacy regulations such as HIPAA. This audit trail enhances transparency and accountability, meeting the requirements for safeguarding sensitive child welfare data. By integrating secure media capture of our solution with CCWIS, Cardinality's solution empowers child welfare professionals in West Virginia to document and manage critical case-related information effectively. This functionality enhances decision-making, supports compliance, and strengthens the overall child welfare process.

- 10. Documenting Updates for Goals, Tasks, and Steps:** Cardinality's WV-MACS solution enables authorized users to document updates related to the completion of case-specific goals, tasks, and steps. This functionality supports key child welfare processes, such as tracking progress on reunification plans, meeting safety milestones, scheduling meetings, or completing required training modules, maintaining compliance with the requirements of West Virginia DHS.

Using the solution's task management module, users can update task statuses, add comments, and document progress directly through an intuitive user interface. Each update is securely linked to the relevant case record in the CCWIS, enabling accurate tracking and promoting accountability. Users will be able to smoothly input updates and mark tasks as completed, providing a clear overview of case progress.

- 11. Requesting and Viewing Upcoming Meetings:** The solution features a configurable scheduling module integrated with a shared calendar system. Users can request meetings and view scheduled appointments, including visitation sessions, Socially Necessary Services (SNS) appointments, Multidisciplinary Team (MDT) meetings, court dates, and more. Through an intuitive user interface, users can interact with a calendar view that displays events by day, week, or month, allowing real-time updates and improved accessibility. Meeting details, such as date, time, agenda, and participants, can be securely integrated with the CCWIS/PATH system, facilitating accurate documentation and traceability.

- 12. Functionality to Upload Verification Documents:** Cardinality's WV-MACS solution includes a robust Enterprise Document Management System (EDMS) that supports a wide range of document formats, including AVI, BMP, DOC, DOCX, JPEG, JPG, MP4, PDF, TIFF, TXT, and XLS. This flexibility maintains compatibility with diverse documentation and media requirements, enabling users to securely upload, view, and manage various file types. Each document is enriched with configurable metadata fields—such as title, category, description, document type, author, and timestamp—enabling efficient organization and searchability.

The EDMS provides advanced capabilities for tagging, packaging, and categorizing case-specific information. Leveraging AI-based classification powered by Natural Language Processing (NLP) and Machine Learning (ML), the solution automates document categorization, facilitating scalability, reducing manual errors, and streamlining the case management process. The EDMS also supports secure digital storage, indexing documents by unique identifiers, creation time, author, and document thumbprints, facilitating traceability and accessibility. Uploaded documents are securely archived in the CCWIS, indexed for traceability, and integrated smoothly with other business functions, enhancing operational flexibility. The modular document upload component integrates smoothly across all business functions and modules, maintaining flexibility and scalability for future needs. The EDMS also supports archival, retrieval, and expunging, enabling secure and traceable document management aligned with child welfare requirements.

Through the flexible user interface, users can easily upload documents via a drag-and-drop or file selection feature. The backend processes these uploads, validating file format and size while securely transmitting them to Amazon S3 for encrypted storage. AWS Lambda automates file processing, enriching metadata, and maintaining compliance with validation rules. Metadata is stored in Amazon RDS for PostgreSQL, linking documents to specific cases for quick retrieval. AWS CloudTrail logs all upload actions, providing a transparent audit trail for compliance and accountability.

This feature is included in the current software release and will be implemented by the planned phase go-live date, in accordance with the State's configuration planning. By offering secure, efficient document upload and management capabilities, the WV-MACS solution supports streamlined workflows and enhanced collaboration across child welfare processes.

- 13. Digital Signature Capability:** Cardinality's WV-MACS solution enables authorized users to digitally sign documents securely and efficiently, with signed documents stored in the Comprehensive Child Welfare Information System (CCWIS)/PATH system. This functionality enhances approval workflows, validates document authenticity, and aligns with legal and regulatory standards. Our solution can be integrated with digital signing tools (third-party APIs for digital signature services like Adobe Sign or DocuSign).

Authorized users, such as caseworkers, foster parents, and legal representatives, can digitally sign critical documents like consent forms, safety plans, and family agreements through a user-friendly interface. The solution verifies user authentication and role-based permissions using the RBAC module, enabling secure and authorized access.

- 14. Primary Information Upload Confirmation with Mobile Accessibility:** The solution allows authorized users, such as caseworkers and foster parents, to input and review critical data, including visitation logs, medical updates, and verification documents, through an intuitive and mobile-responsive interface. Before submission, users are presented with a confirmation step to validate the completeness and accuracy of their entries, minimizing errors and maintaining data integrity. This feature enhances accountability and prevents incomplete or erroneous submissions to the CCWIS/PATH system.

The solution prioritizes compliance by logging all user actions through AWS CloudTrail, capturing details of data entry, validation, and submission for audit purposes. With its user-friendly interface, secure workflows, and robust compliance measures, the WV-MACS solution enhances data accuracy, operational efficiency, and traceability. By integrating upload confirmation and mobile accessibility, the solution meets the requirements of modern child welfare communication systems, empowering users to manage critical information effectively while adhering to regulatory standards.

- 15. Secure Access to Documentation:** Cardinality's WV-MACS solution leverages its robust Role-Based Access Control (RBAC) framework to provide authorized users with secure access to a wide range of case-related documentation. This includes essential records such as educational evaluations, medical and dental records, therapeutic and mental health reports, home evaluations, visitation logs, family and safety plans, caseworker contact logs, court filings, and demographic information. This functionality supports effective case management and informed decision-making while maintaining compliance with privacy and child welfare regulations.



**16. Calendar Module:** Cardinality's solution incorporates a robust calendar module that enables authorized users to efficiently schedule and manage events related to a child welfare case. This feature facilitates smooth coordination among stakeholders while maintaining compliance with child welfare requirements. Authorized users can add, modify, or delete events, such as appointments, non-emergency medical visits, Guardian Ad Litem (GAL) meetings, Multidisciplinary Team (MDT) meetings, visitations, vacations, court dates, and Socially Necessary Services (SNS) provider appointments. By centralizing event/meeting management, the calendar module fosters efficient planning and improves operational workflows.

The solution utilizes Role-Based Access Control (RBAC) to enable secure access to the calendar module. This feature restricts access based on user roles, allowing caseworkers, foster parents, and legal representatives to view or manage events as per their responsibilities. The calendar module is fully integrated with the Comprehensive Child Welfare Information System (CCWIS) / PATH system. Events scheduled through the calendar are synchronized with CCWIS in real time, so that the centralized system remains the authoritative source of truth for all case-related activities.

By implementing our calendar module, the child welfare mobile application communication system can achieve streamlined scheduling, enhanced coordination, and improved case outcomes. The solution's design aligns with the operational and regulatory needs of child welfare agencies, enabling authorized users to manage events effectively while safeguarding sensitive data and maintaining a centralized record within the CCWIS/PATH system.

**17. Performance reporting:** The WV-MACS solution will be able to create a performance report that shows the time measurement of the user's responsiveness to questions or requests. Our solution includes a robust reporting module designed to generate detailed performance reports that measure the time taken by users to respond to questions, requests, or tasks. These reports provide valuable insights into user responsiveness, fostering accountability, enhancing workflow efficiency, and identifying areas for operational improvement. Leveraging advanced tools like MicroStrategy, Power BI, Crystal Reports, and Tableau, the reporting module delivers comprehensive data visualizations and actionable insights to meet the demanding needs of child welfare systems.

The performance reports capture essential metrics, including the time a request or question was initiated, the timestamp of user responses, and the total elapsed time between initiation and resolution. Additionally, the system enriches these metrics with metadata such as the user's role, the type of request, and the associated case details. This comprehensive data collection enables stakeholders to evaluate responsiveness accurately and implement necessary improvements to achieve better outcomes.

The reporting module supports both pre-built and custom reporting capabilities. Pre-built reports cover standardized metrics and are categorized based on operational needs, such as geographic regions (e.g., county, city) or case types. Custom, ad hoc reports allow users to tailor insights to specific needs through user-friendly interfaces provided by tools like Tableau and Power BI. These ad hoc reports are classified by turnaround times, maintaining flexibility and adaptability for immediate and long-term analytical requirements.

Dynamic dashboards enhance the reporting experience by offering real-time data visualization. Stakeholders can configure and monitor key performance indicators (KPIs) with tools like

MicroStrategy, which enable the creation of interactive heat maps, trend analyses, and visual summaries. Dashboards are intuitive and provide day-to-day operational insights, enabling users at all levels—caseworkers, supervisors, and administrators—to easily access and interpret the data.

Data security is integral to our solution; all collected data is encrypted both in transit and at rest, stored securely in Amazon RDS for PostgreSQL, and synchronized with Amazon S3. Role-based access control enables sensitive performance data to only be available to authorized users, and audit trails maintained by AWS CloudTrail provide a transparent record of user activities, supporting regulatory compliance and accountability.

The reporting module integrates effortlessly with the Comprehensive Child Welfare Information System (CCWIS)/PATH system, enabling all performance data to be synchronized with case records for a centralized view. By associating metrics with specific cases, the system enables holistic evaluations of user performance while maintaining data consistency across platforms.

By incorporating advanced analytics tools and providing a secure, centralized, and user-friendly reporting environment, Cardinality's solution empowers child welfare agencies/DHS to monitor user responsiveness effectively. This functionality promotes timely decision-making, accountability, and operational efficiency, ultimately driving better outcomes for children and families.

- 18. Reporting module: Pre-defined/Standard and ad-hoc reporting:** Cardinality's solution provides a robust reporting module designed to create performance reports through flexible functionality, offering both predesigned or standard templates and ad hoc reporting capabilities. This dual approach enables users to access standardized reports for routine metrics such as system performance, user activity, and compliance, while also enabling the generation of configured insights tailored to specific operational or analytical needs. The combination of prebuilt and ad hoc options facilitates comprehensive monitoring, informed decision-making, and adaptability to evolving DHS/child welfare requirements.

The system integrates dynamic data visualization tools, including dashboards, heat maps, and KPI trackers, allowing users to explore relationships between data elements and derive actionable insights. Users can export reports in various formats, such as PDF, Excel, and CSV, for sharing or offline analysis. Advanced tools like MicroStrategy, Power BI, Crystal Reports, and Tableau further enhance reporting capabilities, supporting both technical and non-technical users in creating tailored visualizations.

Smooth integration with the Comprehensive Child Welfare Information System (CCWIS)/PATH system maintains data consistency and alignment with case records. The solution captures real-time and historical data, enriching reports with metadata for traceability. Role-based access controls (RBAC) safeguard sensitive information, so that reports are accessible only to authorized personnel. Additionally, audit logs capture all reporting activities, supporting accountability and compliance with regulatory standards.

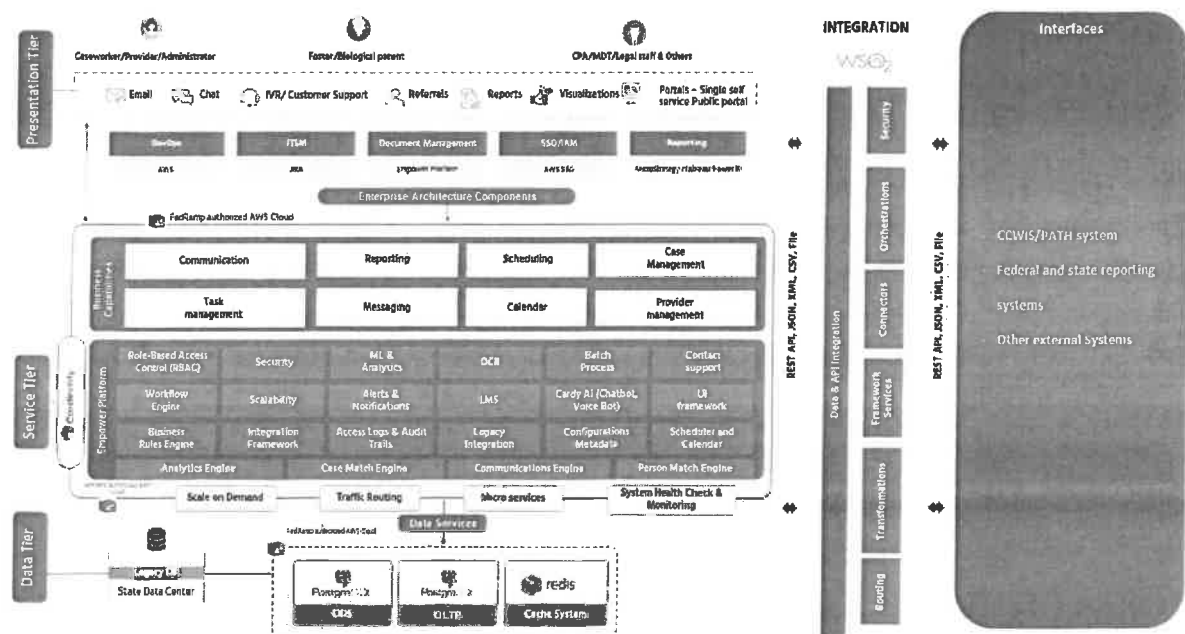
This flexible and secure reporting module empowers West Virginia DHS to monitor performance, track user activities, and analyze case outcomes effectively. By combining predesigned and ad hoc reporting capabilities with advanced visualization tools and robust security, Cardinality's solution supports data-driven decision-making, operational efficiency, and regulatory compliance, aligning with the diverse needs of modern child welfare systems.

## 5.2 Technical Requirements

### Solution architecture:

The WV-MACS solution is built on a robust, multi-tiered architecture designed to deliver secure, scalable, and efficient management of child welfare operations. By integrating advanced business capabilities, a powerful service layer, and smooth interfaces, the WV-MACS solution addresses the diverse needs of the West Virginia Department of Human Services (DHS). This architecture enables secure data exchange, interoperability with current systems, and scalability for future enhancements.

The WV-MACS solution architecture (**Figure 22**) is structured across three primary tiers: Presentation Tier, Service Tier, and Data Tier, each serving distinct but interconnected functions.



**Figure 22: WV-MACS solution architecture**

**Presentation Tier:** The presentation tier acts as the user-facing interface, facilitating a smooth experience for all stakeholders, including caseworkers, foster parents, biological parents, SNS providers, multi-disciplinary teams, legal staff, and administrators. This tier provides access to a unified public portal designed for both self-service and role-specific interactions. Stakeholders interact through a single, consolidated portal that simplifies access to tools and resources. Caseworkers, for instance, can manage cases, schedule appointments, and communicate securely, while foster and biological parents can view case updates, submit documentation, and track their interactions. The portal design enables ease of use and fosters collaboration among all participants in the child welfare ecosystem. Key features of our solution will include email, chat, IVR-based customer support, referrals, reporting, and data visualizations.

**Service Tier:** The service tier forms the heart of the WV-MACS solution, delivering critical business capabilities and functionalities required to manage child welfare operations. These include:

- **Communication and Messaging:** Secure, role-based messaging capabilities for real-time collaboration among stakeholders.
- **Case Management:** Comprehensive tools to track, update, and manage case details, participants, and activities.
- **Task Management and Scheduling:** Intuitive scheduling tools for managing appointments, hearings, and deadlines.
- **Reporting and Analytics:** Real-time reporting tools to provide actionable insights and measure performance metrics.

The service tier is powered by Cardinality's Empower Platform, which incorporates advanced components such as:

- **Role-Based Access Control (RBAC):** Facilitates secure, role-specific access to data and tools.
- **Workflow configurator and Business Rules Engine:** Automates complex workflows and enforces business rules efficiently.
- **Machine Learning and Analytics:** Provides predictive insights to enhance decision-making processes.
- **Alerts and Notifications:** Keeps stakeholders informed about critical updates and deadlines.
- **Learning Management System (LMS):** Facilitates training and workforce development for agency staff.
- **Legacy Integration:** Enables smooth connectivity with existing systems like PATH and CCWIS.
- The platform also supports key features such as OCR for document processing, batch processes for bulk data handling, and Cardy AI for chatbot and voice-based interactions.

**Data Tier:** The data tier provides efficient data storage, retrieval, and processing, serving as the foundation for the solution's operations. It consists of:

- **PostgreSQL Databases**
- **Operational Data Store (ODS):** Facilitates real-time data processing for operational needs.
- **OLTP (Online Transaction Processing):** Manages high-volume transactional workloads.
- **Cache System (Redis):** Improves performance by enabling fast access to frequently used data.
- **State Data Center Legacy Databases:** Maintains compatibility with existing infrastructure, maintaining data integrity during transitions.
- Additionally, the data tier includes advanced features like traffic routing and health monitoring to enable optimal system performance. Scalability is achieved through dynamic resource allocation, allowing the system to handle increased workloads without disruptions.

### Enterprise Architecture Components

The WV-MACS solution will leverage enterprise-grade components to enhance efficiency and integration. These include:

- **DevOps (AWS):** Supports continuous deployment, monitoring, and scaling.
- **ITSM (JIRA):** Manages service requests and incident tracking.
- **Document Management (Empower Platform):** Facilitates secure and efficient document handling.
- **SSO/IAM (AWS SSO):** Manages secure single sign-on and identity management.
- **Reporting Tools (MicroStrategy, Tableau, Power BI):** Provide advanced dashboards and visualizations for comprehensive analytics.

These components enable the solution to be both robust and adaptable, meeting current requirements while allowing for future enhancements.

### Integration and Interfaces

A key strength of our WV-MACS solution is its ability to smoothly integrate with internal and external systems. The architecture utilizes WSO2 Enterprise Integrator to manage and orchestrate these integrations effectively.

#### Integration Features:

- **Data & API Integration:** Facilitates smooth data exchange between the WV-MACS solution and other systems.
- **Framework Services:** Provides data transformation, routing, and orchestration capabilities.

#### Integration Channels:

- REST APIs for real-time interactions
- Support for JSON, XML, and CSV formats for data exchange
- Batch processes for handling large-scale data transfers

#### Interfaces:

- **CCWIS and PATH Systems:** Enable real-time, bidirectional data exchange for case updates, placements, and other critical information
- **Federal and State Reporting Systems:** Maintain compliance by facilitating smooth data submission to regulatory bodies
- **Other External Systems:** Allow integration with third-party tools and services for additional functionality

The integration framework enables data to flow securely and efficiently, enhancing interoperability and compliance with federal and state regulations.

### Scalability and Security

The WV-MACS solution is hosted on a FedRAMP-authorized AWS Cloud, providing a secure and scalable infrastructure. Key security features include:

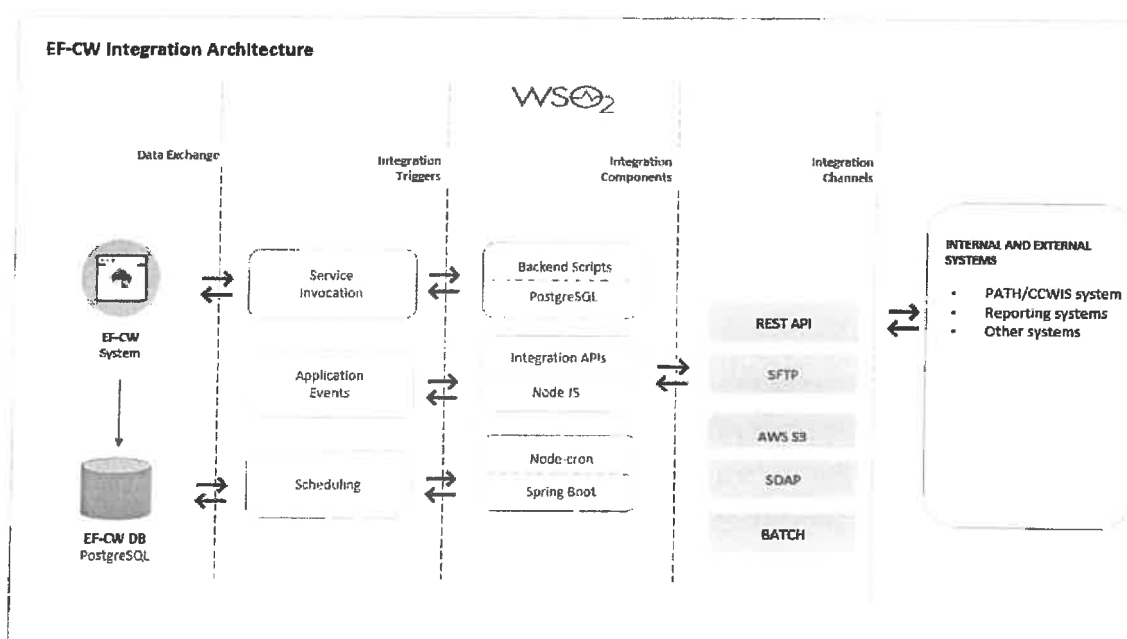
- **Role-Based Access Control (RBAC):** Limits access to authorized users based on their roles
- **End-to-End Encryption:** Maintains data security during transit and storage
- **Logs and Audit Trails:** Provide comprehensive monitoring to track all activities and maintain data integrity

Scalability is achieved through features like dynamic resource allocation, enabling the system to handle growing demands without compromising performance. This enables the solution to adapt to future needs, whether due to increased users, data volume, or new functionalities.

The WV-MACS solution architecture is a comprehensive, secure, and scalable framework tailored to the unique needs of West Virginia DHS. By combining a multi-tiered structure with enterprise-grade components and robust integration capabilities, the solution facilitates smooth operations, enhanced collaboration, and improved outcomes for children and families. This architecture is pre-built to meet today's needs while remaining adaptable for the future, making it an ideal choice for modernizing child welfare operations.

## Integration architecture

The WV-MACS solution is designed to provide smooth and secure integration with internal and external systems, addressing the diverse operational needs of the WV DHS. This architecture (**Figure 23**) facilitates efficient data exchange, compatibility with existing systems, and compliance with federal and state mandates. By leveraging modern technologies and industry-standard protocols, the WV-MACS solution facilitates real-time and scheduled integrations that enhance communication and collaboration among stakeholders.



**Figure 23: WV-MACS Integration architecture**

At the core of the architecture will be the WV-MACS solution, powered by a PostgreSQL database that supports all data operations. Integration is triggered through multiple mechanisms, including service invocations, application events, and scheduled tasks. This multi-layered approach enables data to flow smoothly and reliably, whether in real-time or as part of routine batch processes. Service invocations handle immediate requests, application events capture system-level changes, and scheduling enables periodic data synchronization, allowing for flexible and comprehensive integration capabilities.

The solution employs a robust set of integration components to manage these interactions effectively. Backend scripts in PostgreSQL handle data transformations, while lightweight Node.js APIs act as an integration layer, maintaining scalability and efficient communication with external systems. For scheduled tasks, tools like Node-Cron and Spring Boot orchestrate data updates at predefined intervals, enabling automation of repetitive processes. These components work together to create a reliable and adaptable integration framework.

The solution leverages WSO2 Enterprise Integrator, a robust middleware platform, to streamline data exchange, enable real-time integration, and maintain compliance with federal and state mandates. This comprehensive approach enhances communication, collaboration, and decision-making across stakeholders and systems. WSO2 Enterprise Integrator plays a pivotal role in managing and orchestrating all integration activities. Acting as the central middleware layer, WSO2 enables smooth

connectivity between the WV-MACS solution and external or internal systems through its integration components.

To facilitate secure and efficient data exchange, the solution utilizes a variety of integration channels. REST APIs will enable real-time, synchronous interactions with internal or external systems, while SOAP APIs enhance compatibility with legacy systems that rely on XML-based communication. For file-based data transfers, the solution leverages SFTP (Secure File Transfer Protocol), and AWS S3 provides a cloud-based mechanism for storing and retrieving large datasets securely. Batch processes are employed for bulk data handling, offering flexibility for systems requiring periodic synchronization instead of continuous updates.

The WV-MACS solution integrates smoothly with both internal and external systems critical to the child welfare program's success. For internal systems, it facilitates bidirectional communication with PATH and CCWIS, enabling real-time updates to case records, placements, and communication logs. It can also integrate with state or federal reporting systems to provide dynamic dashboards and analytics that aid in decision-making. The architecture's modular design supports custom integrations with third-party systems, facilitating future scalability and adaptability to evolving agency needs.

The security and scalability of the WV-MACS solution make it an ideal choice for DHS. By leveraging industry-standard protocols, secure cloud services like AWS S3, and role-based access controls, the solution maintains compliance with data privacy regulations such as HIPAA and FERPA. The WV-MACS solution provides a secure, scalable, and adaptable framework to meet the integration needs of West Virginia DHS. By facilitating smooth connectivity with internal and external systems, the solution enhances data accuracy, streamlines workflows, and supports the agency's mission to improve outcomes for children and families. This robust solution is pre-built to drive operational efficiency and enable the agency to remain agile in the face of evolving technological and regulatory requirements.

## 6. Vendor Staffing

**4.1 Vendor Staffing:** Vendor should identify its staff for this project and include resumes for key staff that demonstrate relevant experience with similar projects (i.e., engagement manager, project manager, business analyst, and technical staff). If key project staff are added or replaced during the Project, the Agency reserves the right to review the qualifications and responsibilities of the staff and approve the assignment of the staff before they are officially added to the Project and before they perform any work on the Project. The Vendor should notify the State within two business days if key project staff are added or replaced during the Project. (RFP Section 4.2.1.5)

### Proposed Organization Structure

Team Cardinality is committed to assembling a high-performing, diverse, and inclusive team to successfully deliver the WV-MACS Solution for WV DHS. We have identified key personnel to fulfill critical leadership and management roles, facilitating smooth communication, issue resolution, and successful project execution.

- ❖ **Senior Executive for Escalation:** To address project risks, issues, or concerns that cannot be resolved by the project team, Cardinality designates **Toni Blue Washington** as the senior executive. Toni's role will include:
  - Providing strategic oversight and decision-making authority.
  - Acting as the escalation point for unresolved project risks and concerns.
  - Maintaining alignment between the project's objectives and the Agency's strategic goals. Toni brings extensive leadership experience and a proven track record in managing complex projects, making her a reliable point of contact for high-level escalations.
- ❖ **Dedicated Project Manager for Implementation: Harsha Velamuri**, will lead the implementation phase of the WV-MACS solution. Harsha's responsibilities will include:
  - Overseeing project planning, scheduling, and execution.
  - Managing project deliverables, timelines, and budgets in alignment with the Agency's requirements.
  - Facilitating communication and collaboration between Cardinality, the Agency, and other stakeholders.
  - Proactively identifying and mitigating risks to promote project success.

*"Harsha was the project manager for Georgia Communicare Project in 2023 where Cardinality implemented the Mobile application communication solution for the DHS team. His experience in Agile project management methodologies make him exceptionally qualified to manage the implementation process efficiently and effectively."*

### Proposed Key Persons for this Project:

Cardinality's key resources proposed for this project are given below in **Exhibit 3**. Their resumes are attached in Appendix 1 at the bottom of this document.





Names	Role	Engagement Role
Toni Blue Washington	Accounts Executive	<ul style="list-style-type: none"> <li>• Providing strategic oversight and decision-making authority.</li> <li>• Acting as the escalation point for unresolved project risks and concerns.</li> <li>• Maintaining alignment between the project's objectives and the Agency's strategic goals. Toni brings extensive leadership experience and a proven track record in managing complex projects, making her a reliable point of contact for high-level escalations.</li> </ul>
Harsha Velamuri	Project Manager	<ul style="list-style-type: none"> <li>• Manages the project schedule, assists with team coordination, and is responsible for the delivery &amp; implementation of WV-MACS.</li> <li>• Day-to-day management of project activities.</li> <li>• Hold regular project team meetings (weekly/monthly) with WV representatives and other Program stakeholders to set project priorities and communicate detailed project status.</li> <li>• Serves as the point of escalation for project risks and issues and will coordinate with WV DHS agency project managers.</li> </ul>
Chanakya Katukojwala	Solution Architect	<ul style="list-style-type: none"> <li>• Oversee the development of the proposed solution and provide overall direction for system architecture.</li> <li>• Lead the development team and ensure requirements are implemented in a cohesive, streamlined, and technically sound manner.</li> <li>• Provide technical support translating business requirements into technical requirements.</li> <li>• Ensure that system enhancements are strategically sound and meet the long-term vision of the proposed solution</li> </ul>
Bose Subash	Software Development Lead	<ul style="list-style-type: none"> <li>• Responsible for customizing and configuring the WV-MACS solutions' technical requirements, as well as supporting data configuration and interface integration.</li> <li>• Responsible for handling Cardinality Platform development in its agile sprints across the module sprints.</li> </ul>

Ravi Motwani	Test Lead	<ul style="list-style-type: none"> <li>Responsible for the development and implementation of the test plan, along with leading the Testing team.</li> <li>Work with the WV DHS to define the scope of testing, oversee all testing activities, and apply appropriate test measurements and metrics.</li> </ul>
Yashwanth U	Business Analyst	<ul style="list-style-type: none"> <li>Responsible for gathering and analyzing business requirements, enabling project goals to be met, and serving as a bridge between stakeholders and the development team.</li> </ul>
Derrick Stevens	SME / Trainer	<ul style="list-style-type: none"> <li>Responsible for conducting Training needs, Assessments, and developing Training Plans.</li> <li>Develop training materials, including user manuals, guides, and multimedia presentations.</li> <li>Conduct instructor-led training sessions, facilitate virtual training programs, and manage documentation and reports.</li> </ul>

***Exhibit 3: Key Persons for WV-MACS project Implementation***

#### **Addition or Replacement of Key Project Resources:**

Team Cardinality acknowledges and fully complies with the requirement regarding key project staff changes. If any key project staff are added or replaced during the project, we will promptly notify the State within two business days. Additionally, we will provide the qualifications and responsibilities of the proposed staff for the Agency's review and approval before they are officially assigned and begin work on the project. This ensures transparency, continuity, and alignment with project objectives.

***For the Organization Chart, please refer to Figure 5 in the Executive Summary section.***

## 7. System Information

### System Information: The Agency requires a Vendor-hosted Solution. (RFP Section 4.2.1.6)

Cardinality's WV-MACS solution follows a vendor-hosted model and will be hosted in AWS GovCloud (US-East), maintaining full compliance with the agency's requirement for secure and reliable hosting. AWS GovCloud is specifically designed for U.S. government workloads, offering robust features such as enhanced security, data residency, and regulatory compliance. All agency data will be securely stored in U.S.-based data centers, meeting standards such as FedRAMP, ITAR, and CJIS, thereby safeguarding sensitive child welfare information.

In this hosting model, Team Cardinality will be responsible for hosting, maintaining, and supporting the solution. This includes maintaining availability, performance, and security through proactive system monitoring, regular updates, and comprehensive disaster recovery plans. By taking ownership of these responsibilities, we alleviate the operational and technical burdens on the agency, enabling them to focus on their core child welfare objectives.

Our hosting model offers several key benefits, including scalability, allowing resources to grow with the agency's needs; cost efficiency, by removing the need for infrastructure investments; and reliability, facilitating high uptime and accessibility. Additionally, this approach enhances data security and simplifies maintenance. This model provides a streamlined, secure, and efficient operational experience for West Virginia DHS.

### 7.1 The Solution license and/or subscription option(s) (RFP Section 4.2.1.6.1)

Team Cardinality adopts an industry-standard Software-as-a-Service (SaaS) model to license the proposed WV-MACS solution to agencies. Under this model, agencies pay an annual subscription fee to access Cardinality products and services. The pricing/licensing is flexible and can be tailored to align with agency-specific requirements, providing a cost-effective and scalable solution.

Our SaaS model is based on the number of agency workers who require access to the system. The licensing is offered on a 'Named User' basis, where each Named User is an individual agency employee, contractor, or affiliate with a unique login to the system. The tiered licensing model is designed to align with the agency's workforce size and operational needs. Key user groups, such as administrators, internal users, and external users, are included in the license calculations, while citizen users are excluded. This enables the pricing to remain fair and directly tied to the active system users.

The license pricing includes:

- Access to the low code Empower platform and all associated applications and portals.
- All third-party licenses required for system operations, such as the Report Engine and Business Rules Engine.
- Cloud hosting fees, integrated as part of the AWS-hosted solution.

#### Transition to Subscription-Based Pricing:

Upon completing the implementation phase, the licensing model transitions to a subscription-based per-user pricing structure. Under this structure, agencies pay an annual recurring fee for ongoing access to the SaaS platform and its features, facilitating predictable and transparent pricing.

**Support Services and Maintenance:**

The subscription fees include comprehensive support services, such as:

- Timely issue resolution.
- Regular maintenance updates and system monitoring.
- Continuous improvement recommendations to optimize system performance.

The annual maintenance fee also covers regular upgrades and feature enhancements, enabling the WV-MACS solution to evolve with the agency's needs over time. These services are integrated into the Monthly Maintenance & Operations (M&O) Fee, providing reliable and uninterrupted system support throughout the contract period.

**Hardware and Hosting Costs:**

As the solution is hosted on AWS, all hardware costs are consolidated within the AWS hosting fees, facilitating a streamlined and cost-efficient pricing model for infrastructure needs.

This licensing model enables the WV-MACS solution to be accessible, scalable, and cost-effective for West Virginia DHS, catering to a wide range of stakeholders, including 6,000 children/youth in foster care, 850 child welfare workforce members, 67 SNS provider agencies, 55 legal community users, and 10 CPAs. By incorporating flexible pricing, robust support services, and smooth cloud hosting, the solution empowers agencies to focus on improving child welfare outcomes while maintaining financial predictability.

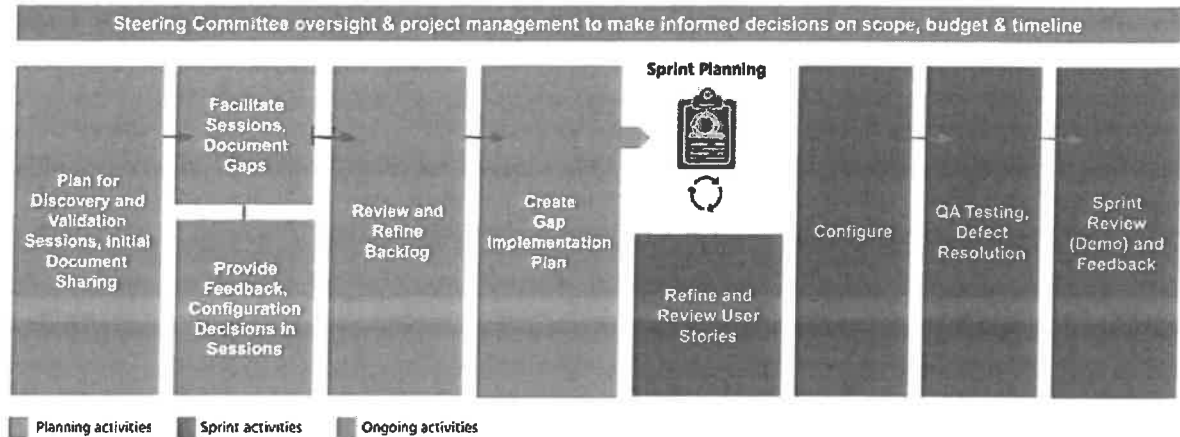
**7.2 The current release and maturity of the Solution (RFP Section 4.2.1.6.2)**

Team Cardinality will deliver its latest Child Welfare mobile application communication software, EF-CW v2025.4.1 - v0 (Base version), to West Virginia DHS within 30 days of project kickoff. This will serve as the baseline version for the modern West Virginia Child Welfare Mobile application communication software (WV-MACS v0).

Our team will be following a gap-based implementation methodology; the baseline version will be used for conducting discovery sessions, and gaps are incrementally addressed using our gap-based implementation model.

EF-CW v2025.4.1 will serve as the WV-MACS Version 0 (v0), and during Sprint 1, we will address some of the identified gaps and update v0 to v0.1, making incremental progress toward WV-MACS Version 1 (v1), the planned go-live version. This iterative process will continue through each sprint, resulting in intermediate versions such as v0.2, v0.3, and so on. Throughout the DDI process, we will deliver incremental progress toward the go-live version, WV-MACS v1 (Phase 1), which is targeted for completion by Aug 2025 and WV-MACS v2 (Phase 2) completion by Dec 2025.

Below **Figure 24** is an outline of our proposed approach for incremental configuration, starting with requirement validation, which creates the initial backlog for subsequent refinement and delivery in sprints.



**Figure 24: Incremental solution configurations**

Team Cardinality's approach to continuous discovery stands in contrast to traditional project methodologies and other vendors. We do not expect every unknown to be defined or every decision to be made prior to commencing development. This method proves valuable, especially when complete requirements are challenging to define up-front. Each sprint in our hybrid-agile model builds upon the last, allowing the integration of feedback and adaptation to new discoveries and decisions throughout the project's progression.

Starting with discovery sessions showcasing demos of our base product, participants and decision makers can immediately relate their business processes or legacy system functionalities to the new solution. This approach not only highlights gaps but also focuses on tactical configurations that are documented for backlog refinement. Prioritized end-to-end workflows, developed through agile sprints, expose necessary decisions, dependencies, user profiles, and other critical elements early in the project, reducing overall implementation risks.

The focus on implementing a basic end-to-end workflow in the initial sprints enables vital features to be operational early on. Frequent live demos coupled with focused review sessions with West Virginia DHS Leadership help refine user stories, manage and prioritize backlogs, and approve demonstrations, thereby maintaining a dynamic and responsive project environment. This approach enables Team Cardinality to remain aligned with stakeholder expectations and project goals, facilitating a successful and timely project delivery.

**7.3 The number of non-production environments included in the subscription or license (RFP Section 4.2.1.6.3)**

Apart from the production environment, our subscription includes four non-production environments: **Development, Staging, Testing, and Training**. These environments are isolated to support iterative development, rigorous testing, user acceptance validation, and training activities. This setup facilitates a robust deployment pipeline, maintaining system integrity and enabling smooth transitions from development to production.

**7.4 Data hosting location(s), with consideration for the fact that Agency data must be stored in data centers located in the U.S. (see Attachment B: Software as a Service Addendum) (RFP Section 4.2.1.6.4)**

Our solution will be hosted in AWS GovCloud (US-East), maintaining compliance with the requirement that all agency data must be stored in the U.S.-based data centers. AWS GovCloud (US-East) is specifically designed for U.S. government workloads, offering enhanced security, data residency, and regulatory compliance, including FedRAMP, ITAR, and CJIS standards. Its geographic proximity to West Virginia reduces latency, providing faster response times and improved system performance for users. Additionally, AWS GovCloud offers built-in encryption for data at rest and in transit, robust disaster recovery capabilities, and scalability to meet future West Virginia DHS needs, delivering reliability and security for sensitive data.

**7.5 Scheduled maintenance including the maximum number of hours per month the system will be unavailable due to maintenance activities and how maintenance will be planned to avoid disruption. (RFP Section 4.2.1.6.5)**

**Maintenance & Operations**

Team Cardinality has the experience of successfully transitioning responsibilities to State teams in the transition from implementation to maintenance operations. Our goal through this plan is effective knowledge transfer in a structured transition that is smooth to end users and does not detrimentally impact system performance or support. We will be working with the State to maintain operational integrity through M&O activities throughout the length of the Contract. The M&O responsibilities and activities commence at the end of the DDI phase. In the initial months of M&O, we will provide stabilization M&O services. After the initial phase, we will start to provide Steady State M&O services, which are expected to need fewer resources with the reduction in issues, defects, and help desk tickets. We recognize the importance of maintaining the system's stability, addressing any emerging issues, and providing efficient support to DHS throughout the M&O phase.

The M&O Plan will outline the specific activities, roles, responsibilities, and resource allocation for the services therein. By adhering to the plan and leveraging the knowledge gained during the pilot, our team will provide effective M&O services that meet DHS expectations. This will facilitate a smooth transition to the Steady State operations. During the Support Phase, we will provide comprehensive maintenance and operations (M&O) support for the system, adhering to a detailed M&O plan that outlines procedures for system operation, standard service-level agreements for performance, issue resolution, and a robust change management process. Team Cardinality will enable a smooth transition to Maintenance & Operations by focusing on supporting users, promptly identifying and resolving system issues, and implementing prioritized changes and enhancements in planned releases.

Our extensive experience in transitioning maintenance to State teams and operating within various support and M&O models positions us well to deliver continuous value to the WV-MACS Solution through updates and enhancements. Throughout this phase, regular planned activities such as disaster recovery testing, security patching, and ongoing capacity analysis/resource optimization will be conducted. Regular reports will be provided, and engagement will be maintained at multiple levels to provide transparency and accountability.

During the transition from statewide implementation to maintenance, we are committed to supporting the state team throughout this process. We will begin transition work early in the project, working closely with the state team through implementation and dedicated knowledge transfer to equip them with the necessary tools and knowledge for success. Ideally, these resources will be key participants in UAT and system training efforts and become SMEs in the new system. The plan for knowledge transfer will outline the roles and responsibilities, along with the timeline for the knowledge transfer. The plan will be documented and delivered in the M&O Knowledge Transfer Plan.

Ongoing WV-MACS solution operations will include updates, patches, repairs, defect resolution, software upgrades, and technical support throughout the contract term. Additionally, all impacted documentation, including training materials, will be updated in parallel with enhancements to verify that artifacts are current at implementation.

Our **Project Manager Harsha**, will manage ongoing communications with the State, including periodic status reports and meetings, immediate issue notifications, and advance notification of scheduled system downtime, so that all requirements are met, and the system remains robust, secure, and optimized.

Our system will be available for 99.9% of the time, excluding the scheduled maintenance activities. For any outage, we will notify the team within 4 hours and prioritize swift resolution.

### Implementation-to-Maintenance Transition

The primary goal for this Maintenance and Operations (M&O) support phase is to provide system reliability, meet the evolving needs of users, address any issues that arise, and enable continuous alignment with State and Federal requirements. Team Cardinality has the experience of successfully maintaining applications with State partners and successfully transitioning maintenance operations to State teams. Following the statewide implementation, the focus will shift to support and operations. We will leverage the child welfare implementation team for M&O activities, which foster continuity, deep system understanding, the ability to quickly adapt to changing requirements, and enable State teams to scale up faster. This integrated support model (**Figure 25**) promotes a smooth blend of development, maintenance, and operations to support end users. Cardinality provides M&O support post-implementation.



**Figure 25: M&O transition methodology**

The following are key tasks for our team during M&O:

- Providing technical support and incident/problem management functions to support users and resolve any identified system issues.
- Proactive monitoring and problem detection to identify any software glitches, defects, or performance-related issues.

- Planning, coordinating, and implementing maintenance releases, security enhancements, defect resolutions, and prioritized enhancements.
- Ongoing maintenance of system training artifacts and system documentation.
- Performance monitoring and the implementation of efficiency enhancements, i.e., refining database requests, enhancing code, and integrating caching strategies.
- Incorporating security improvements, patches, and industry best practices to secure the application from potential breaches.
- Change and impact analysis to support stakeholder decision making, prioritization, and release scheduling.
- Supporting Federal certification efforts and reviews with Federal stakeholders.

### **General Systems Support**

Our system is meticulously designed to meet all the requirements for General Systems Support. By leveraging the scalability, flexibility, and reliability of cloud infrastructure, our solution enables smooth technical and functional operation of the WV-MACS Solution.

### **Technical and Functional Support**

Our solution goes beyond traditional technical and functional support methods by incorporating intelligent chatbots and built-in context-aware Knowledge Management System (KMS) tools. These advanced features enhance the support experience for users of the WV-MACS solution. The intelligent chatbots are equipped with natural language processing capabilities, allowing them to understand and respond to user inquiries in a conversational manner. They can provide real-time assistance, answer common questions, and guide users through various system functionalities. The chatbots also use the KMS, a vast repository of system-related knowledge, which includes FAQs, troubleshooting guides, and best practices. This knowledge is continuously updated and enriched, so that users receive accurate and up-to-date information.

We also have a dedicated support team available to address user inquiries, troubleshoot issues, and provide guidance to system users. Through various communication channels, such as email, phone, or a dedicated support portal, users can reach our support team for prompt assistance.

### **Defect Resolution**

Defect resolution is our priority to maintain high performance. The system promptly identifies, and addresses reported defects. Our support team works diligently to investigate, analyze, and resolve any issues encountered by users. For emergency defects requiring immediate attention, we provide an escalation matrix for support to make sure the system is addressed and concluded.

### **Routine Maintenance**

The system allows smooth routine maintenance changes. Our team will be responsible for managing necessary maintenance tasks, such as security patches, equipment configuration changes, and so on. These changes are implemented with minimal disruption to the system, facilitating continuous availability and optimal performance. We work closely with the State to schedule maintenance activities during periods of low system usage, minimizing any potential impact on system availability. By adhering to mutually agreed-upon maintenance schedules, we will provide uninterrupted access to the WV-MACS solution.



### **Downtime Communication**

We maintain open and transparent communication with the State regarding any activities that might impact system downtime. In case of urgent deployments or patches, we promptly notify the State, providing detailed information about the planned downtime, its duration, and any necessary actions on the State's part. This allows the State to inform users, plan accordingly, and implement any required contingencies.

### **Ad-hoc Report and Query Development**

The communication system for child welfare will offer support for ad-hoc reports and query development requests. All stakeholders will be able to generate custom reports or queries to extract specific information or perform data analysis, as needed.

### **Infrastructure Management**

Our comprehensive support model includes maintaining the application infrastructure and toolset for all non-production and production users of the WV-MACS Solution. We verify that the underlying infrastructure remains robust and up-to-date, capable of supporting the system's current and future needs. This involves forecasting and obtaining the necessary license agreements to maintain compliance with applicable regulations and licensing requirements. We will be addressing all functional issues, applying patches and updates, performing preventative maintenance, planning, and executing system upgrades, as well as regularly monitoring system performance and providing performance reports to the State. Additionally, we proactively communicate all available information on product roadmaps, planned upgrades, and enhancements to keep the State fully informed. We value the State's input to maintain alignment with their requirements and goals. Through these measures, we facilitate the WV-MACS Solution to remain resilient, secure, and optimized.

### **Application Monitoring**

We use the extensive infrastructure services available as part of the AWS platform to deliver a high-performance system to the users. The cloud infrastructure is constantly monitored using AWS CloudWatch, which is a monitoring and observability service for the application infrastructure. It provides data and actionable insights to monitor the applications and helps identify and respond to performance changes and optimize resource utilization. Infrastructure and Performance logs are continuously captured and will be used for publishing scheduled reports highlighting the performance metrics of the application. These performance logs will be used by our team to validate that the application meets or exceeds the expectations of DHS.

The CloudWatch Synthetics' capability to create "canaries" helps assess the performance of the application from a user standpoint. It provides insights into key metrics such as Availability, Latency, Load time, and API response times, which provide a detailed understanding of the application performance. These canaries can be scheduled to run every minute, providing a complete log of application performance during business hours. This helps optimize the user experience and application performance.

CloudWatch Synthetics together with AWS X-Ray, provides a timeline view of the requests as they travel through the application. It provides visual data across payloads, APIs, functions, and so on, offering detailed traces and constructing a service map. This service map is then used to generate powerful analytics to quickly identify and debug issues before users encounter them. X-Ray Analytics helps run analytics to filter, compare, and analyze traces to identify root causes of application

performance issues. Enabling AWS CloudWatch Service Lens creates a highly observable map of our services, providing rich insights into the traces, metrics, alarms, logs, and related application health and performance indicators.

This log will be used to provide a dashboard that offers ad-hoc analytics and insights, including metrics such as application uptime during business hours, Average Response Rate (ARR), and others. Our solution will be configured to provide an ARR of 1 second or lesser, which can be periodically validated. It will also be designed to provide a high uptime of 99.999% if we enable multi-AZ configuration in AWS.

Our comprehensive application monitoring includes troubleshooting, security incident management, and helpdesk support. We proactively monitor the WV-MACS Solution to maintain smooth and uninterrupted operation. Our dedicated support team is equipped to handle security incidents promptly, employing best practices and incident response protocols to mitigate risks effectively. Additionally, we provide help desk support, offering timely assistance and guidance to users encountering any challenges or requiring system-related support. As part of our commitment to continuous improvement, we provide recommendations on architecture, software, or hardware adjustments that can minimize operational risks. These recommendations are shared with the State every semester, enabling proactive risk mitigation and verifying that the system operates in an optimized environment.

### **Issue Management**

Our commitment to providing reliable support for the system includes proactive planning and flawless execution to minimize issues. However, if incidents or problems do occur, our support team will work closely with DHS to resolve them in a timely manner. We have a clear escalation procedure and a matrix so that any production issues receive the necessary attention. This verifies that critical issues are escalated through the appropriate channels, providing swift resolution and minimizing any potential impact on system functionality.

Our approach to providing technical support and comprehensive incident management is based on our experience supporting users, empowering State support teams, and implementing modernized systems and industry best practices following the ITIL framework. We propose following a tiered support model, using JIRA to track and manage incidents while maintaining a linkage with requirements and configurations. Moreover, the Incident Management Plan will be formalized with DHS.

Based on our success in transitioning user support in Maryland and other States to State teams, we are confident we can enable, empower, and support DHS technical support team. As part of our support process, resolutions are validated by the reporting user to validate that the reported problem is solved. Through JIRA, end-users will receive email updates throughout the process, and requirements can be linked directly to incidents and reported upon. Each tier in the process takes responsibility for correlating and linking the ticket to relevant requirement(s), other incidents, test cases, processes, and more. JIRA allows for ease of search in finding and associating requirements with incidents. It will enable this traceability, enabling impact analysis, change control, and thorough testing. Additionally, JIRA will empower the support team with dashboards and metrics for monitoring and reporting on incidents.

A Triage SOP will be developed and approved by DHS outlining the initial impact assessment and ticket severity/priority. As part of the ticketing process, and with each subsequent review, the impact of the problem will be assessed, and the ticket's severity will be designated. The severity will drive escalation and align with the Escalation Plan. This tiered approach verifies that incidents are managed efficiently and effectively, minimizing downtime and facilitating the continued operation of the system.



The incident management process will follow a tiered approach to categorize and manage incidents based on their severity and impact. This approach validates that incidents are addressed in a timely and effective manner, aligning with the Escalation Plan and the Communications Plan. The severity levels, as outlined in the scope of work, are categorized into four levels: Critical, High, Medium, and Low. Each level has a specific description and resolution time:

- **Critical:** System failure, unable to proceed with selected function or dependent components unavailable or functionally incorrect. Resolution time will be within four hours of identification.
- **High:** Unable to proceed with selected function or dependent components unavailable or functionally incorrect, but an acceptable workaround is available. Resolution time will be within one business day of identification.
- **Medium:** Restricted function capability, but processing can continue. Resolution time will be within five business days of identification or resolution time approved by the State.
- **Low:** Minor cosmetic changes needed, usability errors that do not affect the quality and correctness of function. Resolution time will be within two weeks of identification or resolution time approved by the State.

### Access Management

Our team's RBAC (Role-Based Access Control) plays a crucial role in providing access management within the WV-MACS solution application. RBAC limits safe access to information by granting access privileges based on specific roles assigned to individuals. It accommodates the access controls for all existing roles in the CCWIS system.

Additionally, the solution allows for the creation and configuration of new roles as needed, providing adaptability, and verifying that access privileges remain aligned with the evolving needs of the system. We will assist in defining user roles and security configurations for the system, including the creation of new roles, and monitoring of user access rights based on internal requirements. We will verify the proper management of unique login IDs and security profiles for authorized users, including contractors, as designated by DHS.

### Performance Monitoring Tools

We prioritize delivering robust and high-performing systems. We achieve this through a multi-layered performance testing methodology that leverages industry-leading tools like LoadRunner, JMeter, Dynatrace, AppDynamics, and CA Introscope. This comprehensive approach assesses the entire technical architecture, including code, integrations, databases, networks, and hardware, validating all interfaces function optimally under varying loads and defined performance requirements. We identify and address potential bottlenecks proactively, enabling the interfaces to handle real-world demands.

Furthermore, Cardinality employs a proactive performance monitoring strategy. Our team conducts daily monitoring of system operations, recommending necessary adjustments to maintain peak efficiency and user experience. This ongoing monitoring encompasses all system components, including operating systems, third-party integrations, databases, and related infrastructure. We also analyze and probe system components upon request, assessing database integrity and performance. Based on these findings, we recommend actions to meet or improve upon established Service Level Metrics (SLMs), maintaining your system consistently delivers exceptional performance.

## **Release Management**

After the implementation, we will follow a well-defined release strategy for continuous improvement, as part of the Maintenance & Operations phase. The three-pronged approach to addressing system upgrades and enhancements is as follows:

Our WV-MACS solution follows a structured release management process to provide continuous improvement and alignment with user needs. Major releases will introduce significant updates to infrastructure and user experience, incorporating user feedback to align with industry best practices. In addition, minor releases will deliver cumulative enhancements and bug fixes based on continuous user surveys, enabling quicker adoption of improvements while minimizing risk and cost. For urgent needs, critical patch releases are deployed collaboratively by the customer success and implementation teams to address specific issues impacting projects. These hotfixes are cumulative, resolving critical bugs, and are subsequently included in the next minor release, facilitating smooth system updates and stability.

## **Release Planning and Communication**

We will verify that there is a smooth upgrade and enhancement process with minimal disruption and user impact. For all changes, we conduct a thorough technical impact analysis and risk identification, proactively addressing and mitigating potential issues. We perform comprehensive testing, encompassing functional, regression, performance, and security aspects, as per State requirements. Our team actively supports user acceptance testing and orchestrates migration to production, aligning with scheduled maintenance windows to minimize downtime.

Furthermore, we incorporate release reviews as a regular agenda item in our M&O status meetings. This collaborative approach allows State staff to provide input on minor releases, stay informed of upcoming features and fixes, and discuss the integration of these enhancements into the project's overall release schedule. During these sessions, we provide summaries of included features and fixes, update system documentation with dated and appended change logs, and furnish DHS with comprehensive release notes detailing changes, potential impacts, and any necessary user or administrator instructions. This proactive communication empowers the State to plan for upcoming updates and enable a smooth transition during product upgrades and system enhancements.

Team Cardinality is committed to minimizing downtime during routine maintenance and planned updates by scheduling these activities outside business hours. Our approach involves planning releases, security patching, and other impactful activities to minimize business disruptions, typically completing these tasks at night with special operational procedures in place. We strive to minimize impacts and complete routine updates in the shortest windows possible. Generally, minor and major releases are completed within a few hours outside of business hours (overnight or weekends), complemented by releases for bug fixes and enhancements.

Release dates and maintenance windows will be coordinated with the agency. We have established special procedures for staff to access critical data during maintenance windows, such as allowing operational staff access to pre-production environments for decision-making purposes. This schedule facilitates timely updates while providing flexibility to bundle and deploy changes systematically. High-impact issues that significantly affect end-users may prompt expedited releases to verify critical fixes are addressed swiftly. Release preparation includes comprehensive testing, documentation, and

communication to validate stakeholders are well-informed and the deployment process is smooth. Once validation in the staging environment is complete, updates are rolled out to production.

To address critical post-release issues, we implement an agile patch management process that allows for the release of emergency patches outside the regular schedule. Continuous post-release monitoring is crucial to promptly identify and resolve unforeseen issues in the production environment. Stakeholder feedback will be actively collected to validate the effectiveness of bug fixes and enhancements, facilitating continuous improvement of the release process. This iterative approach, driven by feedback and evolving business needs, enables the WV-MACS solution to remain robust and user-centric.

### **Surge Support capability**

Team Cardinality is prepared to smoothly manage surge scenarios and manage exceptional system performance even during periods of exceptionally high activity. Our comprehensive plan leverages the inherent scalability of the cloud and our commitment to proactive support and collaboration with DHS. Firstly, our AWS-based system is designed to automatically scale resources—compute power, storage, and database capacity—in real-time to accommodate sudden spikes in user activity or data volume. This dynamic scaling, powered by the elasticity of the AWS cloud platform, enables our system to effectively handle increased load without compromising performance or user experience.

Additionally, we continuously monitor system health and performance metrics. This proactive approach allows us to identify potential bottlenecks or resource constraints before they impact system availability. In the event of a surge, real-time alerts will notify our team, enabling us to take proactive measures and scale resources pre-emptively to mitigate any potential performance issues.

Finally, Team Cardinality provides round-the-clock support during both normal operations and surge events. Our dedicated support team will be readily available 24/7 to collaborate closely with DHS. This collaboration provides clear communication and a prompt response to any surge-related needs or requests. Our team will work diligently to address your requirements and verify the system continues to function optimally throughout the surge event. By prioritizing open communication and collaboration throughout the process, we can effectively address surge scenarios and maintain minimal disruption to your operations.

### **Helpdesk Support**

Team Cardinality has more than 20 years of experience successfully supporting both daily development and daily Operations and Maintenance (O&M) across several of our government contracts. We understand the critical nature of the defined hours of operation and will continue to operate within the existing hours of operation as defined in the solicitation. Team Cardinality will provide coverage for all 3-tier support (Tier 1, Tier 2 & Tier 3) with coverage during those hours through staggered shifts and provide on-call support on weekends and holidays.

**Tier 1 Support:** Team Cardinality's Help Desk team will provide Tier 1 support to end users. Team Cardinality will assist them with various system-related technical issues, including but not limited to outages or programming errors. Our proposed solution includes various user assistance features like:

- Self-serve resolutions related to login, password resets, etc. using Forgot Password and MFA features.
- Chatbot Assistant and Knowledge Management System (KMS) with access to FAQs and How-to training videos.

- In-built contact support feature for Easy ticket creation, communication, regular updates, and tracking to resolution.
- The Role Based Access Control component of the Cardinality solution will be accessible to manage user roles, accounts, and permissions. Team Cardinality will provide comprehensive training, detailed product documentation, and How-to training videos in KMS to empower the system administrators.

These features will make it easy for all users to self-serve and resolve the most common issues in accessing the system.

The Tier 1 help desk team will be able to report issues to Team Cardinality's Tier 2 helpdesk team via multiple channels:

- Chatbot Assistant
- Agency's existing Ticketing Tool
- In-built contact support feature for ticket creation
- Support Email Id
- Contact the product support engineer by phone.

**Tier 2 Support:** Team Cardinality's Tier 2 engineers will support more complex issues related to applications, cases, workflows, and user configuration issues. We will work with users and leverage system administration and troubleshooting tools to resolve incidents. These responsibilities will include handling application issues, user issues, workflow issues, and more. Our Tier 2 engineers will use application logs, DB Queries, and application configurations to resolve issues. Tier 2 will maintain metrics on ticket trends and identify areas of value to target. This process will include expanding the knowledge base with known issues and resolutions and communicating them to Tier 3 when critical incident categories need to be prioritized. Typically, Tier 2 issues are resolved through configuration changes or database fixes.

**Tier 3 Support:** Tier 3 support is provided by Team Cardinality's experienced product specialists with in-depth functional and technical knowledge. This is available for both operational and advanced issue resolutions. Our specialists have technical and engineering proficiency, complemented by business and process expertise, enabling them to effectively manage the application, review Tier 3 issues, and devise resolution strategies based on ticket severity, risk, and impact. Tier 3 support offers an advisory role to Tier 2 support, offering guidance on troubleshooting, system training, SOP creation and improvement, knowledgebase enhancement, and resolving user tickets when needed. Typically, Tier 3 issues involve resolution through configuration changes, database fixes, and emergency code releases.

Team Cardinality will have a resource available 24/7 to support the WV MACS users for critical production issues (Severity Tier 1), where the platform is entirely non-functional and inaccessible to all users. For routine customer support, we will staff the following hours:

- Staffed Monday–Friday, 7:00 AM to 7:00 PM Eastern time (EST).
- Severity one issues during off hours and weekends will trigger an alert from the operations team and will be sent to the on-call personnel responsible for engaging the proper resources and coordinating communications.

- On-call team members respond to the pager duty alert within 15 minutes.
- If the issue is internal to WV-MACS systems, we will engage the appropriate on-call staff until the issue is resolved. Our resources in our developer labor category will provide support for this Tier 3 ticket resolution.

## 8. Compliance with Mandatory Project Requirements (§ 4.2.2)

**8.1 General Project Requirement:** Vendor must host an initial planning session(s) with the Agency within 30 days after project start date, with the goal to finalize the project plan and schedule. (RFP Section 4.2.2.1)

Within 30 days of the project start date, Team Cardinality will host initial planning sessions with the WV DHS team as part of the Initiate Phase. These sessions aim to align on the project's future vision, finalize the project plan, and establish governance and communication processes. Key activities include conducting kickoff meetings to align with stakeholders, defining project goals, confirming requirements, and identifying any gaps between the baseline solution and project needs. Additionally, we will collaborate with DHS to establish workstreams (agile teams), create work plans, and outline deliverables, timelines, and resource requirements. This process enables clear communication, stakeholder engagement, and an agreed-upon Scope of Work (SOW) to guide the project's success.

**8.2 Vendor Staffing:** The awarded Vendor will provide staffing resources to successfully complete the implementation tasks, including system configuration, customization, testing, training, and go-live support tasks to meet Agency requirements. The Vendor's internal policies and procedures for hiring must comply with ((RFP Section 4.2.2.2):

→ WV Office of Technology Policies (<https://technology.wv.gov/ot-policies>), particularly PO1012 Contract Management (RFP Section 4.2.2.2.1)

→ Agency Office of Shared Administration the Office of Management Information Services (OMIS) Policy #0529 (Attachment C: Vendor/Contractor Employee Background Check Policy) (RFP Section 4.2.2.2.2)

→ OMIS Procedure #OP-35 (Attachment D: Vendor/Contractor Employee Background Check Procedure). (RFP Section 4.2.2.2.3)

Team Cardinality confirms that our team will fully adhere to the staffing requirements outlined in Section 8.2 of the RFP. Our internal hiring policies and procedures are fully compliant with the WV Office of Technology Policies, including PO1012 Contract Management, as well as the Agency's Office of Shared Administration requirements. We have carefully reviewed Attachment C (Vendor/Contractor Employee Background Check Policy) and Attachment D (Vendor/Contractor Employee Background Check Procedure), and our staffing practices align with OMIS Policy #0529 and OMIS Procedure #OP-35. Cardinality is committed to providing the necessary resources to complete all implementation tasks, including system configuration, customization, testing, training, and go-live support, while meeting or exceeding Agency requirements.

**8.3 Project Manager:** The awarded Vendor will provide a project manager-and the Agency will provide a project monitor--during the system implementation phase. (RFP Section 4.2.2.3)

Team Cardinality has identified **Harsha Velamuri** as the Project Manager for this project. He will be responsible for the successful implementation of our solution, and he will coordinate with the agency provided Project Monitor during the implementation phase.



**8.4 Training Requirements: The Vendor must provide current, digital user-specific training and information, including but not limited to: (RFP Section 4.2.2.4)**

**8.4.1 On-demand video instructions or demonstrations for each type of user ((RFP Section 4.2.2.4.1)**

**8.4.2 Digital user guides or manuals (RFP Section 4.2.2.4.2)**

The training content must be tailored to specific roles and users, including, but not limited to the roles listed in Table 1 above and others who will need information and/or participate in the continuum of care for the child.

Cardinality is fully committed to delivering comprehensive, role-specific training to support the successful adoption and usage of the WV-MACS solution. Our training approach is designed to empower all stakeholders—including caseworkers, foster parents, biological parents, CPAs, SNS providers, MDT members, and legal representatives—with the knowledge and resources needed to navigate the system effectively.

## Comprehensive Digital Training Program

To align with the Agency's training requirements outlined in Section 4.2.2.4, Cardinality will develop and deliver a robust, multi-format training program that includes:

### 1. On-Demand Video Instructions and Demonstrations (4.2.2.4.1)

Cardinality will produce high-quality, user-specific video training modules tailored to different roles within the child welfare ecosystem. These on-demand instructional videos will provide step-by-step demonstrations on key functionalities, ensuring that each user understands how to efficiently perform their tasks within the system. Training topics will include, but are not limited to:

- **Case Navigation & Document Access:** How to securely log in, navigate the system, retrieve case files, and view relevant documentation.
- **Document Upload & Management:** Proper methods for uploading, tagging, and managing case documents while ensuring compliance with metadata and validation requirements.
- **Scheduling & Calendar Management:** Instructions on setting up visitation schedules, MDT meetings, and court dates.
- **Secure Communication & Collaboration Tools:** Best practices for using the system's messaging and alerts module to communicate effectively with other authorized users.
- **Electronic Signatures & Form Submissions:** How to securely sign and submit digital forms, including release forms.

Each training module will be interactive, incorporating guided walkthroughs and knowledge checks to reinforce learning. The content will be hosted on a secure, web-based training portal, allowing users to access materials at their convenience.

### 2. Digital User Guides and Manuals (4.2.2.4.2)

In addition to video-based training, Cardinality will provide comprehensive digital user guides and manuals tailored to each user role. These resources will include:



- **Step-by-Step Instructions:** Detailed walkthroughs of system functionalities with annotated screenshots.
- **Troubleshooting & FAQs:** Common user issues and their resolutions to support independent problem-solving.
- **Role-Based Training Content:** Specific guides for caseworkers, foster parents, legal representatives, and administrators to align with their distinct responsibilities.
- **System Update & Feature Enhancements Documentation:** Regularly updated documentation to reflect new features, ensuring ongoing user proficiency.

These materials will be easily accessible via the WV-MACS portal and downloadable in multiple formats (PDF, HTML, interactive web pages) to accommodate different learning preferences.

### Tailored Training for Specific User Roles

Understanding that different user groups have varying levels of technical expertise and system interaction, Cardinality will customize training content based on the specific needs of each role. As outlined in Table 1 of the RFP, this includes:

- **Caseworkers & Supervisors:** In-depth system training covering case management, documentation, reporting, and compliance workflows.
- **Foster Parents & Biological Guardians:** User-friendly training focusing on secure document access, electronic form signing, and communication tools.
- **CPAs & SNS Providers:** Guidance on data sharing, appointment scheduling, and reporting functionalities.
- **Legal Professionals (GALs, Court Officials):** Training on accessing and reviewing legal documents, signing court-related forms, and secure communication within the system.
- **Agency Administrators:** Advanced training on system configuration, user management, reporting, and audit functionalities.

### Flexible Training Delivery & Ongoing Support

- **Self-Paced Learning:** Users can complete training at their convenience, with the ability to revisit materials as needed.
- **Live Webinars & Q&A Sessions:** Cardinality will supplement digital training with periodic live training sessions, offering real-time engagement with system experts.
- **Help Desk & Knowledge Base:** A dedicated support portal will provide additional self-service resources, including troubleshooting guides and video FAQs.

Cardinality's training program is designed to provide a seamless learning experience, equipping all stakeholders with the skills necessary to maximize the value of the WV-MACS solution. Our combination of on-demand video tutorials, digital user guides, and role-based training ensures that every user can confidently navigate and utilize the system to enhance collaboration and efficiency in child welfare case management.



**8.5 Operational Technical Support:** The Vendor must provide technical support for State and public users. Users may communicate issues to the Vendor by telephone. The Vendor must provide a telephone number that is answered by qualified technical staff who are available to users Monday through Sunday from 7 a.m. to 7 p.m. eastern time (ET). The Vendor must provide after-hours and holiday on-call support for critical incidents from expert technicians who are familiar with the Agency. The Vendor must respond to user support requests in the caller's preferred language or with oral interpretation services. (RFP Section 4.2.2.5)

Team Cardinality is dedicated to delivering reliable and responsive technical support for both State and public users. We will provide a toll-free telephone number, enabling direct access to qualified technical staff who are available Monday through Sunday from 7 a.m. to 7 p.m. Eastern Time (ET). Our support team is trained to address user inquiries, troubleshoot issues, and resolve problems efficiently, maintaining high levels of user satisfaction and system reliability.

To address critical incidents outside standard operating hours, we will provide after-hours and holiday on-call support. This will be managed by a dedicated team of expert technicians who are well-versed in our systems, facilitating prompt and effective resolution of high-priority issues. A defined escalation matrix will guide incident management so that urgent matters are routed and addressed quickly, minimizing potential disruptions.

Cardinality will staff its support team with representatives fluent in commonly spoken languages other than English such as Spanish. For cases where immediate multilingual support is unavailable, Cardinality will integrate third-party language interpretation services to facilitate real-time communication with users. Users contacting the support center will have the option to select their preferred language via IVR (Interactive Voice Response) or chatbot prompts. To further support users in their preferred language, Cardinality will provide translated FAQs, user guides, and troubleshooting materials.

Our support services are structured within a tiered model to enable efficient issue resolution. Tier 1 handles basic troubleshooting and inquiries, Tier 2 addresses more complex issues requiring advanced expertise, and Tier 3 focuses on critical system-level support and root cause analysis. Every issue reported will be logged in our incident management system, such as JIRA, with users receiving unique ticket numbers for tracking and regular updates during the resolution process.

Team Cardinality will also leverage proactive monitoring tools, such as AWS CloudWatch, to identify and mitigate potential issues before they impact users. Our support approach is designed to enable minimal downtime, rapid issue resolution, and continuous alignment with the State's expectations. By combining robust support processes, expert staffing, and a focus on inclusivity, we aim to deliver a smooth technical support experience for all users.

**8.6 Service Level Agreement (SLA):** The Vendor must acknowledge and agree to the SLA requirements outlined in Appendix A: Service Level Agreements (SLAs). (RFP Section 4.2.2.6)

Cardinality acknowledges and fully agrees to the **Service Level Agreement (SLA)** requirements outlined in **Appendix A: Service Level Agreements (SLAs)**. We recognize the critical importance of maintaining system reliability, performance, and responsiveness to meet the needs of the agency and its stakeholders. Cardinality commits to achieving **99.9% system uptime**, delivering consistent

availability of the solution. Additionally, we will adhere to the specified **issue tracking, response, and resolution timelines**, addressing issues promptly based on their severity to minimize disruptions and maintain smooth operations.

We further confirm our commitment to providing comprehensive **support services** during the defined hours, including on-call availability for critical incidents. Cardinality will deliver detailed **monthly performance reports** that include issue summaries, resolution timelines, and corrective actions taken to improve system performance continually. Our team is dedicated to aligning with the outlined SLAs, facilitating a reliable, transparent, and high-performing solution that meets the agency's expectations.

**8.7 Functional and Technical Requirements:** The Vendor must indicate in Appendix B: Functional and Technical Requirements that it will furnish all mandatory requirements. (RFP Section 4.2.2.7)

Team Cardinality fully acknowledges that our solution, WV-MACS, will comply with all the requirements outlined in **Appendix B: Functional and Technical Requirements of the solicitation**. We are committed to delivering a solution that meets the expectations set forth in the solicitation. Our team has conducted a thorough review of each mandatory requirement, and we have carefully documented our responses in Appendix B, clearly indicating our capability to fulfill those needs. For each requirement, we have specified whether the functionality is provided out-of-the-box or achieved through minor configurations, facilitating complete transparency and alignment with the State's expectations. Our solution is built on a robust, scalable, and secure microservices architecture, leveraging industry best practices and advanced technologies to maintain compliance with functional and technical standards. Additionally, we have developed a systematic approach to implementation and ongoing support to enable the timely and efficient delivery of all mandatory functionalities. This approach underscores team Cardinality's dedication to addressing the State's child welfare operational priorities, maintaining compliance, and delivering a solution that fosters long-term success and sustainability.

**8.8 Reporting:** The Vendor must include reporting functionality as part of the Solution (RFP Section 4.2.2.8)

### **Compliance with Reporting Requirements**

Team Cardinality has reviewed the reporting requirements outlined in the West Virginia RFP and is fully committed to addressing those expectations. Reporting plays a critical role in operational efficiency and data-driven decision-making, and our solution offers robust, intuitive, and adaptable reporting capabilities using our reporting module. Designed with ease of use in mind, our reporting module integrates smoothly with industry-standard platforms, including MicroStrategy, Power BI, Tableau.

### **Standard Reports**

Our solution includes pre-built reports tailored to meet West Virginia's needs, offering immediate insights and actionable data outputs. These reports can be executed directly within the system and exported in formats such as Microsoft Excel, CSV, and Adobe PDF.

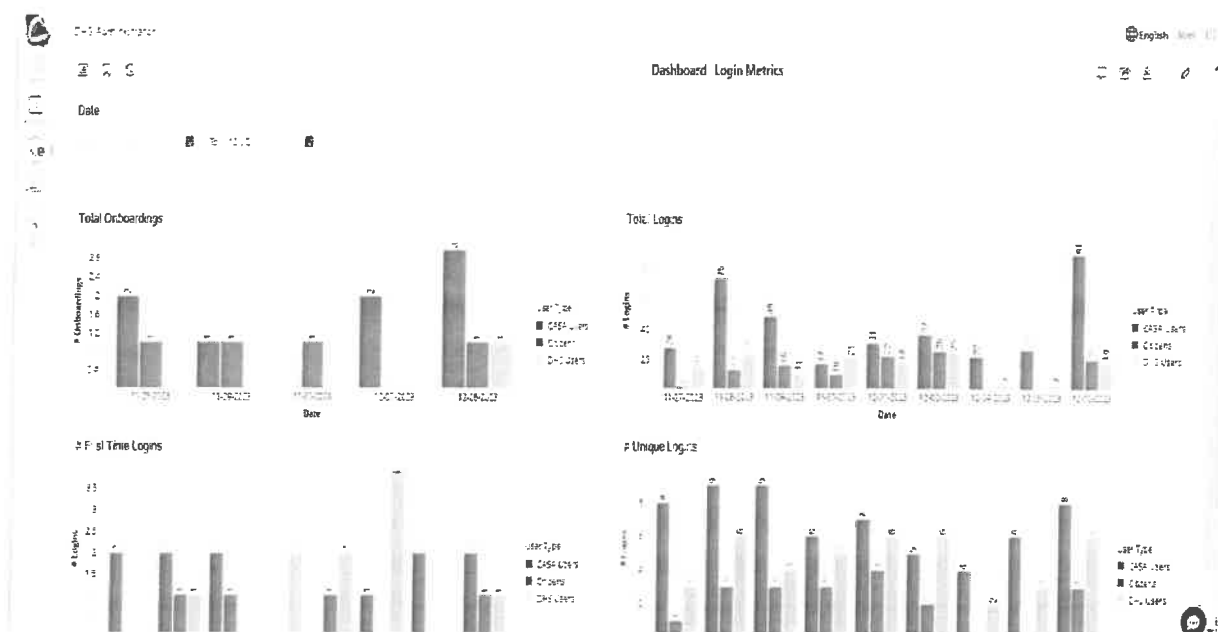
### **Ad Hoc Reporting**

Recognizing the need for flexibility, our solution provides a secure and user-friendly environment for creating ad hoc reports. This functionality enables state personnel to generate custom reports to meet unique and dynamic needs

### Dedicated Reporting Environment

To enhance performance, our solution incorporates a dedicated reporting environment that uses a segregated data store for real-time or near real-time reporting. Processor-intensive reports run asynchronously, enabling core system operations to remain unaffected. Advanced users can employ SQL support for detailed data manipulation, while tools like MicroStrategy enable the creation of dynamic dashboards as shown in **Figure 26**, offering stakeholders insights through visualizations, trends, and KPIs.

The solution includes an Enterprise Data Warehouse (EDW) that consolidates all data into a centralized repository. This enables real-time and batch access, streamlining data processing for large volumes of information. Data staging, cleansing, and processing uphold integrity, allowing for faster data retrieval and analysis. This infrastructure empowers West Virginia to meet its reporting obligations efficiently and effectively.



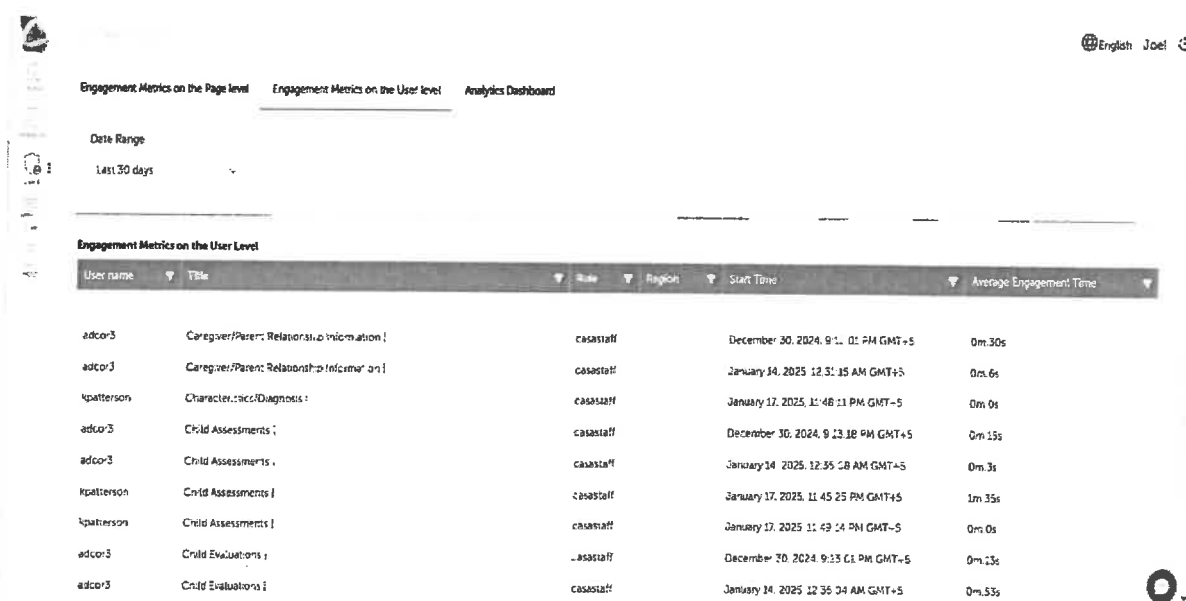
**Figure 26: Configurable dashboard screen**

### Dynamic Dashboards and Self-Service BI

Dynamic dashboards as shown in **Figure 27** form a critical feature of our solution, providing visualizations such as histograms, trend analyses, area charts, and KPIs. These dashboards are customizable based on user roles and offer a self-service BI layer, empowering users to create their

own dashboards and analytics independently. This feature reduces reliance on IT support while maintaining robust security through Role-Based Access Control (RBAC).

Our solution delivers a robust and flexible reporting system tailored to meet West Virginia's specific needs. By offering pre-built and ad hoc reporting capabilities, dynamic dashboards, and secure API connectivity, our solution enables state agencies to make informed decisions quickly and securely. With a dedicated reporting environment and centralized data management, West Virginia will have the tools necessary to generate actionable insights and achieve operational excellence.



**Figure 27: Report/metrics on user level showing average engagement time**

**8.9 System Security:** The Vendor must provide a plan for business continuity and disaster recovery (BCDR). The BCDR plan will include complete, proper, and routine data and information backups. The plan will describe the resolution time of issues with varying severity levels and the frequency of review and update. Vendors must provide a copy of their standard BCDR plan as an attachment to their technical proposal. (RFP Section 4.2.2.9)

### Business Continuity and Disaster Recovery Plan

Team Cardinality recognizes that fulfilling all commitments during emergencies is essential for sustainable business operations. As a provider of IT systems and products to government agencies, we prioritize maintaining and restoring service levels in the event of an emergency. Our approach includes both short-term and long-term strategies to facilitate business continuity and the delivery of critical services. A copy of our Standard BCDR Policy and Plan is attached as separate documents vide file name:

#### 1. Business Continuity and Disaster Recover policy

## 2. Business Continuity Plan

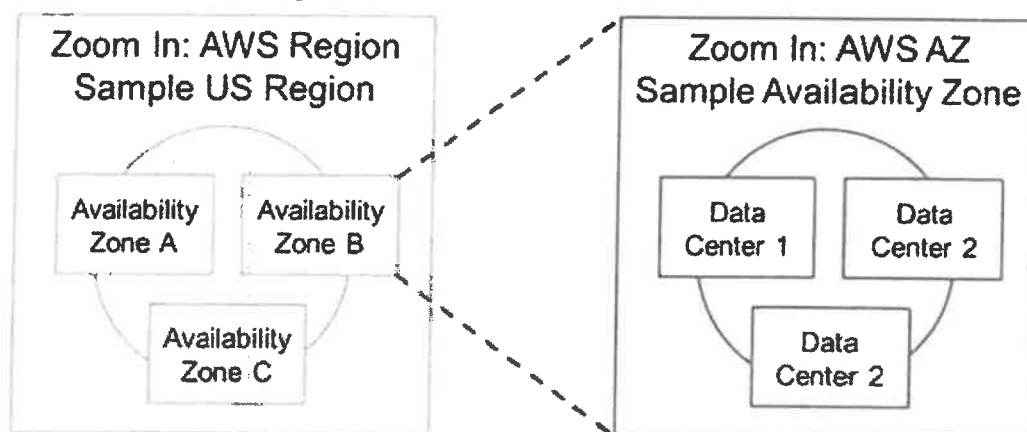
As system and product companies leveraging cloud-based architecture on FedRAMP-certified AWS GovCloud (GovCloud), we are well-equipped to manage sensitive data and regulated workloads. Our commitment to meeting stringent U.S. government security and compliance standards underpins our robust disaster recovery and business continuity plans.

### Proposed Approach to Disaster Recovery and Business Continuity:

To ensure business continuity and minimize downtime, a robust disaster recovery (DR) strategy is followed while implementing the solution. This involves regularly scheduled backups of critical data, replication of systems to a secondary site, and periodic DR drills to validate the recovery processes. The DR plan includes procedures for restoring system functionality in the event of natural disasters, hardware failures, or other disruptive events.

This cloud-hosted SaaS solution does not require any external hardware or infrastructure for Disaster Recovery or Business Continuity. Backups are maintained automatically as part of cloud data storage with multiple copies of all data being stored in multiple servers, data centers, and different geographical locations, based on how the cloud service provider is configured. This high level of redundancy helps prevent any loss in the performance of the application and accounts for the high availability of the system with virtually no possibility of data loss.

Our AWS cloud solution enables us to deliver a broad suite of services in support of WV DHS. As depicted in **Figure 28**, AWS ensures redundancy and fault tolerance via availability zones (AZs) – distinct data centers within an AWS region, each featuring redundant power, networking, and connectivity.



**Figure 28: AWS Availability Zones**

When a major disaster occurs at the primary site, we can restore services quickly through the AWS cloud solution. We follow a proven methodology that incorporates best practices and global industry standards from the Information Technology Infrastructure Library (ITIL). By adhering to a system backup schedule, storing geo-redundant copies of data backup, and having prepared staff members and

comprehensive plans, we ensure that the State has complete solution recovery capabilities in the event of any unforeseen circumstances.

To validate the effectiveness of our contingency and disaster recovery plans, we conduct rigorous testing at least twice annually. These tests allow us to identify any necessary modifications to the plan(s) and ensure minimal interruption to service during implementation. Our team works closely with the State to coordinate testing activities, prioritizing limited system downtime.

Furthermore, we conduct an annual backup restore test, including backup media restoration and failover/fallback operations at the designated disaster recovery (DR) location. This test ensures the reliability and successful restoration of data and services in a simulated DR scenario.

By adhering to these robust contingency and disaster recovery measures, we aim to provide continuous service availability, safeguard critical data, and minimize any potential impact of disruptions on operations. Our system incorporates the following preventative controls and recovery strategies:

- **High Availability:** We leverage Elastic Load Balancer (ELB) to increase system availability. Cloud EC2 Instances that fail are seamlessly replaced by leveraging AWS Auto Scaling behind the load balancer. We use State-approved AWS GovCloud Availability Zones (AZs), which are distinct geographical locations engineered to be insulated from failures in other AZs. We will host Amazon EC2 instances in multiple AZs, so the application is protected from failure of a single location.
- **Highly available, durable data Storage:** We will leverage AWS storage solutions that deliver highly scalable, durable, and reliable cloud storage for backup, and support mission-critical databases. Amazon S3 will be used to store database backups. It offers flexibility, agility, geo-redundancy, and robust data protection.
- **Host level issues and disk failures:** We will leverage EBS volumes which will be attached to EC2 and are automatically replicated within a single availability zone. To increase durability further, point-in-time snapshots would be created to store data on volumes in Amazon S3, which would be then replicated to multiple AZs.
- **Point-in-time database recovery:** We will leverage the Amazon RDS automated backup feature, which keeps automated backups for a configurable number of days (called the backup retention period). The database backup can be used to restore the database instance to any specific time during this retention period.
- **Recovery Objectives (RTO and RPO):** Cardinality.ai ensures compliance with stringent Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Leveraging AWS's high availability zones and Geo-redundant Storage (GRS), we ensure that data is consistently replicated across regions to provide seamless failover capabilities. Our **RTO targets a recovery within four hours**, while our **RPO guarantees no more than one hour of data loss**. Continuous replication using AWS Site Recovery keeps the warm standby environment up to date with the production environment.

**Business continuity:** Disruptions, whether they arise from facility closures, staffing challenges, weather anomalies, natural calamities, supply deficits, technical glitches, utility failures, or any other unforeseen

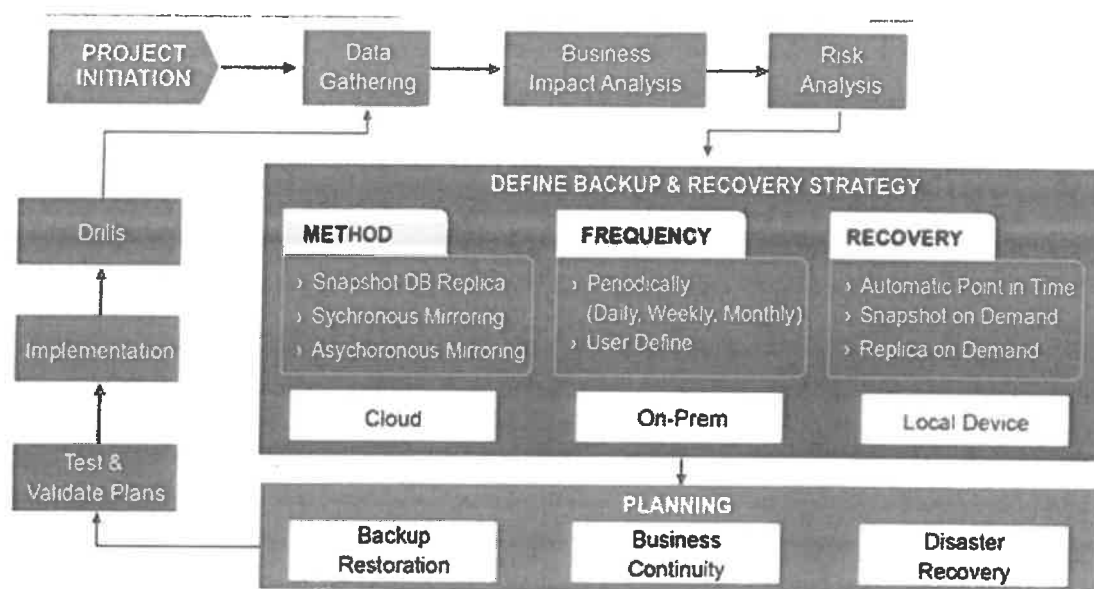


circumstances, can have profound implications on the system's operations. To address this, our comprehensive Business Continuity Plan (BCP) is meticulously crafted to navigate these challenges, ensuring the system's robustness and adaptability.

Our BCP will not only identify the essential business functions that are paramount for continuity but will also conduct a thorough Business Impact Analysis. This analysis will assess the potential ramifications of various disruptions, thereby aiding in the prioritization of recovery strategies. A hallmark of our plan is the clear delineation of roles and responsibilities, ensuring that in times of crisis, every team and individual knows their duty, eliminating confusion and expediting response times. Communication, we believe, is a key differentiator in such scenarios. Our structured communication protocols will ensure timely and accurate information dissemination to all stakeholders, fostering transparency and trust.

We understand the importance of reliable back-up environments from a Business Continuity perspective. Our cutting-edge cloud tools allow creating back-ups that will minimize operational impacts during recovery. The detailed plan for data loss prevention, back-ups, recovery procedures, and planned DR testing will be documented and delivered in the Disaster Recovery and Business Continuity Plan.

Our approach to planning and managing back-ups is shown in **Figure 29** below. We will work closely with the WV DHS team to finalize the detailed plans in alignment with the Division, Department, and State's Disaster Recovery and Business Continuity Plans.



**Figure 29. Backup Management Lifecycle**

**Business Impact Analysis and Risk Assessment:** We identify the most important business functions and the IT systems and assets that will require support for disaster recovery and business continuity. Next will be the risk assessment to examine the internal and external threats and vulnerabilities that could negatively impact IT assets.

**Defining Backup Strategy:** Our backup strategy is developed based on the insights obtained through data gathering, Business Impact Analysis (BIA), and Risk Assessment. It is closely aligned with our Disaster Recovery strategy, which will be further elaborated on in this section. Our approach encompasses the following best practices:

- **SNAPSHOT-based protection:** We have pre-defined backup subroutines for AWS. As per this method, a copy of the data volume will be taken and placed in the project cloud instance, ensuring redundancy across multiple availability zones. The first snapshot will be typically a full copy of the volume, whereas ongoing snapshots will be incremental data-block changes. Additionally, snapshot backups can also be augmented with flat backups, where snapshot copies will move to low-cost storage.
- **Database Replica Backups:** For backing up the database, a method of creating the read-only replica will be followed. Such replicated databases are typically a real-time copy of the database that runs on other servers.
- **Synchronous mirroring:** We may consider synchronous mirroring, where data is written to parallel disks simultaneously, which can be preferred for low input/output situations.
- **Using scheduler services for auto backups:** This method will be used to take backup of the files from devices (desktops, laptops, tablets, and mobile) and any on-premises application servers

**Recovery:** Replication with Failover and Switchback will be implemented to facilitate transition of responsibilities between primary and standby servers, ensuring a high level of system availability. Point-in-time recovery (PITR) will be utilized whenever necessary to restore the database to a specific state from a previous point in time. By employing non-disruptive continuous archival, the restored environment will closely align with the most recent version of available data. To create additional servers for testing or development purposes, restore utilities will be employed using Dumps and Cold backups, thus providing the required flexibility and versatility.

**Planning, Testing, and Implementation:** We will develop the Disaster Recovery and Business Continuity Plan that will ensure the timely restoration of systems for users. To implement the backup procedures, necessary modifications will be made across various systems, and thorough validations will be conducted to ensure the backup meets the expected requirements.

**Drills:** We will periodically perform backup recovery drills to ensure all backup and recovery processes are working. Drills create awareness within the team for ease of execution and effectiveness during an actual event. We use lessons learned from drills to make appropriate changes to processes.

### **Business Continuity Implementation**

The BCP team at Cardinality is identified at three different levels within the organization and are designated to the respective roles in the event of a disaster with regular training and re-grouping to discuss best practices and implementation plans.

**Level 1** - Senior Management Resource - Leader or Project Manager of the BCP Operation - 1 or more

**Level 2** - Manager and or Customer or Client Representative- 3 or more - responsible for the execution of the plan during the disaster and the one who directs employees in the event

**Level 3** - A frontline employee engaged in the day-to-day operations and works on the directions of the manager during the event.

**Backup and Restoration:** Cardinality uses the following general guidelines and procedures for backup and recovery. Each process is also guided by unique backup and restore plans and procedures based on the specifics of the activity involved:

**Back-up of Data**

- Server backups will be performed every business night, excluding holidays.
- Backups performed on Friday will be kept for a month before recycling.
- The last backup of every month will be considered the monthly backup and kept for a year before recycling.
- Backups will be automated using state-agreed software products/AWS.
- Backups will always be performed before upgrading or modifying a server.

**Disaster Recovery Testing:** Cardinality follows intensive disaster recovery testing methodologies with a detailed Discovery Plan Review to find inconsistencies and missing elements; Tabletop exercises that go through the process step-by-step and educate on gaps and Simulation Scenarios to see if the disaster recovery procedures and resources, including backup systems and recovery sites allocated for disaster recovery and business continuity work. The simulation involves running a variety of disaster scenarios to see if the teams involved in the DR process can restart technologies and business operations quickly and effectively. We also include a Disaster Recovery Checklist to establish what is tested and what is not:

- Identify goals, objectives, and procedures to create a post-testing analysis. Create a test team, including SMEs and make sure everyone is available for the planned testing date.
- Carefully document and be prepared to edit your DR plan and disaster recovery testing scripts.
- Include all relevant technology elements and processes being tested in the plan.
- Ensure the test environment is ready and won't affect production systems or conflict with other activities.
- If testing is going to take a significant amount of time, schedule it far in advance.
- Perform a practice exercise before the disaster recovery test goes live to uncover and fix potential problems.
- Stop and review the test when issues arise and reschedule if necessary.
- Keep comprehensive records of start and end times, what occurred, what worked and what didn't.
- Update disaster recovery and business continuity plans and other documents based on what's been learned from the DR test.

## 9. Response to Qualifications and Experience (§ 4.3)

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives were and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

### 9.1 Qualification & Experience Information (§ 4.3.1)

**Business:** Vendor should briefly describe the company's core business, background, and experience in providing IT solutions to government health and human services agencies. (RFP Section 4.3.1.2)

#### Cardinality.ai

Cardinality.ai is the modernization alternative that innovative states are using to better serve citizens. Over 5000 caseworkers across 10 government agencies, 6 states, 13 nonprofits, and healthcare providers are already using Cardinality's pre-built solutions. Cardinality is a SaaS company, founded in 2017, helping government agencies achieve better outcomes through artificial intelligence and the strategic use of data.

Our solutions, engineered for health and human services programs, deliver enhanced efficiency and improve the lives of citizens. Together with our agency customers, we achieve remarkable outcomes for families. Our built-for-government suite of case management solutions employs configurable functional modules, cloud-based tech, powerful AI assistant, an intuitive interface, and data-driven workflows on a low-code platform that enables agencies to modernize faster and with greater confidence than custom development projects. With 10M+ Americans already benefiting from its applications, we are well on our way to changing a billion lives.

Cardinality's suite of AI SaaS solutions and low code **Empower Platform** enables all stakeholders to achieve more with better, faster, and more affordability. At Cardinality, we are dedicated to delivering data technology solutions that enable governments to achieve better outcomes. Central to our operations is a committed team of over 200 professionals and subcontractors. This dedicated workforce is essential to our ability to innovate and deliver impactful solutions that improve public services and governance.

**Our Core at a Glance:** Cardinality's primary objective is to make modern technology solutions accessible to government agencies without the difficulties of prolonged implementation times or failed custom applications. By doing so, Cardinality hopes to empower stakeholders, including elected officials, policy leaders, government workers, constituents, and families, to achieve more while spending less. Cardinality's solutions have already been implemented by multiple government agencies, making a difference in the lives of millions of Americans across state and local governments.

Our current offerings encompass diverse products and services designed to meet our clients' varied needs. The figure below illustrates our comprehensive portfolio, highlighting the main categories of our

offerings, the key features of each product and service, and how they interconnect to provide holistic solutions. Each segment of the infographic is meticulously crafted to highlight the breadth and depth of our capabilities, verifying that our clients can easily identify solutions that align with their specific requirements.

### Cardinality Offerings: Pre-built Solutions



**Figure XX: Our offerings**

### Cardinality's experience:

Cardinality has successfully completed numerous projects of comparable scale and magnitude. We would like to call out some of our key projects of similar size and scope to demonstrate our capabilities in managing this project.

#### • Georgia Department of Human Services (GA DHS) - Cardinality.ai

In June 2023, GA DHS partnered with Cardinality for the configuration, implementation, and support of a modern Foster Care System that includes an communication module to foster communication and collaboration among stakeholders, intuitive and easy-to-use Self-Serve Portal for recruiting and onboarding foster parents and engaging with CASA volunteers, a modern and AI-enabled CMS for license managers to process applications and manage providers, as well as smooth and secured integration with CCWIS systems for timely information sharing.

Georgia Communicare is a set of interconnected web portals and mobile app specifically designed to enable enhanced and streamlined communication and data access between DHS case managers and external parties (CASA Volunteer, Biological Parents, and Foster Parents) to a foster care case ( Refer link: <https://dfcs.georgia.gov/services/georgia-communicare>).

Because of our pre-built WV-MACS solution and the innovative gap-based implementation methodology, phase 1 was implemented in a record time of three months, with phase 2 and mobile app rolled out state-wide in the next 5 months. As of September 2024, over 7,500 external users—including CASA volunteers, foster parents, and biological parents—along with more than 3,000 Georgia DHS caseworkers, have been onboarded. They are now equipped to enhance the well-being and safety of children through real-time digital communication and information sharing.

Cardinality's configurable low-code platform with multiple functional modules providing capabilities around workflows, assessments, analytics, RBAC, APIs, etc. is being leveraged to build the Foster Care Provider Management Solution, hosted on AWS. Phase 1 and Phase 2 went live with the Self-Serve Portal for multiple personas and are being actively used by more than 4000 internal and external users, including Foster Parents, Biological Parents, and Agency Staff.

- **Modernized Maryland's CJAMS System**

Cardinality's configurable low-code platform with multiple functional modules providing capabilities around workflows, assessments, analytics, APIs, etc. was leveraged to build a modern, intuitive, and mobile-friendly Child, Juvenile & Adult Management System (CJAMS), components of which were also leveraged by other applications that were being modernized.

Cardinality implemented a new fully CCWIS-compliant system providing comprehensive case management capabilities, integrated Title IV-E eligibility determination, and integrated financial management and provider management capabilities. The Cardinality system supports all major processes and programs, including Intake, Investigation, Child Protective Services, In-Home Services, Out-of-Home Services, Foster Care, Permanency services (Reunification, Adoption, and Guardianship), and Independent Living Services.

Verifiable outcomes intended and achieved: Since going live in 2020, CJAMS has equipped Child Welfare caseworkers to become more efficient and improve outcomes for vulnerable children.

- 70% reduction in cases with recurrence of maltreatment for children.
- 25% decrease in removal of child from home per 1,000 children, even though an overall increase in the number of cases reported.
- 22% reduction in re-entry in the foster care system after reunification with the family of origin.
- Baseline solution and platform met 88% of CCWIS requirements and over 70% of State child welfare requirements.
- 300+ screens, multiple workflows, and integrations with over 18 inter/intra-agency systems across child, adult, and juvenile welfare domains.
- Used by approximately 5,000 caseworkers, supporting six million citizens.
- Smooth migration of close to 12 million records from various entities, including MD DHS and the Maryland Department of Health (MDH).

The CJAMS serves the State of Maryland, a densely populated state with approximately 1.3 million children and around over 6,000 child maltreatment cases reported annually. The platform was deployed across Maryland in four phases, beginning with a pilot covering 5% of the caseload and gradually expanding to other counties. The pilot phase was completed within 19 months, with statewide deployment achieved in 27 months. Additionally, the base platform continues to receive biannual upgrades to maintain its alignment with evolving requirements and operational excellence.

- **Indiana Department of Child Services - Comprehensive Child Welfare Information System (CCWIS):**

Cardinality is responsible for configuring and implementing the Eligibility and Finance modules. Cardinality's solution is based on a multi-cloud strategy where most of the user engagement-rich

modules are developed in Salesforce and process-intensive modules are developed and hosted on AWS. This new system will help IN DCS to improve its ability to provide services; enable staff to drastically reduce administrative workload and focus on field activity to drive measurable outcomes for child welfare; and assist agency leadership in their effort to achieve the safety, permanency, and wellbeing of children and families in their care. The system supports all major processes and programs such as Family Preservation, Foster Care, Adoption, Guardianship, Collaborative Care, and Medicaid.

The scope of the Pilot and Phase 1 of this Child Welfare project focuses on Eligibility, including foster care, collaborative care, guardianship, Medicaid, adoptions, and family preservation. Phase 2 of the project will cover all the financial processes needed for child welfare case management, including Medicaid cases involving Social Security Income (SSI) benefits. Eligibility is currently in the UAT phase, and the configuration of the Finance module is yet to begin.

Post implementation, the system will be used by around 7000 internal users and 3000 external users. In its end state, the system will be hosted on AWS and have approximately 130 screens and about 45 workflows specific to Financial and Eligibility modules.

Once implemented, the solution will serve the state of Indiana, which handles over 20,000 child maltreatment cases annually. Indiana focuses on scaling services to effectively cover both its urban and rural populations, enabling comprehensive support for children and families across the state.

### **Cyquent.inc (Subcontractor for this Project)**

Cyquent, established in 2001, has been at the forefront of technology transformation and digital innovation, delivering solutions that meet the complex demands of modern case management systems.

With 24 years of proven experience in supporting our government clients, Cyquent excels in providing a comprehensive range of IT enterprise services. These services include Application Development, COTS Implementations, Digital Transformation, Application Modernization, Systems and Data Integration, Operations and Maintenance, PMO, and full SDLC support for both commercial and public-sector clients. Our expertise extends to designing and developing scalable software, web portals, web applications, and mobile apps, which are instrumental in transforming our clients' organizations and enhancing their operational efficiency.

Cyquent's first prime contract in 2011 was the migration of Arlington County legacy case management (CASE) and purchase order system (POS). These legacy systems were built on the county mainframe and had to be converted from the IBM mainframe server to a web-based Microsoft platform system. The data from the legacy systems had to be converted and migrated to the new systems. The system interfaces with other County systems also had to be built on the new Microsoft platform. Cyquent successfully transformed and delivered the case management system within an aggressive timeline of one year. Cyquent provided the complete lifecycle of implementation and migration. The existing business processes and requirements were analyzed; the project management plan for the entire engagement was created, including project schedule, configuration management, change management, risk management, and communications plan. Tasks, intermediate milestones, and deliverables were built into the project schedule. The entire implementation lifecycle was carefully managed throughout all phases of the engagement, including requirements analysis, design and architecture phase, coding and testing phase, systems and acceptance testing phase, and finally, the

"go live" phase. The deliverables included the new web-based system, completed data conversion of all data from the mainframe to SQL Server, and conversion of all system interfaces and reports.

Some of Cyquent's public sector clients in the United States are listed below:

- Arlington County, Virginia
- Food and Drug Administration
- General Services Administration
- Harford County, Maryland
- Library of Congress
- Maryland Department of Health
- Maryland Department of Human Services
- Maryland Department of Information Technology
- Maryland Healthcare Commission
- Montgomery County, Maryland
- National Institutes of Health
- New York City
- New York State Department of Health and Human Services
- Pennsylvania Department of Transportation
- Pennsylvania Department of Human Services
- Social Services Administration
- US Copyright Office
- Virginia Information Technologies Agency
- Virginia State Corporation Commission

Cyquent's commercial clients include Discovery, Deloitte, Fannie Mae, Freddie Mac, National Football League (NFL), Verisign, Verizon, Leidos, ServicePower, Carefirst BlueCross BlueShield, OSSM Inc., Miller Zell, MobiSaaS, Trusted QA, Principal Financial Group, Cognizant, American Story Channel, BIRetail, CGI, ContextWeb, Healable, RaceTrac, and Vinculum Group, among others.

Team Cyquent brings decades of expertise and innovation to deliver comprehensive IT and digital modernization solutions tailored to the evolving needs of clients. Our extensive experience and proven capabilities in case management systems make us the ideal partner for innovative and reliable solutions. Our key strengths that we bring to this engagement:

- **Proven Expertise in Health and Human Services Platforms**

Cyquent's notable projects include the Maryland Total Human Services Integrated Network (MD THINK) and Montgomery County's Enterprise Integrated Case Management (eICM) System. These systems streamline service delivery, foster cross-agency data sharing, and enhance client outcomes by leveraging advanced technologies like cloud platforms, AI/ML models, and shared data repositories

- **Agile Methodologies and Human-Centered Design**

Cyquent employs Agile development frameworks and iterative processes to ensure flexibility, stakeholder collaboration, and timely delivery. The use of user research methods such as journey mapping, focus groups, and prototyping ensures that solutions are intuitive and meet the needs of



diverse users. This aligns with the RFP's emphasis on user-friendly, scalable platforms that integrate with existing systems while maintaining HIPAA compliance

- **Advanced Technology and Data Capabilities**

Cyquent excels in integrating AI and machine learning for operational efficiencies. This includes automated eligibility determination, fraud detection, and predictive analytics to optimize resource allocation and service delivery. The proposed system will support ad hoc reporting, data visualization, and real-time analytics, addressing the RFP's requirements for robust data management and reporting

- **Comprehensive Project Management and Support**

Cyquent's structured project management approach ensures successful execution, from requirements gathering to deployment. The company prioritizes change management, risk mitigation, and continuous quality assurance to deliver reliable solutions. Additionally, Cyquent provides 24/7 support, detailed training, and a seamless transition plan post-implementation to ensure ongoing success and user satisfaction.

- **Commitment to Security and Compliance**

Cyquent ensures adherence to strict security standards, including HIPAA and the 21st Century Cures Act, with features like role-based access, audit trails, and data encryption. This commitment ensures that sensitive information remains protected across platforms and workflows, meeting the RFP's stringent security and compliance requirements.

Team Cyquent, composed of Cyquent and Cardinality, brings unparalleled expertise in IT services and digital modernization, delivering innovative and scalable case management solutions for government agencies across the United States. With decades of experience in modernizing human services systems, our human-centered technology solutions enhance efficiency, improve service delivery, and ensure better outcomes for clients. Some noteworthy and relevant examples of Team Cyquent's current and past experience within last 5 years include:

Project	Description
<b>Maryland Department of Human Services, Maryland Total Human Services Integrated Network (MD THINK)</b>  <b>(May 2018 – May 2025)</b>	Developed unified, modular care and case management systems that integrate services across multiple programs, including SNAP, TANF, Medicaid, and Child Welfare. These solutions align closely with Orange County's requirements for a multi-program system designed to address the diverse needs of populations such as prenatal and postpartum clients, older adults, and high-risk groups. By leveraging robust system design principles, Cyquent creates platforms that streamline service delivery across complex programs

<b>Montgomery County Department of Health and Human Services, Enterprise Integrated Case Management (eICM) System – Operations and Maintenance</b>  <b>(Sep 2021 – May 2026)</b>	<p>Enterprise Integrated Case Management (eICM) System operations and maintenance (O&amp;M) contract for the legacy eICM system to meet DHHS' mission objectives, which include administering, delivering, and implementing 134 Federal, State, and County programs. We Agile/DevOps, O &amp; M, and enhancement services supporting efficient service delivery for State and County administered citizen services.</p>
<b>Montgomery County Department of Health and Human Services, Enterprise Integrated Case Management (eICM) System - Modernization</b>  <b>(May 2023 – May 2026)</b>	<p>Designed and implemented unified case management systems, such as the eICM system for Montgomery County's Department of Health and Human Services (DHHS), integrating over 70 programs into a single, modernized platform. This system supports coordinated care and consolidated access to services, aligning closely with Orange County's need for an integrated care and case management system. By addressing the unique requirements of a wide range of services, eICM effectively delivers a centralized solution that promotes efficiency and accessibility for diverse programs.</p>
<b>Medicaid Enterprise Systems Modular Transformation (MMT), Maryland Department of Health (MDH)</b>  <b>(Sep 2021 – Aug 2026)</b>	<p>Implemented and maintained a number of modernization initiatives. This includes enterprise-wide technology solutions that are shared between multiple systems, such as Enterprise Integration Services, Enterprise Electronic Document Management, and Enterprise Data Warehouse / Decision Support System. The individual modules (applications) that are being developed use these shared enterprise-wide technology solutions.</p>
<b>Maryland Department of Health, Maryland Primary Care Program (MDPCP)</b>  <b>(May 2019 – Dec 2019)</b>	<p>Provided support, optimization, and resources to ensure that the Participants' Health Information Technology (HIT) and Electronic Health Record (EHR) systems are compliant with the program and reporting needs of MDPCP and have the necessary skills and technology to enable the data capture, transfer and reporting needs of the program.</p>

**Corporate Identity:** Vendor should provide the identity of any parent corporation, including address, phone and fax numbers, federal employer identification number (FEIN) or tax ID number, company website, and contact email. Provide the identity of any subsidiaries, as applicable. (RFP Section 4.3.1.2)

**Response:**

**Cardinality.ai**

Item	Detail
Company Name:	Elixir Lab USA Inc (d/b/a Cardinality.ai)
Type of Entity (Legal Status):	Corporation
Physical Address	267, Kentlands Boulevard, Suite #5092, Gaithersburg, Maryland (MD), 20878
Contact person and Designation	Anna Harper, Chief Administrative Officer
Phone	(513) 907-1068
FEIN	82-2663839
Business Website:	<a href="http://www.cardyai.com">www.cardyai.com</a>
Email Address	<a href="mailto:sales@cardyai.com">sales@cardyai.com</a>

**Exhibit 4: Cardinality's Profile**

**Cyqunet.inc:**

Cyquent Inc, which is a certified Minority Business Enterprise (MBE), will be partnering with us in implementing the WV-MACS solution. Please find the profile of Cyquent Inc below:

Item	Detail
Company Name:	Cyquent Inc
Type of Entity (Legal Status):	Corporation
Physical Address	155 Gibbs St., Suite 531, Rockville, MD 20850
Contact person and Designation	Brian Zernhelt, VP Business Development
Phone	443-690-0880
FEIN	51-0406912
Business Website:	<a href="https://cyquent.com/">https://cyquent.com/</a>
Email Address	<a href="mailto:Brian.Zernhelt@Cyquent.com">Brian.Zernhelt@Cyquent.com</a>

**Exhibit 5: Cyquent's profile**



## Business Units and Functional Relationships

1. **Product and Engineering Team:** This team is responsible for the development, enhancement, security & compliance, and innovation of Cardinality's software solutions, including the WV-MACS solution. The team works closely with the customer-facing ("Operations & Support team") to incorporate client feedback and verify that our solutions meet the latest technological standards and client requirements. Verifies that all products and services meet regulatory standards and quality benchmarks. This team conducts regular audits, manual and automated testing of solutions, and validation processes to maintain high standards of quality and compliance.

**Operational Relationship:** Collaborates with the Operations & Support teams to verify the product is well-suited to meet West Virginia DHS's needs and requirements. Engages in continuous improvement based on user feedback and emerging industry trends. Verifies that the WV-MACS solution complies with all relevant federal and state regulations and that West Virginia DHS data is handled securely and efficiently.

2. **Operations & Support Team:** This team manages the deployment and integration of Cardinality's solutions within client environments. This team includes project managers, system integrators, and technical specialists who oversee the end-to-end implementation process. They verify that our solutions integrate smoothly with clients' existing systems and workflows. This team provides ongoing support and training to clients' post-implementation. The support team assists with troubleshooting, system updates, and user training. They offer a help desk service and verify that clients maximize the benefits of our solutions.

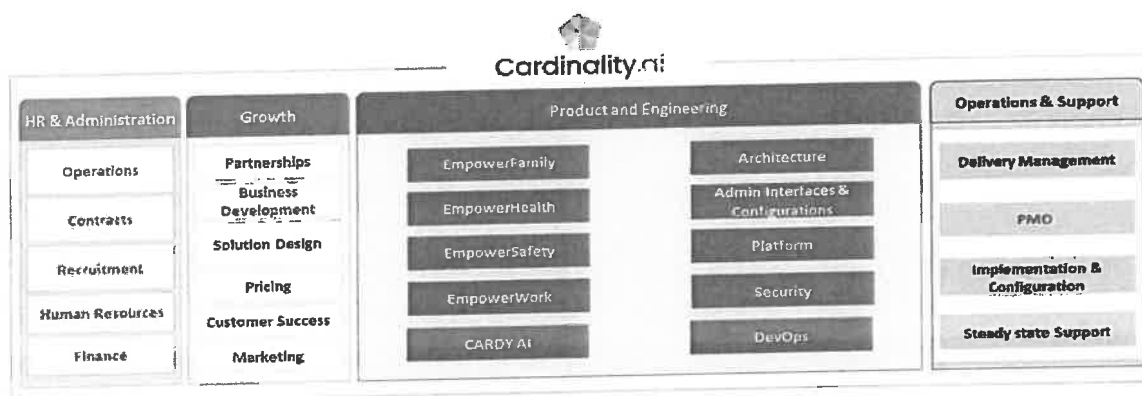
**Operational Relationship:** Works directly with West Virginia stakeholders to tailor the WV-MACS solution to their specific requirements, managing a smooth and timely implementation process. Acts as the primary point of contact for the WV-MACS solution post-implementation, verifying that any issues are promptly addressed and that users are fully trained and supported.

3. **Growth Team:** Manages client relationships, partner engagement, business development, solution design, pricing, and marketing efforts. This team focuses on understanding client needs, presenting tailored solutions, and maintaining ongoing client and partner engagement. For this proposal, we have partnered with **Cyquent Inc.**

**Operational Relationship:** Engages with West Virginia DHS to understand their needs and verifies that our proposals align with their strategic goals. Provides detailed product demonstrations, organizational strengths, and capabilities, and gathers client feedback for continuous improvement.

4. **Human Resources and Administration:** Manages recruitment, employee development, and training programs. This team focuses on building a skilled workforce and providing continuous professional development opportunities.

**Operational Relationship:** Verifies that our team members working with West Virginia DHS are highly skilled and up to date with the latest industry standards and best practices.



**Figure 31: Organizational structure**

### How Team Cardinality Meets West Virginia DHS Needs and Requirements?

- Alignment with Strategic Goals:** Our organizational structure verifies that every team works towards West Virginia DHS strategic goals, with clear communication channels and collaborative efforts across departments.
- Efficient Implementation, Ongoing Support, and Adaptability:** The "Operations & Support" team promotes a smooth and efficient deployment of the WV-MACS solution, tailored to meet the specific needs of West Virginia DHS, minimizing disruption, and maximizing efficiency. They verify that West Virginia DHS receives continuous support, that all issues are resolved promptly, and that users are fully trained.
- Regulatory Compliance and Quality Assurance:** The **Product & Engineering** team verifies that all aspects of the WV-MACS solution adhere to federal and state regulations, providing a secure and reliable solution. They continually enhance our solutions based on client feedback and industry trends, verifying that West Virginia DHS benefits from the latest technological advancements.

By leveraging our comprehensive and client-focused organizational structure, Cardinality is well-positioned to meet the requirements of West Virginia DHS, delivering a high-quality, efficient, and compliant workforce development solution.

### Cyquent Inc

Our Partner Cyquent's organizational structure highlights a clear delineation between strategic leadership provided by the executive team and the operational management carried out by the management team. Each individual in the management team plays a crucial role in their specific area, contributing to the overall success and efficiency of the company.

The organizational chart provided depicts the structure of the management and executive teams of a company. Here's a breakdown of the roles and the hierarchy as presented in the chart:

## Executive Team

**Sagar Sawant - Founder and CEO:** As the Chief Executive Officer and founder, Sagar Sawant holds the top position within the company, responsible for setting the strategic direction and overall management.

**Priya Tejwani - Chief Operating Officer (COO):** The COO manages the day-to-day administrative and operational functions of the company, reporting directly to the CEO.

**Niraj Jagasia - Chief Growth Officer (CGO):** The CGO is responsible for driving business growth through marketing, sales, and business development strategies.

## Management Team

Below the executive team, the management team includes various senior roles, each overseeing specific functional areas within the company:

**Brian Zernhelt - Vice President, Account Management:** He is responsible for maintaining and growing the company's relationships with its key accounts.

**Shashank Davanagere - Senior Director, Technology:** This role would involve overseeing the company's technology strategy and implementation, including software development and IT infrastructure.

**Prachi Shah - Director, Accounts and Billing:** Prachi Shah manages the company's financial accounts and the billing process, ensuring that finances are handled efficiently and transparently.

**Kaksha Merchant - Senior Director, Delivery:** Responsible for the delivery of services or products to clients, ensuring that projects are completed on time, within budget, and to the satisfaction of clients.

**Subhash Shirole - Director, Talent Acquisition:** This role focuses on recruiting talent, managing hiring processes, and developing strategies to attract skilled employees.

**Tamara Wilhite - Director, Human Resources:** Tamara handles internal HR responsibilities, including workforce development, employee relations, and compliance with labor laws.

Figure 32 illustrates Cyquent's Organization Chart



**Figure 32: Company Organizational Chart**

**Locations:** Vendors should describe the geographical locations of their firm at the national, regional, and local levels, as applicable. Identify all locations that will be used to support a resultant contract and the operations managed from these locations. Clearly identify any overseas locations which may be used to support the resultant contract. No State data may be stored on servers or systems outside of the United States of America (U.S.), including U.S. Territories.

Cardinality is strategically positioned to support contracts at the national, regional, and local levels through our office locations in the United States, supplemented by our offshore development center. The below table is an overview of our geographical presence and how each location contributes to the support and execution of contracts:

S No	Office	Address	Operations Handled
1	Headquarters	267, Kentlands Boulevard, Suite #5092, Gaithersburg, MD 20878	Project Management, Client Services, Administration
2	Regional Office 1	Pike & Rose, 909 Rose Avenue, North Bethesda, MD 20852	Sales and Marketing, Customer Support
3	Regional Office 2	1650 Tysons Boulevard, Suite #1530, McLean, VA 22101	Consulting Services, Business Development



4	Regional Office 3	7345, 164th Ave NE, Ste 145 #187, Redmond, WA 98052	Research and Development (R&D), Technical Support
5	Offshore Development Center	Chennai, India	Supports our SDLC particularly in the early stages of development & testing and software engineering.

**Exhibit 6: Office locations within USA & India****Sub-contractor - Cyquent**

S No	Office	Address	Operations Handled
1	Headquarters	155 Gibbs St., Suite 531 Rockville, MD 20850	Data Analytics and Artificial Intelligence, App Development, Agile Consulting and Staff Augmentation

**Exhibit 7: Cyquent's Office location**

All state data will be stored on servers or systems inside the United States of America (U.S.), including U.S. Territories.

**References:** The Vendor should provide three (3) references from system implementation projects or systems in operation within the last five (5) years that demonstrate the Vendor's ability to achieve the goals and objectives in Section 4.2 and meet the requirements in the RFP.

Vendors may provide only one (1) reference per project performed and should include details about the Project such as project goals and objectives, general functionality, implementation timeline, and length of time the system has been in operation if applicable. The State strongly prefers three (3) references from different state engagements where a Child Welfare client communications system is currently being or has been implemented and is in operation.

**Cardinality's Reference**

Reference 1	Detail
Reference Company Name:	Department of Human Services (DHS), Georgia (GA)
Company Address:	47 Trinity Ave. S.W. Atlanta, Georgia (GA) 30334

Type of Industry:	Government
Contact Name:	Sriram Subramaniam
Contact Phone Number:	404-788-1144
Contact Email Address:	<a href="mailto:Sriram.Subramaniam@dhs.ga.gov">Sriram.Subramaniam@dhs.ga.gov</a>
Description of system(s) implemented:	<p><b>Project Name:</b> Georgia Foster care - Communicare</p> <p><b>Scope of Work:</b> The Georgia Division of Family and Children Services (DFCS) is developing a new portal and Foster Care Management System to improve communication among CASA volunteers, foster and biological parents, and DFCS staff. This initiative aims to streamline processes, reduce delays, and missed appointments, and enhance advocacy for children in foster care. The new system will be adaptable and easy to update, aligning with changing policies and regulations. This project represents DFCS's commitment to better support children in foster care by improving coordination and information sharing among all involved parties.</p> <p><b>Cardinality's Involvement:</b> Cardinality is configuring and deploying its pre-built, fully-featured, and modern EmpowerFamily Child Welfare Foster Care System. The EFCW solution includes a comprehensive out-of-the-box Foster Care Management System and Self-Serve Portal. It is designed to meet the needs of different personas, such as CASA volunteers, biological parents, foster care providers, special attorney generals, and others. EFCW provides each user with necessary information and participation capabilities. User experience, feature availability, and data access are efficiently managed through Role-Based Access Control.</p> <p>The intended benefits are listed below:</p> <ul style="list-style-type: none"> <li>● <b>Improved Communication</b> - The portal will improve communication between CASA volunteers, case managers, and supervisors. It provides CASA volunteers with the contact information of newly-assigned case managers and enables secure and efficient communication through nudges and chat features, improving communication, speed, and quality.</li> <li>● <b>Reduced workload for case managers</b> - The portal automates administrative tasks for the CASA program, reducing case managers' workload. Volunteers can submit reports online, eliminating the need for paper reports, and freeing up case managers' time for higher-priority tasks.</li> <li>● <b>Modular Modernization</b> - The CASA Volunteer Portal is a key component of the Foster Care Solution, improving communication between volunteers, parents, and DFCS. Its incremental development allows for the quick release of essential features while continuing to refine the module.</li> </ul>

	<ul style="list-style-type: none"> <li>● <b>Increased real-time access to critical information</b> - The portal offers real-time access to case records for all parties, empowering CASA volunteers to make informed decisions regarding the welfare of their assigned foster children without delays.</li> <li>● <b>Child Welfare Centric</b> - Empowering volunteers with comprehensive data, targeting holistic child welfare and rapid issue resolution.</li> </ul>
Date of Implementation:	<p>June 2023 - Ongoing</p> <ul style="list-style-type: none"> <li>● <b>Phase 1 (Sept 2023, Go-live)</b> - Integrated portal for Foster, Biological parents, and CASA volunteers to provide a child's continuum of care. Streamlined access to critical case information like medical/health, education, and placement information.</li> <li>● <b>Phase 2 (December 2023, Go-live)</b> - Introduced Mobile App along with enhanced features for secondary case managers, SMS-based multi-factor authentication, multi-lingual support, and improved case search</li> <li>● <b>Phase 3 (Planned Go-live, Sept 2024)</b> - Foster Parent Onboarding Portal (Planned Go-live by July 2024), CPA FP Onboarding &amp; FP Invoicing</li> </ul>

Exhibit 8: Reference 1 - GA Foster care: Communicare (DHS)

Reference 2	Detail
Reference Company Name:	Department of Human Services (DHS), Georgia (GA)
Company Address:	47 Trinity Ave. S.W. Atlanta, Georgia (GA) 30334
Type of Industry:	Government
Contact Name:	Sreeji Vijayan
Contact Phone Number:	860-833-7559
Contact Email Address:	<a href="mailto:sreeji.vijayan@dhs.ga.gov">sreeji.vijayan@dhs.ga.gov</a>
Description of system(s) implemented:	<b>Project Name:</b> Georgia Medicaid Redetermination Noticing Solution

	<p><b>Scope of Work:</b> Georgia DHS/DFCS's objective was to prevent any communication breakdown with citizens and to ensure uninterrupted access to their vital healthcare benefits. The agency wanted to implement a solution to find alternative addresses for clients and generate notices to reduce returned emails and incorrect termination.</p> <p><b>Cardinality's Involvement:</b> Cardinality configured and implemented the Notice Generation Module of its EmpowerHealth Integrated Eligibility Solution to meet the requirement of DHS. It is built on Cardinality's low-code platform (EmpowerPlatform) which has components such as template designer, workflow designer, form builder, reporting &amp; analytics, RBAC, API etc. enabling faster implementation and easier maintainability.</p> <p>The solution was implemented in just 4 months and went live in June 2023. This solution worked in tandem with Georgia Gateway receiving data about returned addresses via SFTP, which is the primary Integrated Eligibility System for the State.</p> <p>The benefits of the solution are listed below:</p> <ul style="list-style-type: none"> <li>• Members receive important and timely notifications</li> <li>• Reduction in the risk of interruptions or gaps in benefits and services</li> <li>• Prevention of incorrect terminations</li> <li>• Continuous Measurement and improvements using insights from Dashboards and Reports</li> </ul> <p><b>Georgia Sees Results in 4 Months:</b> The Noticing Solution for Medicaid Redetermination for the Georgia Department of Human Services (GA DHS) is an example of how our hybrid-agile approach using EmpowerPlatform solved a critical and time sensitive need of dealing with challenges of PHE Unwinding.</p> <p>The solution went live in 4 months with an end-to-end workflow to receive returned address information from Gateway system via SFTP, using the match-and-search algorithm to find alternate addresses in multiple databases and generating multi-lingual notices for printing.</p>
Date of Implementation:	March 2023 - June 2023

**Exhibit 9: Reference 2 - GA Medicaid Redetermination (DHS)**

**Cyquent's Reference:**

Reference 3	Detail
Reference Company Name:	Maryland Department of Human Services
Company Address:	Address: 849 International Drive, Suite 320, Linthicum Heights, MD 21090
Type of Industry:	Government
Contact Name:	Ms. Rebekah Judah
Contact Phone Number:	443-571-2485
Contact Email Address:	Rebekah.Judah@Maryland.Gov
Description of system(s) implemented:	<p><b>Project Name:</b> Maryland Total Human Services Integrated Network (MD THINK)</p> <p><b>Scope of Work:</b> Develop a scalable and modular app to support multiple human services programs.</p> <ul style="list-style-type: none"> <li>• Enable smooth interoperability and data-sharing across mobile and web platforms.</li> <li>• Improve case management by integrating various services into a user-friendly application.</li> <li>• Enhance user experience through automated workflows, real-time updates, and push notifications.</li> <li>• Provide advanced analytics and reporting capabilities to drive data-informed decision-making.</li> <li>• Maintain security, compliance, and accessibility through role-based access controls, HIPAA compliance, and responsive design.</li> </ul> <p><b>Cyquent's Involvement:</b> Cyquent was involved in accomplishing the below deliverables</p> <ul style="list-style-type: none"> <li>• <b>Mobile and Web-Based Unified Case Management:</b> A single app to manage multiple human services programs.</li> <li>• <b>Interoperability:</b> Real-time data exchange across mobile platforms and third-party systems.</li> <li>• <b>Automated Workflows:</b> Task management, appointment scheduling, and service coordination features.</li> <li>• <b>Advanced Analytics &amp; Reporting:</b> Intuitive dashboards with performance tracking and insights.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>User-Centered Design:</b> Accessible, mobile-first interfaces with automated reminders, self-service tools, and integrated chat support</li> <li>• <b>Security &amp; Compliance:</b> Secure login, multi-factor authentication, role-based access, and encrypted data transmission.</li> </ul>
Date of Implementation:	<ul style="list-style-type: none"> <li>• <b>Project Initiation:</b> May 2018</li> <li>• <b>Design &amp; Development:</b> 2018 – 2020</li> <li>• <b>Beta Launch:</b> 2020</li> <li>• <b>Full Release &amp; Statewide Implementation:</b> 2021-</li> <li>• <b>Ongoing Maintenance &amp; Enhancements:</b> 2021 – Present</li> <li>• (Contract end date: May 2025)</li> </ul>

**Exhibit 10: Reference 3 - Maryland DHS MD THINK Reference**

## 9.2 Response to Mandatory Requirements (§ 4.3.2)

Vendors must demonstrate that they have successfully implemented and operated a Child Welfare client communications system for a government agency in the U.S. in compliance with all federal and state regulations within the five (5) years prior to this bid opening. Vendors may use one (1) or more of the references provided in response to Section 4.3.1.5 to satisfy this requirement.

### **Project Name: Georgia Department of Human Services - Foster Care/Communicare**

**Project Description:** Cardinality has successfully deployed its comprehensive EmpowerFamily Child Welfare Foster Care (EF-CWFC) solution in Georgia, providing a robust Foster Care Management System complemented by user-friendly Self-Serve Portals.

**Georgia Communicare** is a set of interconnected web portals and mobile app specifically designed to enable **enhanced and streamlined communication and data access** between DHS case managers and external parties (CASA Volunteer, Biological Parents and Foster Parents) to a foster care case (Refer link: <https://dfcs.georgia.gov/services/georgia-communicare>).

Because of our pre-built solution and the innovative gap-based implementation methodology, phase 1 (**Integrated portal for Foster, Biological parents, and CASA volunteers**) was implemented in a record time of three months, with phase 2 and mobile app rolled out state-wide in the next 5 months. As of September 2024, over 7,500 external users—including CASA volunteers, foster parents, and biological parents—along with more than 3,000 Georgia DHS caseworkers, have been onboarded. They are now equipped to enhance the well-being and safety of children through real-time digital communication and information sharing.

Cardinality's solution included a comprehensive out-of-the-box Foster Care Management Solution and Self-Serve Portal. The project involved:

- Connecting child welfare caseworkers, Court Appointed Special Advocates (CASAs), foster parents, and biological parents

- Equipping primary parties in a foster care case with secure communication and data management capabilities, with different permission levels for each user group
- Providing interconnected web portals to support and enhance communication within child welfare programs

#### Key Features and Enhancements:

- Secure data and file sharing
- Person-to-person chat capabilities
- Appointment scheduling and calendar management
- Calendar integration for appointments
- Child portrait visibility on youth records
- Multiple CASA volunteer assignment capability for a single youth
- Display of CCFA Assessments for CASA and DHS staff
- Improved notifications for all users, including new chat and document approval notifications
- Medicaid number display
- Real-time access to Medicaid cards for foster parents
- Direct invoice submission capability for foster parents through the Communicare Portal

**Implementation Approach:** Cardinality used a gap-based implementation model, similar to the approach proposed for the West Virginia project. This model involved:

- Delivering an initial baseline version of the solution within 30 days of project kickoff
- Conducting discovery sessions to identify gaps and address them incrementally
- Delivering incremental updates at the end of each sprint, minimizing delivery risks and maintaining transparency.

#### Technology Stack:

Cardinality used the Empower low-code platform for Georgia Communicare, which allowed for configuration and customization without extensive coding. The platform supports secure data and file sharing, person-to-person chat, appointment scheduling, and calendar management.

The technology stack also enables integration with other systems, including the **Georgia SHINES** child welfare information system which is similar to the **PATH CCWIS** system in West Virginia. Cardinality emphasizes a user-friendly experience for various user groups, including caseworkers, CASAs, foster parents, and biological parents.

#### Key Components of Cardinality's Technology Stack for Georgia Communicare

- **Low-code Platform:** This enables quick development and deployment of features.
- **Modular Architecture:** Allows for flexibility and scalability as the system evolves.
- **Security and Encryption:** Enables the protection of sensitive data.
- **API and Integration Framework:** Enables smooth data exchange with other systems.
- **Self-Service Portals:** Provides user-friendly interfaces for foster parents, CASAs, and other stakeholders.
- **Mobile Application:** Offers convenient access to Communicare features for DHS employees.
- **Data Analytics and Reporting:** Provides insights to improve decision-making.
- **Training and Support:** Includes training materials, resources, and ongoing support.

#### Specific Technologies and Tools

- **AWS Cloud:** Provides secure and scalable infrastructure for the solution.
- **Talend/State Tool:** Used for data integration and transformation.
- **MicroStrategy/State Tool:** Enables reporting and data visualization.
- **DocuSign:** Facilitates electronic signatures.
- **Google Maps:** Used for GPS home location features.

Our experience with the Georgia Communicare project showcases our expertise in Child Welfare Client Communication systems, encompassing data management, user experience, training, support, and project management. This proven capability positions us as a strong partner to fulfill the needs of WV DHS.



## 10. Availability of Information (§ 6.8)

Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-1 I(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3. d.

By signing below, I certify that I have reviewed this RFP in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any state agency that may require registration.

Elixir Lab USA Inc. (d/b/a) Cardinality.ai

(Company)

Anna Harper, Chief Administrative Officer

(Representative Name, Title)

(513) 907-1068

(Contact Phone/Fax Number)

06-Feb-2025

(Date)

# **REQUEST FOR PROPOSAL**

## **(Department of Human Services CRFP BSS2500000001)**

### **Appendix A: Service Level Agreements (SLAs)**

The Agency will monitor the Vendor's performance during the contract period. Each SLA establishes the performance level expected by the Agency in a particular area. Performance standards are identified within each SLA and are to be measured and reported each month by the Vendor.

#### **Right to Retainage**

The Agency and the Vendor agree that failure by the Vendor to perform per established SLAs results in a loss to the Agency. If the Vendor fails to meet the identified SLA, the Agency may retain a percentage of the total monthly subscription invoice as identified in each SLA and deduct said amounts from the fees due to the Vendor.

The following describes the SLAs established at the time of this RFP publication. The Vendor must ensure the System performance meets the following performance standards:

#### **I. SLA – System Downtime**

- a. Definition:** The system must be available 24 hours a day, seven days a week, and 365 days per year. Downtime is defined as the time during which any component(s) of the System is not functioning or available for any reason. Production downtime is the time during which the System is not available for its intended use in production. There are two types of downtime, as defined below:
  - **Scheduled Downtime:** Any period that the System, or any component(s) of the System, is unavailable for its intended use that has been reviewed and approved by the Agency in advance of the service interruption. Scheduled downtime that has received approval from OMIS does not count toward downtime performance standards.
  - **Unscheduled Downtime:** Any period the System, or any component(s) of the System, is unavailable for its intended use that the State has not approved before the service interruption.
- b. Performance Standard:** Monthly Uptime = 99.9%
- c. Retainage:**
  - Less than 99.9% but greater than or equal to 99.0% = 5% of the monthly invoice
  - Less than 99.0% but greater than or equal to 95.0% = 25% of the monthly invoice
  - Less than 95.0% = 100% of the monthly invoice

#### **II. SLA – Issue Tracking**

- a. Definition:** After go-live, the Vendor must provide software tools to enable the tracking of a specific defect from identification through resolution, including all testing performed to ensure the correct fix is in place. Vendor will escalate all defects to the Agency in a CAP.

# **REQUEST FOR PROPOSAL**

## **(Department of Human Services CRFP BSS2500000001)**

- b. Performance Standard:** All defects identified by the Vendor, the Agency, or public users must be included in a CAP provided to the Agency on a weekly basis or more frequently as requested by the Agency.
- c. Retainage** Two percent (2%) of the monthly invoice in which the performance standard was not met.

### **III. SLA – Issue Response and Resolution**

- a. Definition:** Issues identified by the Vendor or Agency must be categorized by level of impact, responded to in a defined period, and resolved within a defined period. Levels of impact are:
  - **Critical:** Total system failure, critical system functionality is unavailable with no workaround available, or Agency clients or stakeholders are at risk of failing to meet legal or child welfare policy requirements.
  - **High:** Partial system failure where certain non-critical functionality will not operate, but users can still access critical functionality of the main system or where a work around is not available. Agency clients or stakeholders are not at risk of failing to meet legal or child welfare policy requirements.
  - **Medium:** Non-critical functionality of the system has failed, but operation is not affected or only slightly impaired. Error limits the functionality or usefulness of the system, but not critical to the continued operations. A workaround is readily available and can be applied or used with little or no operational impact and no data integrity issues.
  - **Low:** Minimal problems in the system arising from a misleading or unsatisfactory component or feature. The problem can be circumvented with no operational impact and there are no data integrity issues.
- b. Performance Standard:**
  - **Critical:** Vendor must respond via an agreed-upon communication method to the Agency point of contact within one (1) hour of receipt of initial notification. Vendor must provide a fix or temporary workaround within eight (8) hours of initial notification, including after hours and weekends. If a workaround is provided, a complete fix will be implemented within 24 hours of the workaround.
  - **High:** Vendor must respond via an agreed-upon communication method means to the Agency point of contact within two (2) hours of receipt of initial notification. Vendor must provide a fix or workaround within 24 hours of initial notification. If a workaround is provided, a complete fix will be implemented within 48 hours of the workaround.
  - **Medium:** Vendor must respond via an agreed-upon communication method means to the Agency point of contact within four (4) hours of receipt of initial notification. Vendor must provide a fix or workaround within five calendar days of initial notification. If a

# **REQUEST FOR PROPOSAL**

## **(Department of Human Services CRFP BSS2500000001)**

workaround is provided, a complete fix will be implemented within five calendar days of the workaround.

- **Low:** Vendor must respond via an agreed upon communication method means to the Agency point of contact within 24 hours of receipt of initial notification. Vendor must provide a fix in a support release within 30 days of the initial notification.
- c. **Retainage:** Five percent (5%) of the monthly invoice in which the performance standard was not met.

### **IV. SLA – Hours of Operation**

- a. **Performance Standard:** The Vendor's System technical support must be available to users Monday through Sunday from 7 a.m. to 7 p.m. eastern time (ET). The Vendor must provide after-hours and holiday on-call support for critical incidents from expert technicians who are familiar with the Agency.

Response times to support requests must be less than 15 minutes for at least 95% of the requests.

The Vendor must respond to user support requests in the caller's preferred language or with oral interpretation services.

- b. **Retainage:** Five percent (5%) of the monthly invoice in which the performance standard was not met.

### **V. SLA – Monthly Reporting**

- a. **Performance Standard:** Vendor must provide the Agency with monthly reports due no later than the 15<sup>th</sup> of each month. Reports should include, but will not be limited to:

- System downtime information
- CAP including all issues added in the prior month and all outstanding issues
- Issue response and resolution metrics
- Technical support response metrics

- b. **Retainage:** Two percent (2%) of the monthly subscription invoice in which the performance standard was not met.

### **VI. Corrective Action**

When an SLA is not met, the Vendor is expected to provide the Agency with a written detailed CAP with the monthly report, which describes:

- a. The missed SLA
- b. Full description of the issue
- c. Cause of the problem

## **REQUEST FOR PROPOSAL**

**(Department of Human Services CRFP BSS2500000001)**

- d. Risks related to the issue**
- e. The resolution, including any failed solutions implemented before resolution**
- f. Proposed corrective action going forward to avoid missing the SLA in the future**

Upon receipt of the CAP, the Agency may request a meeting to further discuss related issues. The Vendor is to implement the proposed corrective action only upon Agency approval.

# **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

## **Appendix B: Functional and Technical Requirements**

## Appendix B: Functional and Technical Requirements

Table of Contents		
Tab No.	Requirements Category	Number of Requirements
1	Functional	17
2	Technical	12
	<b>Total</b>	<b>29</b>
Requirements Criticality Indicators		
Indicator	Definition	
Mandatory	Functionality is necessary for the system to support current or planned State business processes.	
Desirable	Functionality is desired, but not necessary, for the system.	
Vendor Response		
Response Indicators: When providing responses to the requirements, Vendors shall use the following response indicators:		Instruction
<b>S</b>	<b>Standard:</b> Feature/Function is included in the current software release and will be implemented by the planned phase go-live date as part of the proposal from Vendors in accordance with agreed-upon configuration planning with the State.	Vendors are encouraged, but not required, to provide additional information in the Comments column to further demonstrate the system's ability to meet the requirement.
<b>F</b>	<b>Future:</b> Feature/Function will be available in a future software release available to the State by the phase implementation required, at which point it will be implemented in accordance with agreed-upon configuration planning with the State.	If a response indicator of "F" is provided for a requirement that will be met in a future software release, the Vendor shall indicate the planned release version as well as the date the release will be available.
<b>C</b>	<b>Customization:</b> Feature/Function is not included in the current software release, and is not planned to be a part of a future software release. However, this feature could be provided with custom modifications. All related customization costs should be indicated in the Comments column next to the feature/function, and the total cost included in the Cost Proposal deliverable for Configuration and Customization.	If a response indicator of "C" is provided for a requirement that will be met through a custom modification, the Vendor shall include the cost of such a modification in its cost proposal.
<b>T</b>	<b>Third-Party:</b> Feature/Function is not included in the current software release, and is not planned to be a part of a future software release. However, this feature could be provided with integration with a third-party system. This system should be specified.	If a response indicator of "T" is provided for a requirement that will be met by integration with a third-party system, the Vendor shall identify this third-party system and include the cost to secure this system in its cost proposal.
<b>N</b>	<b>No:</b> Feature/Function cannot be provided.	Any blank response will be considered an "N".

Functional					
*Phase Implemented: Requirements for functionality first implemented in Phase 1 (by September 1, 2025) of the project will be marked as 1 and functionality first implemented or updated in Phase 2 (no later than July 1, 2026) will be marked as 2.					
Req. #	Requirement Description	Mandatory/Desirable	Phase Implemented per W. Va. Code §49-2-111(c)(1) language*	Vendor Response	Comments
Communication					
F.C.1	The Solution must include the following features in its messaging functionality: a. Allow authorized users to securely communicate and send messages among authorized users b. View message history	Mandatory	1		
F.C.2	The Solution must include notifications to authorized users when information is new or tasks are due. Alerts should be provided when tasks require a user's attention or changes to the child's case are noted/documented (e.g., change to placement location).	Mandatory	1		
F.C.3	The Solution must archive communication into the CCWIS, including but not limited to text, email, and/or chat, via a format or process that successfully interfaces with the CCWIS.	Mandatory	1		
F.C.4	The Solution should provide secure messaging functionality in multiple platforms, including but not limited to email, chat and/or text.	Desirable	1		
F.C.5	The Solution should include the following features in its messaging functionality: a. File-share with authorized user(s)	Desirable	2		
Information Access					
F.I.1	As the Solution components becomes interfaced with the CCWIS, the Solution must pull/push information (i.e., function bidirectionally) with the CCWIS where the CCWIS is the sole source of any/all information and documentation - and archive of such information and documentation - for all foster cases.	Mandatory	2		
F.I.2	The Solution must allow RBAC to access case record information in the CCWIS, such as education, medical, dental, mental health, psychology evaluation, and visitation records.	Mandatory	2		
F.I.3	The Solution must allow RBAC to upload to the portal, to be stored in the CCWIS, any/all case documentation such as family plans, safety plans, photos, and verification documents.	Mandatory	2		
F.I.4a	The Solution should allow authorized users to: a. Enter online/offline messaging (e.g., SMS/Email/In-App), to be uploaded to the CCWIS immediately (if online) or as soon as connectivity is restored (if offline) b. Video/audio conferencing with authorized users, and with a recording function	Desirable	1		
F.I.4b	The Solution should allow authorized users to: a. Take a photo, video, or audio recording b. Document updates, such as completion of goals/tasks/steps c. Request and view upcoming meetings with case workers d. Upload verification documents (e.g., pay stubs, lease agreement, certificates of completion, etc.)	Desirable	2		
F.I.5	The system should allow access to various document formats, including but not limited to: a. AVI b. BMP c. DOC d. DOCX e. JPEG f. JPEG g. JPG h. MP4 i. PDF j. TIFF k. TXT l. XLS	Desirable	2		
F.I.6	The Solution should allow authorized users digital signatures to be collected on documents that are stored in the CCWIS.	Desirable	2		
F.I.7	The Solution should provide primary information upload confirmation prior to the CCWIS interface, in relation to Technical requirement T.G.8.	Desirable	2		



F.I.8	<p>The Solution should allow authorized user(s) to access documentation including but not limited to the following examples:</p> <ul style="list-style-type: none"> <li>a. Educational evaluation/records</li> <li>b. Medical evaluation/records</li> <li>c. Dental evaluation/records</li> <li>d. Therapeutic/mental health records</li> <li>e. Home evaluations</li> <li>f. Visitation/family time records</li> <li>g. Case or family plan</li> <li>h. Safety Plan or Assessment</li> <li>i. Case worker contact log</li> <li>j. Court filing</li> <li>k. Demographic information</li> </ul>	Desirable	2		
Scheduling					
F.S.1	<p>The Solution should include a calendar module accessible for all authorized users that allows users to schedule events involved in the respective child's case (e.g., visitation sessions for foster child and biological parent/guardian). The user should be able to add, change, or delete items, including but not limited to:</p> <ul style="list-style-type: none"> <li>a. Appointments</li> <li>b. Non-emergency medical visits</li> <li>c. Guardian Ad Litem (GAL)</li> <li>d. MDT meetings</li> <li>e. Visitations</li> <li>f. Vacations</li> <li>g. Court dates</li> <li>h. SNS provider services</li> </ul>	Desirable	2		
Reporting					
F.R.1	The Solution must create a performance report that shows the time measurement of user's responsiveness to questions or requests.	Mandatory	2		
F.R.2	The Solution should create performance reports through flexible reporting functionality to include both predesigned and ad hoc reporting.	Desirable	2		

Technical					
*Phase Implemented: Requirements for functionality first implemented in Phase 1 (by September 1, 2025) of the project will be marked as 1 and functionality first implemented or updated in Phase 2 (no later than July 1, 2026) will be marked as 2.					
Req. #	Requirement Description	Mandatory/ Desirable	Phase Implemented per W. Va. Code §49-3-114(b) Language*	Vendor Response	Comments
General					
T.G.1	The Solution must allow authorized administrators the capability to grant and deny user access at any time.	Mandatory	1		
T.G.2	The Solution must allow role-based access control (RBAC) to manage user experience, features, and access and/or functionality.	Mandatory	1		
T.G.3	The Solution must be browser agnostic.	Mandatory	1		
T.G.4	Recovery Time Objective (RTO) - In the event of an unplanned outage, the system shall be returned to live operation in 4 hours or less	Mandatory	1		
T.G.5	Recovery Point Objective (RPO) - Data will be backed up in a manner that assures the system can always be restored with no loss of data	Mandatory	1		
T.G.6	The Solution must identify and flag duplicate entries of information.	Mandatory	2		
T.G.7	The Solution should require permission access using a single sign-on (SSO).	Desirable	1		
T.G.8	The Solution should enable authorized users to access and enter information through a mobile device.	Desirable	1		
T.G.9	The Solution should allow RBAC to schedule mass or batch changes at an established time frame.	Desirable	2		
T.G.10	The Vendor should resolve data input errors reported by users within two (2) business days from when the report was received.	Desirable	2		
Security					
T.S.1	<p>The Vendor and the Solution must meet all applicable State and Federal privacy, confidentiality, and security requirements. Per 45 CFR 1355.52 (d) (iii), the CCWIS data must "be exchanged and maintained in accordance with confidentiality requirements in Section 471 (a) (8) of the Act, and 45 CFR 205.50, and 42 U.S.C. 5106a (b) (2) (B) (viii) through (x) of the Child Abuse Prevention and Treatment Act, if applicable, and other applicable federal and state or tribal laws". The Contractor must ensure that all data in its possession meets the standards outlined in 45 CFR 1355.52 (d) (iii) and complies with the following list of Federal standards:</p> <ul style="list-style-type: none"> <li>a. Federal Information Security Risk Assessment (ISRA) Procedures</li> <li>b. CMS System Security Plan</li> <li>c. 42 CFR Parts 412, 413, 422, 433</li> <li>d. 45 CFR Part 160 Administration</li> <li>e. 45 CFR Part 162 Privacy</li> <li>f. 45 CFR Part 164 Security</li> <li>g. Records Usage, Duplication, Retention, Re-disclosure, and Timely Destruction Procedures/Restrictions</li> <li>h. Internal Revenue Service (IRS) Publication 1075 compliance</li> <li>i. Privacy Act of 1974 at 5 U.S.C. 552a</li> <li>j. Federal Information Security Management Act (FISMA)</li> <li>k. SSA Information System Security Guidelines for federal, State, and local agencies</li> <li>l. Title XIX Confidentiality Rules</li> <li>m. CMS Standards and Conditions at 42 CFR 433.112</li> <li>n. ACF CCWIS Design Requirements established in §1355.53</li> <li>o. MARS-E (At a minimum MARS-E 2.0)</li> <li>p. Confidentiality requirements under Section 471(a)(8) of the Social Security Act</li> <li>q. Confidentiality/access requirements under Section 106(b)(2)(a)(v) of the Child Abuse Prevention and Treatment Act</li> </ul>	Mandatory	1		
T.S.2	The Solution should allow a default access level for assigned users of a multi-disciplinary team (MDT) prior to the MDT meeting.	Desirable	2		

# **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

## **Appendix C: Cost Proposal Form**

Appendix C: Cost Workbook

Vendor: *Elixir Lab USA Inc (d/b/a Cardinality.ai)*

Notes

*The costs on this worksheet will be automatically calculated using the information entered on the other worksheets. It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.*

Total Cost Summary								
Description	Implementation	Maintenance & Operations - Base Term			Optional Term 1	Optional Term 2	Optional Term 3	Total Costs
	Years 1-2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	
Project Deliverables & Project Management	\$ 1,670,400.00							\$ 1,670,400.00
Licensing - Subscription	\$ 122,440.00	\$ 593,610.00	\$ 593,610.00	\$ 617,354.40	\$ 617,354.40	\$ 617,354.40	\$ 642,048.58	\$ 3,803,771.78
Total	\$ 1,792,840.00	\$ 593,610.00	\$ 593,610.00	\$ 617,354.40	\$ 617,354.40	\$ 617,354.40	\$ 642,048.58	\$ 5,474,171.78

Appendix C: Cost Workbook

Vendor: Elixir Lab USA Inc (d/b/a Cardinality.ai)

Implementation Services Hourly Rates	
Staff Position	Rate
Account Manager	\$ 150.00
Project Manager	\$ 125.00
Business Lead	\$ 120.00
Technical Lead	\$ 120.00
Implementation Manager	\$ 125.00
Operations Manager	\$ 120.00
Quality Assurance Manager	\$ 110.00
Testing Manager	\$ 110.00
Information Security Architect/Privacy Data Protection Officer	\$ 140.00
Developer	\$ 110.00
Tester	\$ 100.00
Integration Lead	\$ 120.00
Solution Architect	\$ 120.00
UI/UX Designer	\$ 100.00
Support Engineer	\$ 100.00

Maintenance and Operations Services Hourly Rates									
Staff Position	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	
Account Manager	\$ 150.00	\$ 150.00	\$156	\$156	\$156	\$162	\$162	\$162	
Project Manager	\$ 125.00	\$ 125.00	\$130	\$130	\$130	\$135	\$135	\$135	
Business Lead	\$ 120.00	\$ 120.00	\$125	\$125	\$125	\$130	\$130	\$130	
Technical Lead	\$ 120.00	\$ 120.00	\$125	\$125	\$125	\$130	\$130	\$130	
Implementation Manager	\$ 125.00	\$ 125.00	\$130	\$130	\$130	\$135	\$135	\$135	
Operations Manager	\$ 120.00	\$ 120.00	\$125	\$125	\$125	\$130	\$130	\$130	
Quality Assurance Manager	\$ 110.00	\$ 110.00	\$114	\$114	\$114	\$119	\$119	\$119	
Testing Manager	\$ 110.00	\$ 110.00	\$114	\$114	\$114	\$119	\$119	\$119	
Information Security Architect/Privacy Data Protection Officer	\$ 140.00	\$ 140.00	\$146	\$146	\$146	\$151	\$151	\$151	
Developer	\$ 110.00	\$ 110.00	\$115	\$115	\$115	\$120	\$120	\$120	
Tester	\$ 100.00	\$ 100.00	\$104	\$104	\$104	\$108	\$108	\$108	
Integration Lead	\$ 120.00	\$ 120.00	\$125	\$125	\$125	\$130	\$130	\$130	
Solution Architect	\$ 120.00	\$ 120.00	\$125	\$125	\$125	\$130	\$130	\$130	
UI/UX Designer	\$ 100.00	\$ 100.00	\$104	\$104	\$104	\$108	\$108	\$108	
Support Engineer	\$ 100.00	\$ 100.00	\$104	\$104	\$104	\$108	\$108	\$108	

Notes

This tab must be used to provide contractor/subcontractor hourly labor rates for the various classifications and grades of personnel. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Vendor's staff training, project facility, and any other expenses associated with the delivery and implementation of the proposed items must be included in the Vendor's costs and fixed hourly rates.

The Agency will use the "Labor Rates" supplied by the Vendor as a rate card for all future change requests during Implementation or Maintenance and Operations.

Vendor may include additional roles to describe the various classifications and grades of its personnel. Vendors may insert additional rows as required (e.g., a Senior-Level Programmer and a Junior-Level Programmer require two separate rows).

*It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.*

# Appendix C: Cost Workbook

Vendor: Elixir Lab USA Inc (d/b/a Cardinality.ai)

Project Deliverables		Total Cost	Deliverable Cost		
<b>Instructions</b>					
The Agency has included required efforts and deliverables, but Vendors should add any additional deliverables that will be part of each effort and may reorder and renumber efforts or deliverables as needed. The Agency has also included a phased approach to the implementation of the communication system. The Agency will retain 10% of each payment milestone until system acceptance and Phase 2 transition to Operational Support.					
<b>Project Planning</b>					
<b>Payment Milestone 1: Project Planning Complete</b>		\$ 70,400.00			
D001	Project Kick-off Meeting		\$ 10,560.00		
D002	Final Project Management Plan		\$ 10,560.00		
D003	Requirements Refinement and Gap Analysis		\$ 35,200.00		
D004	Implementation Plan		\$ 14,080.00		
	Vendor to add other deliverables as needed		\$ -		
			\$ -		
			\$ -		
			\$ -		
<b>Phase 1 Implementation</b>					
<b>Payment Milestone 2: Phase 1 System Go-Live</b>		\$ 711,360.00			
D006	Installation and Environmental Setup		\$ 67,392.00		
D007	Configuration and Customization		\$ 262,080.00		
D008	Interface Design and Development		\$ 82,368.00		
D009	Testing and Quality Assurance (including User Acceptance Testing [UAT])		\$ 104,832.00		
D010	Development of Video-Based Training and Materials		\$ 52,416.00		
D011	Tracking Video-Based Training Completion		\$ 59,904.00		
D012	Go-Live Readiness Assessment		\$ 22,464.00		
D013	Go-Live Support		\$ 22,464.00		
D014	Go-Live Event		\$ 37,440.00		
	Vendor to add other deliverables as needed		\$ -		
			\$ -		
			\$ -		
			\$ -		
<b>Payment Milestone 3: Phase 1 System Post-Go-Live Support (90 days after Go-Live)</b>		\$ 37,440.00			
D016	Post-Go-Live Support (Transition to Operational Support)		\$ 37,440.00		
D017	Vendor to add other deliverables as needed		\$ -		
			\$ -		
<b>Phase 2 Implementation</b>					
<b>Payment Milestone 4: Phase 2 System Go-Live</b>		\$ 716,800.00			
D018	Configuration and Customization		\$ 250,880.00		
D019	Interface Design and Development		\$ 107,520.00		
D020	Testing and Quality Assurance (including User Acceptance Testing [UAT])		\$ 107,520.00		
D021	Development of Video-Based Training and Materials		\$ 50,176.00		
D022	Tracking Video-Based Training Completion		\$ 57,344.00		
D023	Go-Live Readiness Assessment		\$ 21,504.00		
D024	Go-Live Support		\$ 50,176.00		
D025	Go-Live Event		\$ 71,680.00		
	Vendor to add other deliverables as needed		\$ -		
			\$ -		
<b>Payment Milestone 5: Phase 2 System Post-Go-Live Support (90 days after Go-Live)</b>		\$ 134,400.00			
D027	Post-Go-Live Support (Transition to Operational Support)		\$ 134,400.00		
D028	Vendor to add other deliverables as needed		\$ -		
			\$ -		
<b>Additional Vendor Proposed Deliverables</b>		\$ -			
	Other (specify)		\$ -		
	Other (specify)		\$ -		
	Other (specify)		\$ -		
	Other (specify)		\$ -		
	Other (specify)		\$ -		
	Other (specify)		\$ -		
<b>Total Implementation Costs</b>		<b>\$ 1,670,400.00</b>			

# Appendix C: Cost Workbook

**Vendor:**

**Elixir Lab USA Inc (d/b/a Cardinality.ai)**

Vendor must provide a response in each cost cell of this worksheet.

	Licensing or Subscription Costs							
	Implementation		Maintenance & Operations - Base Term					
	Year 1	Year 2	Year 3	Year 4	Year 5	Optional Term 1 Year 6	Optional Term 2 Year 7	Optional Term 3 Year 8
Licensing	\$ 49,440.00	\$ -	\$ 237,810.00	\$ 237,810.00	\$ 247,322.40	\$ 247,322.40	\$ 247,322.40	\$ 257,215.30
Hosting	\$ 73,000.00	\$ -	\$ 183,000.00	\$ 183,000.00	\$ 190,320.00	\$ 190,320.00	\$ 190,320.00	\$ 197,932.80
Maintenance and Support	\$ -	\$ -	\$ 172,800.00	\$ 172,800.00	\$ 179,712.00	\$ 179,712.00	\$ 179,712.00	\$ 186,900.48
Subscription	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
<b>Total Licensing or Subscription Costs</b>	<b>\$ 122,440.00</b>	<b>\$ -</b>	<b>\$ 593,610.00</b>	<b>\$ 593,610.00</b>	<b>\$ 617,354.40</b>	<b>\$ 617,354.40</b>	<b>\$ 617,354.40</b>	<b>\$ 642,048.58</b>

## Appendix C: Cost Workbook

Vendor: *Elixir Lab USA Inc (d/b/a Cardinality.ai)*

Item #	Attachment	Attachment Section or Page	Description	Rationale	Cost Impact If Assumption is Invalid
1	Appendix C - Cost Proposal Form	5. Licensing-Subscription	The Cardinality solution will be hosted on AWS GovCloud for production instance	The Agency requires a Vendor-hosted Solution	\$ -
2	Appendix C - Cost Proposal Form	5. Licensing-Subscription	AWS Cloud Hosting includes four non-production instances - Development, Integration Testing, UAT and Staging	The number of non-production environments included in the subscription or license	\$ -
3	Appendix C - Cost Proposal Form	5. Licensing-Subscription	The Cardinality SaaS license cost is provided for the following named users: Upto 850 staff and 660 other users.	<p>The number of named users of the solution have been estimated based on the numbers mentioned in Table 1: Interested Parties and Estimated Group Sizes of the RFP document (CRFP BSS2500000001_Complete Solicitation Documents).</p> <p>In the case of SNS Provider Agencies, State Counties (for legal community users) and CPAs, 5 named users have been assumed per provider group as each of these could have multiple staff involved in foster cases.</p>	\$ -
4	Appendix C - Cost Proposal Form	5. Licensing-Subscription	No user license fees is charged for children/youth in foster care	Cardinality does not charge license fees for citizen users of the solution	\$ -
5	Appendix C - Cost Proposal Form	5. Licensing-Subscription	In the Licensing-Subscription tab, cost is not applicable for Year-2 of implementation as the implementation period is for 12 months only	The timeline for implementation of Phase-1 and Phase-2 will be 12 months as per the proposed implementation plan	\$ -
6	Addendum-1	Vendor Questions and Answers #44	Cardinality will leverage the DocuSign licenses of the Agency for e-signature	Cardinality solution can be integrated with digital signing tools such as DocuSign. The license for the same must be procured by the Agency Note: In the cost impact column, the DocuSign cost mentioned is per year	\$ 151,000.00
7	Appendix C - Cost Proposal Form	5. Licensing-Subscription	Cardinality SaaS license cost includes - Yearly 2 upgrades, monthly hot fixes and level 3 support	Inclusions in the SaaS license cost during M&O	\$ -
8	Addendum-1	Vendor Questions and Answers #18	All resources will be based out of the US	All resources are assumed to be based out of the US as per the response provided to vendor question in Vendor Questions and Answers	\$ -
9	Addendum-1	Vendor Questions and Answers #17	Data migration is not part of scope of work	As the data will remain in PATH, there is no need for data migration to the Cardinality solution	\$ -



10	Appendix B - Functional and Technical Requirements	2. Technical T.G.8	Cardinality will deliver a mobile responsive solution. Mobile application development is not part of the scope of work.		\$ 400,000.00
11	Appendix C - Cost Proposal Form	5. Licensing-Subscription	In the Licensing-Subscription tab, license cost includes Cardinality SaaS license and third party software cost. Hence no value is mentioned against subscription cost as it is not applicable		\$ -
12					
13					\$ -
14					\$ -
15					\$ -
16					\$ -
17					\$ -
18					\$ -
19					\$ -
20					\$ -

#### Notes

The Vendor is required to state all assumptions upon which its pricing is being determined. Insert as many lines as necessary to ensure all concerns are accurately expressed. Assumptions shall not conflict with the Terms and Conditions or Mandatory Requirements of this RFP.

The Vendor should provide pricing consistent with the following:

- Apply the pricing in accordance with the Terms and Conditions and Mandatory Requirements of the RFP.
- Clearly identify and explain all of the pricing assumptions made, upon which pricing is predicated including the cost/pricing impact if the assumption is invalid.
- State if any charge is subject to Special Conditions, and clearly specify those conditions and quantify their impact upon the charges.

## Title page

**RFP subject number** : Request for Proposal. CRFP 0511 BSS2500000001

**Vendor's name** : Elixir Lab USA Inc. d/b/a Cardinality.ai

**Business address** : 267 Kentlands Boulevard Suite #5092,  
Gaithersburg, MD 20878

**Telephone number** : (513) 907-1068

**Name of contact person** : Anna Harper, Chief Administrative Officer

**E-mail address** : [sales@cardyai.com](mailto:sales@cardyai.com)

**Vendor signature:**



06-Feb-2025

Date

# **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

## **Attachment A: Federal Funds Addendum**

Please see Federal Funds Addendum in wvOASIS.

**FEDERAL FUNDS ADDENDUM**  
**2 C.F.R. §§ 200.317 – 200.327**

**Purpose:** This addendum is intended to modify the solicitation in an attempt to make the contract compliant with the requirements of 2 C.F.R. §§ 200.317 through 200.327 relating to the expenditure of certain federal funds. This solicitation will allow the State to obtain one or more contracts that satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

**Instructions:** Vendors who are willing to extend their contract to procurements with federal funds and the requirements that go along with doing so, should sign the attached document identified as: "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)"

Should the awarded vendor be unwilling to extend the contract to federal funds procurement, the State reserves the right to award additional contracts to vendors that can and are willing to meet federal funds procurement requirements.

**Changes to Specifications:** Vendors should consider this solicitation as containing two separate solicitations, one for state level procurement and one for county/local procurement.

**State Level:** In the first solicitation, bid responses will be evaluated with applicable preferences identified in sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" to establish a contract for both standard state procurements and state federal funds procurements.

**County Level:** In the second solicitation, bid responses will be evaluated with applicable preferences identified in Sections 15, 15A, and 16 of the "Instructions to Vendors Submitting Bids" omitted to establish a contract for County/Local federal funds procurement.

**Award:** If the two evaluations result in the same vendor being identified as the winning bidder, the two solicitations will be combined into a single contract award. If the evaluations result in a different bidder being identified as the winning bidder, multiple contracts may be awarded. The State reserves the right to award to multiple different entities should it be required to satisfy standard state procurement, state federal funds procurement, and county/local federal funds procurement requirements.

**State Government Use Caution:** State agencies planning to utilize this contract for procurements subject to the above identified federal regulations should first consult with the federal agency providing the applicable funding to ensure the contract is compliant.

**County/Local Government Use Caution:** County and Local government entities planning to utilize this contract for procurements subject to the above identified federal regulation should first consult with the federal agency providing the applicable funding to ensure the contract is compliant. For purposes of County/Local government use, the solicitation resulting in this contract was conducted in accordance with the procurement laws, rules, and procedures governing the West Virginia Department of Administration, Purchasing Division, except that vendor preference has been omitted for County/Local use purposes and the contract terms contained in the document entitled "REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317)" have been added.

## **FEDERAL FUNDS ADDENDUM**

### **REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):**

The State of West Virginia Department of Administration, Purchasing Division, and the Vendor awarded this Contract intend that this Contract be compliant with the requirements of the Procurement Standards contained in the Uniform Administrative Requirements, Cost Principles, and Audit Requirements found in 2 C.F.R. § 200.317, et seq. for procurements conducted by a Non-Federal Entity. Accordingly, the Parties agree that the following provisions are included in the Contract.

#### **1. MINORITY BUSINESSES, WOMEN'S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS: (2 C.F.R. § 200.321)**

- a. The State confirms that it has taken all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. Those affirmative steps include:
  - (1) Placing qualified small and minority businesses and women's business enterprises on solicitation lists;
  - (2) Assuring that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
  - (3) Dividing total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
  - (4) Establishing delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises;
  - (5) Using the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce; and
  - (6) Requiring the prime contractor, if subcontracts are to be let, to take the affirmative steps listed in paragraphs (1) through (5) above.
- b. Vendor confirms that if it utilizes subcontractors, it will take the same affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible.

#### **2. DOMESTIC PREFERENCES: (2 C.F.R. § 200.322)**

- a. The State confirms that as appropriate and to the extent consistent with law, it has, to the greatest extent practicable under a Federal award, provided a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United

States (including but not limited to iron, aluminum, steel, cement, and other manufactured products).

- b. Vendor confirms that will include the requirements of this Section 2. Domestic Preference in all subawards including all contracts and purchase orders for work or products under this award.

- c. Definitions: For purposes of this section:

- (1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

- (2) "Manufactured products" means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

**3. BREACH OF CONTRACT REMEDIES AND PENALTIES:**

(2 C.F.R. § 200.327 and Appendix II)

- (a) The provisions of West Virginia Code of State Rules § 148-1-5 provide for breach of contract remedies, and penalties. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

**4. TERMINATION FOR CAUSE AND CONVENIENCE:**

(2 C.F.R. § 200.327 and Appendix II)

- (a) The provisions of West Virginia Code of State Rules § 148-1-5 govern Contract termination. A copy of that rule is attached hereto as Exhibit A and expressly incorporated herein by reference.

**5. EQUAL EMPLOYMENT OPPORTUNITY:**

(2 C.F.R. § 200.327 and Appendix II)

Except as otherwise provided under 41 CFR Part 60, and if this contract meets the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3, this contract includes the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

**6. DAVIS-BACON WAGE RATES:**

(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this Contract includes construction, all construction work in excess of \$2,000 will be completed and paid for in compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must:

- (a) pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor.
- (b) pay wages not less than once a week.

A copy of the current prevailing wage determination issued by the Department of Labor is attached hereto as Exhibit B. The decision to award a contract or subcontract is conditioned upon the acceptance of the wage determination. The State will report all suspected or reported violations to the Federal awarding agency.

**7. ANTI-KICKBACK ACT:**  
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that it will comply with the Copeland Anti-KickBack Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). Accordingly, Vendor, Subcontractors, and anyone performing under this contract are prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The State must report all suspected or reported violations to the Federal awarding agency.

**8. CONTRACT WORK HOURS AND SAFETY STANDARDS ACT**  
(2 C.F.R. § 200.327 and Appendix II)

Where applicable, and only for contracts awarded by the State in excess of \$100,000 that involve the employment of mechanics or laborers, Vendor agrees to comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

**9. RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT.**  
(2 C.F.R. § 200.327 and Appendix II)

If the Federal award meets the definition of "funding agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

**10. CLEAN AIR ACT**  
(2 C.F.R. § 200.327 and Appendix II)

Vendor agrees that if this contract exceeds \$150,000, Vendor is to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401–7671g) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251–1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

**11. DEBARMENT AND SUSPENSION**  
(2 C.F.R. § 200.327 and Appendix II)

The State will not award to any vendor that is listed on the governmentwide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

**12. BYRD ANTI-LOBBYING AMENDMENT**  
(2 C.F.R. § 200.327 and Appendix II)

Vendors that apply or bid for an award exceeding \$100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

**13. PROCUREMENT OF RECOVERED MATERIALS**  
(2 C.F.R. § 200.327 and Appendix II; 2 C.F.R. § 200.323)

Vendor agrees that it and the State must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the



Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

**14. PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.**  
(2 C.F.R. § 200.327 and Appendix II; 2 CFR § 200.216)

Vendor and State agree that both are prohibited from obligating or expending funds under this Contract to:

- (1) Procure or obtain;
- (2) Extend or renew a contract to procure or obtain; or
- (3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
  - (i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
  - (ii) Telecommunications or video surveillance services provided by such entities or using such equipment.
  - (iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

In implementing the prohibition under Public Law 115-232, section 889, subsection (f), paragraph (1), heads of executive agencies administering loan, grant, or subsidy programs shall prioritize available funding and technical support to assist affected businesses, institutions and organizations as is reasonably necessary for those affected entities to transition from covered communications equipment and services, to procure replacement equipment and services, and to ensure that communications service to users and customers is sustained.

State of West Virginia

By: Althea Greenhowe

Printed Name: Althea Greenhowe

Title: Procurement Specialist, Sr

Date: 5/9/2025

Vendor Name: Elixir Lab USA Inc. d/b/a  
Cardinality.ai

By: Anna Harper

Printed Name: Anna Harper

Title: Chief Administrative Officer

Date: 01/27/2025

**EXHIBIT A To:  
REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY  
CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):**

**W. Va. CSR § 148-1-5**

West Virginia Code of State Rules  
Title 148. Department of Administration  
Legislative Rule (Ser. 1)  
Series 1. Purchasing

W. Va. Code St. R. § 148-1-5  
§ 148-1-5. Remedies.

Currentness

5.1. The Director may require that the spending unit attempt to resolve any issues that it may have with the vendor prior to pursuing a remedy contained herein. The spending unit must document any resolution efforts and provide copies of those documents to the Purchasing Division.

5.2. Contract Cancellation.

5.2.1. Cancellation. The Director may cancel a purchase or contract immediately under any one of the following conditions including, but not limited to:

5.2.1.a. The vendor agrees to the cancellation;

5.2.1.b. The vendor has obtained the contract by fraud, collusion, conspiracy, or is in conflict with any statutory or constitutional provision of the State of West Virginia;

5.2.1.c. Failure to honor any contractual term or condition or to honor standard commercial practices;

5.2.1.d. The existence of an organizational conflict of interest is identified;

5.2.1.e. Funds are not appropriated or an appropriation is discontinued by the legislature for the acquisition;

5.2.1.f. Violation of any federal, state, or local law, regulation, or ordinance, and

5.2.1.g. The contract was awarded in error.

5.2.2. The Director may cancel a purchase or contract for any reason or no reason, upon providing the vendor with 30 days' notice of the cancellation.

5.2.3. Opportunity to Cure. In the event that a vendor fails to honor any contractual term or condition, or violates any provision of federal, state, or local law, regulation, or ordinance, the Director may request that the vendor remedy the contract breach or legal violation within a time frame the Director determines to be appropriate. If the vendor fails to remedy the contract breach or legal violation or the Director determines, at his or her sole discretion, that such a request is unlikely to yield a satisfactory result, then he or she may cancel immediately without providing the vendor an opportunity to perform a remedy.

5.2.4. Re-Award. The Director may award the cancelled contract to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) without a subsequent solicitation if the following conditions are met:

5.2.4.a. The next lowest responsible bidder (or next highest scoring bidder if best value procurement) is able to perform at the price contained in its original bid submission, and

5.2.4.b. The contract is an open-end contract, a one-time purchase contract, or a contract for work which has not yet commenced.

Award to the next lowest responsible bidder (or next highest scoring bidder if best value procurement) will not be an option if the vendor's failure has in any way increased or significantly changed the scope of the original contract. The vendor failing to honor contractual and legal obligations is responsible for any increase in cost the state incurs as a result of the re-award.

5.3. Non-Responsible. If the Director believes that a vendor may be non-responsible, the Director may request that a vendor or spending unit provide evidence that the vendor either does or does not have the capability to fully perform the contract requirements, and the integrity and reliability necessary to assure good faith performance. If the Director determines that the vendor is non-responsible, the Director shall reject that vendor's bid and shall not award the contract to that vendor. A determination of non-responsibility must be evaluated on a case-by-case basis and can only be made after the vendor in question has submitted a bid. A determination of non-responsibility will only extend to the contract for which the vendor has submitted a bid and does not operate as a bar against submitting future bids.

5.4. Suspension.

5.4.1. The Director may suspend, for a period not to exceed 1 year, the right of a vendor to bid on procurements issued by the Purchasing Division or any state spending unit under its authority if:

5.4.1.a. The vendor has submitted a bid and then requested that its bid be withdrawn after bids have been publicly opened.

5.4.1.b. The vendor has exhibited poor performance in fulfilling his or her contractual obligations to the State. Poor performance includes, but is not limited to any of the following: violations of law, regulation, or ordinance; failure to deliver timely; failure to deliver quantities ordered; poor performance reports; or failure to deliver commodities, services, or printing at the quality level required by the contract.

5.4.1.c. The vendor has breached a contract issued by the Purchasing Division or any state spending unit under its authority and refuses to remedy that breach.

5.4.1.d. The vendor's actions have given rise to one or more of the grounds for debarment listed in W. Va. Code § 5A-3-33d.

5.4.2. Vendor suspension for the reasons listed in section 5.4 above shall occur as follows:

5.4.2.a. Upon a determination by the Director that a suspension is warranted, the Director will serve a notice of suspension to the vendor.

5.4.2.b. A notice of suspension must inform the vendor:

5.4.2.b.1. Of the grounds for the suspension;

5.4.2.b.2. Of the duration of the suspension;

5.4.2.b.3. Of the right to request a hearing contesting the suspension;

5.4.2.b.4. That a request for a hearing must be served on the Director no later than 5 working days of the vendor's receipt of the notice of suspension;

5.4.2.b.5. That the vendor's failure to request a hearing no later than 5 working days of the receipt of the notice of suspension will be deemed a waiver of the right to a hearing and result in the automatic enforcement of the suspension without further notice or an opportunity to respond; and

5.4.2.b.6. That a request for a hearing must include an explanation of why the vendor believes the Director's asserted grounds for suspension do not apply and why the vendor should not be suspended.

5.4.2.c. A vendor's failure to serve a request for hearing on the Director no later than 5 working days of the vendor's receipt of the notice of suspension will be deemed a waiver of the right to a hearing and may result in the automatic enforcement of the suspension without further notice or an opportunity to respond.

5.4.2.d. A vendor who files a timely request for hearing but nevertheless fails to provide an explanation of why the asserted grounds for suspension are inapplicable or should not result in a suspension, may result in a denial of the vendor's hearing request.

5.4.2.e. Within 5 working days of receiving the vendor's request for a hearing, the Director will serve on the vendor a notice of hearing that includes the date, time and place of the hearing.

5.4.2.f. The hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the hearing, the Director will issue and serve on the vendor, a written decision either confirming or reversing the suspension.

5.4.3. A vendor may appeal a decision of the Director to the Secretary of the Department of Administration. The appeal must be in writing and served on the Secretary no later than 5 working days of receipt of the Director's decision.

5.4.4. The Secretary, or his or her designee, will schedule an appeal hearing and serve on the vendor, a notice of hearing that includes the date, time and place of the hearing. The appeal hearing will be recorded and an official record prepared. Within 10 working days of the conclusion of the appeal hearing, the Secretary will issue and serve on the vendor a written decision either confirming or reversing the suspension.

5.4.5. Any notice or service related to suspension actions or proceedings must be provided by certified mail, return receipt requested.

5.5. Vendor Debarment. The Director may debar a vendor on the basis of one or more of the grounds for debarment contained in W. Va. Code § 5A-3-33d or if the vendor has been declared ineligible to participate in procurement related activities under federal laws and regulation.

5.5.1. Debarment proceedings shall be conducted in accordance with W. Va. Code § 5A-3-33e and these rules. A vendor that has received notice of the proposed debarment by certified mail, return receipt requested, must respond to the proposed debarment within 30 working days after receipt of notice or the debarment will be instituted without further notice. A vendor is deemed to have received notice, notwithstanding the vendor's failure to accept the certified mail, if the letter is addressed to the vendor at its last known address. After considering the matter and reaching a decision, the Director shall notify the vendor of his or her decision by certified mail, return receipt requested.

5.5.2. Any vendor, other than a vendor prohibited from participating in federal procurement, undergoing debarment proceedings is permitted to continue participating in the state's procurement process until a final debarment decision has been reached. Any contract that a debarred vendor obtains prior to a final debarment decision shall remain in effect for the current term, but may not be extended or renewed. Notwithstanding the foregoing, the Director may cancel a contract held by a debarred vendor if the Director determines, in his or her sole discretion, that doing so is in the best interest of the State. A vendor prohibited from participating in federal procurement will not be permitted to participate in the state's procurement process during debarment proceedings.

5.5.3. If the Director's final debarment decision is that debarment is warranted and notice of the final debarment decision is mailed, the Purchasing Division shall reject any bid submitted by the debarred vendor, including any bid submitted prior to the final debarment decision if that bid has not yet been accepted and a contract consummated.

5.5.4. Pursuant to W.Va. Code § 5A-3-33e(e), the length of the debarment period will be specified in the debarment decision and will be for a period of time that the Director finds necessary and proper to protect the public from an irresponsible vendor.

5.5.5. List of Debarred Vendors. The Director shall maintain and publicly post a list of debarred vendors on the Purchasing Division's website.

5.5.6. Related Party Debarment. The Director may pursue debarment of a related party at the



same time that debarment of the original vendor is proceeding or at any time thereafter that the Director determines a related party debarment is warranted. Any entity that fails to provide the Director with full, complete, and accurate information requested by the Director to determine related party status will be presumed to be a related party subject to debarment.

#### **5.6. Damages.**

5.6.1. A vendor who fails to perform as required under a contract shall be liable for actual damages and costs incurred by the state.

5.6.2. If any commodities delivered under a contract have been used or consumed by a spending unit and on testing the commodities are found not to comply with specifications, no payment may be approved by the Spending Unit for the merchandise until the amount of actual damages incurred has been determined.

5.6.3. The Spending Unit shall seek to collect damages by following the procedures established by the Office of the Attorney General for the collection of delinquent obligations.

#### **Credits**

History: Filed 4-1-19, eff. 4-1-19; Filed 4-16-21, eff. 5-1-21.

Current through register dated May 7, 2021. Some sections may be more current. See credits for details.

W. Va. C.S.R. § 148-1-5, WV ADC § 148-1-5

**End of Document**

© 2021 Thomson Reuters. No claim to original U.S. Government Works.

**EXHIBIT B To:**  
**REQUIRED CONTRACT PROVISIONS FOR NON-FEDERAL ENTITY**  
**CONTRACTS UNDER FEDERAL AWARDS (2 C.F.R. § 200.317):**

**Prevailing Wage Determination**

☐ – Not Applicable Because Contract Not for Construction

☐ – Federal Prevailing Wage Determination on Next Page

## **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

### **Attachment B: Software as a Service Addendum**

Software as a Service Addendum begins on next page.

## Software as a Service Addendum

### 1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

**3. Data Protection and Privacy:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

**4. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) **Incident Response:** The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) **Security Incident Reporting Requirements:** The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) **Breach Reporting Requirements:** Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

**5. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any



type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

**6. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

**7. Termination and Suspension of Service:**

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:
  - 10 days after the effective date of termination, if the termination is in accordance with the contract period
  - 30 days after the effective date of termination, if the termination is for convenience
  - 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

**8. Background Checks:** The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

**9. Oversight of Authorized Persons:** During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

**10. Access to Security Logs and Reports:** The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

**11. Data Protection Self-Assessment:** The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**12. Data Center Audit:** The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**13. Change Control and Advance Notice:** The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

**14. Security:**

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; (3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

**16. Import and Export of Data:** The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

**17. Responsibilities:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

**18. Subcontractor Compliance:** The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

**21. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

**22. Web Services:** The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

**23. Encryption of Data at Rest:** The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

**24. Subscription Terms:** Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

**25. Equitable Relief:** Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: WV DoHS

Signature: Althea Greenhow

Title: Procurement Specialist, Sr

Date: 5/9/2025

Name of Vendor: Elixir Lab USA Inc d/b/a Cardinality.ai

Signature: Ana Harg

Title: Chief Administrative Officer

Date: \_\_\_\_\_

## Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: Elixir Lab USA Inc d/b/a Cardinality.ai

Name of Agency: Department of Human Services

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?  
Yes ☒  
No ☐
2. If yes to #1, does the restricted information include personal data?  
Yes ☒  
No ☐
3. If yes to #1, does the restricted information include non-public data?  
Yes ☒  
No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?  
Yes ☐  
No ☒

5. Provide name and email address for the Department privacy officer:

Name: Chris Snyder

Email address: chris.s.snyder@wv.gov

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: Adam Basha

Email address: adam.basha@cardyai.com

Phone Number: 513-748-0606

## **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

### **Attachment C: Employee Background Check Procedure**

Employee Background Check Procedure begins on next page.



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

## **1.0 PURPOSE**

In accordance with W. Va. Code § 15-2D-3, the Director of the WV Division of Protective Services (DPS) requires all newly hired vendors, contractors, and sub-contractors whose employees are regularly employed on the grounds or in the buildings of the State Capitol complex {this includes all WV Departments of Health (DoH), Health Facilities (DHF), Human Services (DHS), and Office of Shared Administration (OSA) facilities}, or who have access to sensitive and/or confidential data, are required to submit to a fingerprint-based state and federal background check prior to receiving access to State data and/or systems.

This document outlines the procedure all Office of Management Information Services (OMIS) contracted employees must follow when receiving fingerprint-based state and federal background checks, to ensure these investigations are conducted according to established federal and state requirements.

## **2.0 SCOPE**

This procedure applies to all OMIS vendor, contractor, and sub-contractor employees providing services to the State who access, or may potentially access, sensitive and/or confidential data {i.e., protected health information (PHI), personally identifiable information (PII), social security administration (SSA) data, federal tax information (FTI), and/or payment card information (PCI)}.

## **3.0 PROCEDURE**

- 3.1 All OMIS vendors, contractors, and sub-contractors must adhere to the process set forth in Appendix "A" of this procedure, titled *OMIS Vendor/Contractor Background Check and Fingerprinting Procedures*.





**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

- 3.2 Agencies will collaborate, as needed, with the contracting company and DPS to ensure the background check process is applied and administered uniformly, fairly, and without prejudice.
- 3.3 The contracting company will be responsible for all background investigation costs. Payment must be made at the time of the fingerprinting process (see Appendix A).
- 3.4 Background investigations at a minimum, will include the following:
  - 3.4.1 A Federal Bureau of Investigation (FBI) national agency check allows DPS to check the applicant's criminal history in all U.S. states and territories.
  - 3.4.2 A check through local law enforcement in the location(s) the applicant has lived, worked, and/or attended school within the last five (5) years, and if applicable, the appropriate agency for any identified arrests.
  - 3.4.3 Social Security validation, which ensures an applicant's social security number (SSN) is legitimate and finds all names, including aliases and variations, dates of birth and address history associated with the SSN.
  - 3.4.4 Proof of citizenship/residency (i.e., USCIS Form I-9), to validate the applicant is a U.S. citizen or a foreign citizen with the necessary authorization to work in the U.S. (For more information see the following link: <https://www.e-verify.gov>).
- 3.5 All fingerprint-based background checks must be favorably adjudicated prior to allowing the vendor or contractor to access sensitive and/or confidential data.
- 3.6 If the background check does not reveal any type of conviction or disqualifying offense, the DPS will notify the OMIS Compliance and Reporting unit and/or the agency point of contact, as well as the contracting company, that the applicant has



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

passed the background check. In this case, the hiring process or employment status will not be impacted.

- 3.7 Results of unfavorable background checks will be returned to the DPS and treated as confidential. According to federal law, the DPS may only share unfavorable results with the applicant whose background check results in a rejection of employment (i.e., adverse action). Applicants have the right to challenge the accuracy contained in the federal identification record in accordance with state and federal laws and guidelines (see Attachment "A").
- 3.8 Variance/Appeal Process
  - 3.8.1 If the pre-screening process reveals a negative finding, or if the DPS issues a notice of ineligibility, the applicant, or the employer on the applicant's behalf, may file a written request for a variance with the DoH, DHF, DHS and OSA no later than 30-days after the date of the notice. Agencies may grant a variance under the following conditions:
    - (1) Mitigating circumstances surrounding the negative finding or disqualifying offense is provided.
    - (2) DHHR finds that the individual will not pose a danger or threat to residents, members, and their property.
  - 3.8.2 Agencies will mail to the applicant and the contractor a written decision within 90-days of receipt of the request indicating whether a variance has been granted or denied.
  - 3.8.3 If an applicant believes his or her State criminal history record information is incorrect or incomplete, he or she may challenge the accuracy of the record by contacting DPS for a personal review. If the discrepancies are at the charge or final disposition level, the applicant must address this with the court or arresting agency that submitted the record.



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

- 3.8.4 If an applicant believes his or her federal criminal history record information is incorrect or incomplete, he or she may appeal the accuracy of such information by contacting the Federal Bureau of Investigation (FBI) for instructions.
- 3.8.5 If any changes, corrections, or updates are made in the criminal history record information, the DPS will notify the Agency that the applicant has appealed the accuracy of the criminal history records and provide the updated results of the criminal history record information check.
- 3.8.6 If the DPS finds the applicant has intentionally falsified information or misrepresented him/herself in any way (e.g., applicant does not disclose a criminal conviction; fails to provide truthful, accurate, and complete information regarding a criminal conviction(s), etc.) the applicant may be disqualified from hire and/or prohibited from future employment with the State.

**3.9 Provisional Employment**

- 3.9.1 In accordance with §16-46-6 of West Virginia Senate Bill No. 88, a contractor may work on a provisional basis for not more than sixty (60) days pending notification from the DPS regarding the results of the criminal background check only if:
  - (1) The applicant is subject to direct on-site supervision, as specified in rule by the DoH, DHF, DHS and OSA Cabinet Secretaries, during the provisional period; and
  - (2) In a signed statement the applicant must:
    - (A) Affirm that he or she has not committed a disqualifying offense;



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

- (B) Acknowledge that a disqualifying offense reported in the required criminal history record information check shall constitute good cause for termination; and
    - (C) Acknowledge that the contractor may terminate the individual if a disqualifying offense is reported in the background investigation.
  - (3) Provisional contractor employees who have requested a variance will not be required to sign such a statement. A covered contractor may continue to employ an individual if he or she applies for a variance of his or her fitness determination until the variance is resolved.
- 3.10 If the contracting company has conducted state and federal fingerprint-based background checks on its employees within three (3) years of the contract's effective date, a list of authorized staff assigned to the project, as well as results of the checks, must be submitted to the OMIS Director of Compliance and Reporting for review and approval.
- 3.11 Agency contract managers will be responsible for initiating re-investigations for contractors and vendors every three (3) years from the date of their previous background investigations. Agencies have the right to re-screen individuals periodically, consistent with the criticality/sensitivity risk designation of the position.

#### **4.0 ENFORCEMENT**

Violation of this procedure by external entities, including vendors, contractors, and/or consultants, may result in termination of the relationship and/or associated privileges. Violation



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Procedure # OP-35: OMIS Vendor/Contractor  
Employee Background Check Procedure

Revised: February 14, 2024

may also result in civil and criminal penalties as determined by federal and state laws and regulations.

## 5.0 DEFINITIONS

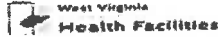
- 5.1 **Adverse Action** - An action companies take based on the information in a background check report that negatively affects applicant's employment. An adverse action letter is a written notice required by federal law, delivered in hard copy or electronic form, that informs a job candidate he or she will not be hired for a particular position because of the findings in a background check.
- 5.2 **Division of Protective Services (DPS)** – Office within the West Virginia Department of Military Affairs and Public Safety created to provide for the safety and security of individuals who visit, conduct business or work at the Capitol Complex and other state facilities.
- 5.3 **Employee** – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of this policy, the term “employee” will include the following: contractors, subcontractors, volunteers, county health department staff, business associates, and any other persons who are determined to be subject to this procedure. This definition does not create any additional rights or duties.
- 5.4 **Federal Tax Information (FTI)** – According to the IRS Publication 1075, FTI is defined as any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.
- 5.5 **Negative Finding** – a finding in the prescreening that excludes an applicant from direct access personnel positions.



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Procedure # OP-35: OMIS Vendor/Contractor  
Employee Background Check Procedure

Revised: February 14, 2024

- 5.6 **Office of Management Information Services (OMIS)** – This office reports directly to the DoH, DHF, DHS and OSA Cabinet Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Agencies.
- 5.7 **Payment Card Industry Data Security Standard (PCI DSS)** – A proprietary information security standard for organizations that handle branded credit cards from the major card schemes.
- 5.8 **Personally Identifiable Information (PII)** - All information that identifies, or can be used to identify, locate, or contact (or impersonate) a particular individual. Personally identifiable information is contained in both public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address, electronic address (including an e-mail address); telephone number or fax number dedicated to contacting the individual at their physical place of residence; social security number; credit and debit card numbers; financial records, including loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints; facial recognition and iris scans; driver identification number; full face image; birth date; birth or adoption certificate number; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet cookie; criminal history, etc. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual, that if disclosed, identifies or can be used to identify a specific individual physically or electronically.
- 5.9 **Protected Health Information (PHI)** - Individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Procedure # OP-35: OMIS Vendor/Contractor  
Employee Background Check Procedure

Revised: February 14, 2024

provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual;
- The provision of health care to an individual; and
- The past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

5.10 **Vendor/Contractor** – See 5.3, definition of Employee

## 6.0 REFERENCES/RELATED MATERIAL

This procedure applies to all relevant federal and state statutes pertaining to the following:

- 6.1 Internal Revenue Service (IRS) Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies; Safeguards for Protecting Federal Tax Returns and Return Information
- 6.2 West Virginia Human Rights Act (WV Code Sec. 5-11-1 et seq.)
- 6.3 WVOT PO1001 – Information Security Policy
- 6.4 OMIS Policy #0512 - Information Security Policy
- 6.5 OMIS Policy #0529 - OMIS Vendor/Contractor Employee Background Checks
- 6.6 Appendix “A” – OMIS Contractor Background Check and Fingerprinting Procedures



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Procedure # OP-35: OMIS Vendor/Contractor**  
**Employee Background Check Procedure**

**Revised: February 14, 2024**

**6.7**    *WV DoH, DHF, DHS and OSA New Contractor/Vendor Employee Checklist*

**7.0**    **REVISION HISTORY**

<b>Version Number</b>	<b>Date</b>	<b>Revisions</b>
Version 1.0	04/26/2021	Original version
Version 1.1	02/01/2022	Converted document from Word to Google Docs; Updated formatting; annual review of content
Version 1.2	02/07/2023	Annual Review; updated policy links
Version 1.3	02/14/2024	Annual Update - changed "DHHR" to "Departments of Health, Health Facilities, Human Services, and Office of Shared Administration", updated links, overall review of content, revised language throughout





State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Procedure # OP-35: OMIS Vendor/Contractor  
Employee Background Check Procedure

Revised: February 14, 2024

**Employee Acknowledgement:**

By signing below, I am acknowledging that I have read, I understand, and will abide by the WV Departments of Health (DoH), Health Facilities (DHF), Human Services (DHS), and Office of Shared Administration (OSA), Office of Management Information Services (OMIS) procedure OP-35, **OMIS Vendor/Contractor Employee Background Check**. I have also been provided a copy of the document. I understand that if I have any questions or concerns related to this or any other policy and/or procedure, I am to bring these to the attention of my immediate supervisor. If my supervisor is unavailable, I will then address these issues with his/her supervisor.

\_\_\_\_\_  
**Print Name**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**

**Supervisor Acknowledgement:**

By signing below, I am acknowledging that the above mentioned employee, has read, understands, and will abide by the OMIS procedure OP-35, **OMIS Vendor/Contractor Employee Background Check**. I have also advised the employee that if any questions or concerns arise regarding this or any other policy and/or procedure, they are to be brought to my attention as soon as possible. If I am unavailable, all issues should then be addressed to my immediate supervisor.

\_\_\_\_\_  
**Print Name**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**

## **REQUEST FOR PROPOSAL**

(Department of Human Services CRFP BSS2500000001)

### **Attachment D: Vendor/Contractor Employee Background Check Policy**

Vendor/Contractor Employee Background Check Policy begins on next page.



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Policy #0529: OMIS Vendor/Contractor**  
**Employee Background Check**

**Revised: February 14, 2024**

## **1.0 PURPOSE**

The WV Departments of Health (DoH), Health Facilities (DHF), Human Services (DHS), and Office of Shared Administration (OSA, Office of Management Information Services (OMIS) is committed to taking meaningful actions to ensure its data, systems, and other assets are properly supported by qualified vendors and contractors. This policy outlines OMIS' guidelines to ensure fingerprint-based state and federal background checks for all contracted employees are conducted according to established standards.

## **2.0 SCOPE**

This policy applies to all DoH, DHF, DHS and OSA vendor, contractor, and sub-contractor employees providing services to the State who access, or may potentially access, sensitive and confidential data {i.e., protected health information (PHI), personally identifiable information (PII), social security administration (SSA) data, federal tax information (FTI), and/or payment card information (PCI)}.

## **3.0 POLICY**

- 3.1 All background checks will be applied and administered uniformly, fairly, and without prejudice.
- 3.2 In accordance with W. Va. Code § 15-2D-3 (e), the Director of the WV Division of Protective Services (DPS) requires any newly hired vendors, contractors, and sub-contractors whose employees are regularly employed on the grounds or in the buildings of the State Capitol complex (this includes all Agency facilities), or who have access to sensitive or critical information, to submit to a fingerprint-based state and federal background check prior to receiving access to use State data and/or systems.



**State of West Virginia**  
**Departments of Health, Health Facilities, and Human Services**  
**Office of Shared Administration**  
**Office of Management Information Services (OMIS)**  
**Policy #0529: OMIS Vendor/Contractor**  
**Employee Background Check**

**Revised: February 14, 2024**

- 3.3 The Agency will work closely with the contracting company and DPS to ensure that each existing vendor, contractor, and sub-contractor with access to sensitive and confidential data receives a complete fingerprint-based state and federal background check. This process is outlined in OMIS Procedure OP-35, *OMIS Vendor and Contractor Employee Background Check Process*.
- 3.4 In accordance with WV State Code, contracting companies will be informed during the contract award process that acceptance of any employee(s) permitted to access PHI, PII, FTI, SSA data, and/or PCI data is contingent upon proof of a favorable background check.
- 3.5 Prior to conducting a background check, a signed, written consent will be obtained from each applicant. Refusal to authorize the background check; failure to disclose a criminal conviction; or failure to provide truthful, accurate, and complete information will render the applicant ineligible for employment with the DoH, DHF, DHS and OSA.
- 3.6 Under certain conditions, a contractor or vendor may work on a provisional basis for not more than sixty days pending notification from the DPS regarding the results of the criminal background check. Additional information is outlined in OMIS Procedure OP-35.
- 3.7 If the contract holder has conducted state and federal fingerprint-based background checks on its employees within three (3) years of the contract's effective date, a list of authorized staff assigned to the project, as well as results of the checks, must be submitted to the DoH, DHF, DHS and OSA bureau or office for review.
- 3.8 Agency contract managers will be responsible for initiating re-investigations for contractors and vendors every three (3) years from the date of their previous background investigations. Agencies have the right to re-screen individuals



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

periodically, consistent with the criticality/sensitivity risk designation of the position.

#### 4.0 ENFORCEMENT

Violation of this policy by external entities, including vendors, contractors, and/or consultants, may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

#### 5.0 DEFINITIONS

- 5.1 **Confidential Data** – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.
- 5.2 **Contractor** – Contractors include, but are not limited to, information providers, information processors, and other organizations that provide information system development, information technology services, consumer assistance, AE business functions, and other outsourced applications, roles, and functions.
- 5.3 **Employee** – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of this procedure, the term “employee” will include the following: contractors, subcontractors, contractors’ employees, volunteers, county health department staff, business associates, and any other persons who are determined to be subject to this procedure. This definition does not create any additional rights or duties.
- 5.4 **Federal Tax Information (FTI)** – According to the IRS Publication 1075, FTI is defined as any return or return information received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.

- 5.5 **Office of Management Information Services (OMIS)** – This office reports directly to the DoH, DHF, DHS and OSA Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Agencies.
- 5.6 **Payment Card Industry Data Security Standard (PCI DSS)** – A proprietary information security standard for organizations that handle branded credit cards from the major card schemes.
- 5.7 **Personally Identifiable Information (PII)** - All information that identifies, or can be used to identify, locate, or contact (or impersonate) a particular individual. Personally identifiable information is contained in both public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address, electronic address (including an e-mail address); telephone number or fax number dedicated to contacting the individual at their physical place of residence; social security number; credit and debit card numbers; financial records, including loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints; facial recognition and iris scans; driver identification number; full face image; birth date; birth or adoption certificate number; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet cookie; criminal history, etc. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual, that if disclosed, identifies or can be used to identify a specific individual physically or electronically.



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

**5.8 Protected Health Information (PHI)** - Individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual;
- The provision of health care to an individual; and
- The past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

**5.9 Sensitive Data** – This includes safeguarded information or anything the organization, its employees, customers, or contractors would expect to be private and protected. Direct access is limited to authenticated and authorized individuals who require access to that information in the course of performing their job duties. Examples include: most data in employee records, employment and training program data, historical records repository data, client-specific data, etc.

## 6.0 REFERENCES/RELATED MATERIAL

- 6.1 Internal Revenue Service (IRS) Publication 1075 – Tax Information Security Guidelines for Federal, State, and Local Agencies; Safeguards for Protecting Federal Tax Returns and Return Information
- 6.2 WV State Code § 15-2D-3 (e) - Duties and Powers of the Director and Officers
- 6.3 West Virginia Human Rights Act (WV Code Sec. 5-11-1 et seq.)



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

- 6.4 WVOT-PO1001 – *Information Security Policy*
- 6.5 WVOT-PO1006 – *Data Classification*
- 6.6 OMIS Policy 0512 - *Information Security Policy*
- 6.7 OMIS Procedure #OP-35 – OMIS Vendor/Contractor Employee Background Check Procedure
- 6.8 Appendix “A” – OMIS Contractor Background Check and Fingerprinting Procedures
- 6.9 *WV DoH, DHF, DHS and OSA New Contractor/Vendor Employee Checklist*





State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

## 7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	04/26/2021	Original Version
Version 1.1	02/01/2022	Converted document from Word to Google Docs; Updated formatting; annual review of content
Version 1.2	02/07/2023	Annual Review; updated links
Version 1.3	02/14/2024	Annual Update - changed "DHHR" to "Departments of Health, Health Facilities, Human Services, and Office of Shared Administration", updated links, overall review of content, revised language throughout



State of West Virginia  
Departments of Health, Health Facilities, and Human Services  
Office of Shared Administration  
Office of Management Information Services (OMIS)  
Policy #0529: OMIS Vendor/Contractor  
Employee Background Check

Revised: February 14, 2024

**Employee Acknowledgement:**

By signing below, I am acknowledging that I have read, understand, and will abide by the WV Departments of Health (DoH), Health Facilities (DHF), Human Services (DHS), and Office of Shared Administration (OSA), Office of Management Information Services (OMIS) policy #0529, **OMIS Vendor/Contractor Employee Background Check**. I have also been provided a copy of the document. I understand that if I have any questions or concerns related to this or any other policy and/or procedure, I am to bring these to the attention of my immediate supervisor. If my supervisor is unavailable, I will then address these issues with his/her supervisor.

\_\_\_\_\_  
**Print Name**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**

**Supervisor Acknowledgement:**

By signing below, I am acknowledging that the above mentioned employee, has read, understands, and will abide by the OMIS policy #0529, **OMIS Vendor/Contractor Employee Background Check**. I have also advised the employee that if any questions or concerns arise regarding this or any other policy and/or procedure, they are to be brought to my attention as soon as possible. If I am unavailable, all issues should then be addressed to my immediate supervisor.

\_\_\_\_\_  
**Print Name**

\_\_\_\_\_  
**Signature**

\_\_\_\_\_  
**Date**