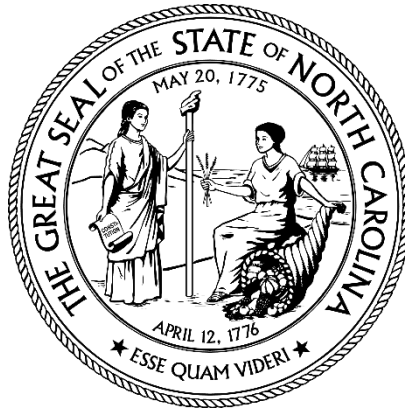




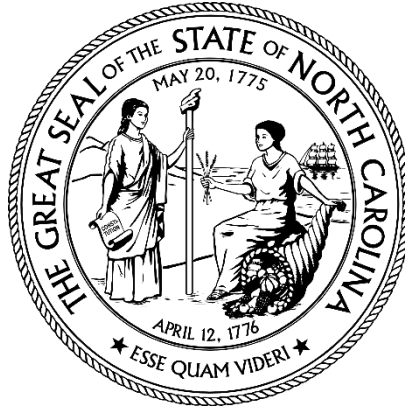
STATE OF NORTH CAROLINA

Department of Health and Human Services

Division of Health Benefits

Request for Proposal #30-2025-037-DHB

Contract Lifecycle Management System



STATE OF NORTH CAROLINA

Request for Proposal

#30-2025-037-DHB

For internal State agency processing, please provide your company's Federal Employer Identification Number or alternate identification number (e.g., Social Security Number). Pursuant to North Carolina General Statute 132-1.10(b) this identification number shall not be released to the public. **This page will be redacted** before the procurement file is made available for public inspection.

This page is to be filled out and returned with your Proposal.

ID Number:

Federal ID Number or Social Security Number

Offeror Name



STATE OF NORTH CAROLINA
Department of Health and Human Services

Refer ALL Inquiries regarding this RFP to:

Michael.c.brown@dhhs.nc.gov
Kevin.barlage@dhhs.nc.gov
Medicaid.Procurement@dhhs.nc.gov

Request for Proposal # 30-2025-037-DHB

Date RFP Issued/Posted: August 19, 2026

Date RFP Submissions due to the Department: at 2:00 p.m. EST

Proposals will be opened: October 23, 2026

Contract Type: Open Market

Commodity Number: 811620 - Cloud-based software as a service

Description: Contract Lifecycle Management System Solution

Using Agency: Department of Health and Human Services, Division of Health Benefits

Requisition No.: N/A

EXECUTION

In compliance with this Request for Proposal (RFP), and subject to all the conditions herein, the undersigned Offeror offers and agrees to furnish and deliver any or all services proposed, at the cost proposed and within the time specified herein. By executing this proposal, the Offeror confirms it has read, understands, and will comply with all specifications and requirements in the RFP and any addenda in the event of contract award. By executing this proposal, the undersigned Offeror certifies that this proposal is submitted competitively and without collusion (N.C. Gen. Stat. § 143-54), that none of its officers, directors, or owners of an unincorporated business entity has been convicted of any violations of Chapter 78A of the General Statutes, the Securities Act of 1933, or the Securities Exchange Act of 1934 (N.C. Gen. Stat. § 143-59.2), and that it is not an ineligible Contractor as set forth in N.C. Gen. Stat. § 143-59.1. False certification is a Class I felony. Furthermore, by executing this proposal, the undersigned certifies to the best of Offeror's knowledge and belief, that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible or voluntarily excluded from covered transactions by any Federal or State department or agency. As required by N.C. Gen. Stat. § 143-48.5, the undersigned Offeror certifies that it, and each of its subcontractors, for any Contract awarded as a result of this RFP, complies with the requirements of Article 2 of Chapter 64 of the NC General Statutes, including the requirement for each employer with more than 25 employees in North Carolina to verify the work authorization of its employees through the Federal E-Verify system. N.C. Gen. Stat. § 133-32 and Executive Order 24 (2009) prohibit the offer to, or acceptance by, any State Employee associated with the preparing plans, specifications, estimates for public Contract; or awarding or administering public Contracts; or inspecting or supervising delivery of the public Contract of any gift from anyone with a Contract with the State, or from any person seeking to do business with the State. By executing this proposal, you attest, for your entire organization and its employees or agents, that you are not aware that any such gift has been offered, accepted, or promised by any employees of your organization. **Failure to execute/sign proposal prior to submission shall render proposal invalid and it WILL BE REJECTED. Late proposals will not be accepted.**

OFFEROR:		
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY & STATE & ZIP:	TELEPHONE NUMBER:	TOLL FREE TEL. NO:
PRINCIPAL PLACE OF BUSINESS ADDRESS IF DIFFERENT FROM ABOVE		
PRINT NAME & TITLE OF PERSON SIGNING ON BEHALF OF OFFEROR:		FAX NUMBER:
OFFEROR'S AUTHORIZED SIGNATURE:	DATE:	EMAIL:

Offer valid for at least **240** calendar days from date of proposal opening unless extended by the State in writing. After this time, any withdrawal of offer shall be made in writing, effective upon receipt by the agency issuing this RFP.

ACCEPTANCE OF RESPONSE

If any or all parts of this proposal are accepted by the State of North Carolina, an authorized representative of the Department of Health and Human Services shall affix his/her signature hereto and this document and all provisions of this Request for Proposal along with the Offeror's proposal, and the written results of any negotiations shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the successful Offeror.

FOR STATE USE ONLY: Offer accepted and Contract awarded this ____ day of _____, 20____, by

(Authorized Representative of NC Department of Health and Human Services)

Table of Contents

1.0	General Procurement Information and Notice to Offerors	6
1.1	Important Notices	6
1.2	Procurement Information	6
1.3	Request for Proposal Functionality and Related Notices	7
1.4	Schedule and Important Events	8
2.0	Purpose of RFP	9
2.1	Introduction	9
2.2	Contract Term	10
2.3	Contract Type	10
2.4	Agency Background	10
3.0	RFP Requirements and Specifications	11
3.1	Scope Of Work	11
3.2	General Requirements and Specifications	16
3.3	Security Specifications	17
3.4	Enterprise Specifications	19
3.5	Business and Technical Requirements	20
3.6	Business and Technical Specifications	28
3.7	Option Requirements and Specifications	33
4.0	Cost of Vendor's Offer	34
4.1	Offer Costs	34
4.2	Payment Schedule	35
5.0	Evaluation	35
5.1	Source Selection	35
5.2	Evaluation Criteria	36
5.3	Best and Final Offers (BAFO)	37
5.4	Possession And Review	37
5.5	Competitive Range	37
5.6	Solution Demonstrations	37
6.0	Vendor Information and Instructions	38
6.1	General Conditions of Offer	38
6.2	General Instructions for Vendor	40
6.3	Instructions for Offer Submission	42
7.0	Other Requirements and Special Terms	46
7.1	Vendor Utilization Of Workers Outside of U.S.	46
7.2	Financial Statements	46
7.3	Financial Resources Assessment, Quality Assurance, Performance and Reliability	47
7.4	Vendor's License or Support Agreements	47
7.5	Resellers - Reserved	47
7.6	Disclosure Of Litigation	47
7.7	Criminal Conviction	48
7.8	Security and Background Checks	48

7.9 Assurances.....	48
7.10 Confidentiality of offers.....	49
7.11 Project Management.....	49
7.12 Meetings.....	50
7.13 Recycling and Source Reduction - Reserved.....	50
7.14 Special Terms And Conditions.....	50
7.15 Technical Operations.....	53
7.16 Help Center.....	54
7.17 Testing.....	55
Attachment A: Definitions.....	57
Attachment B: Department of Information Technology Terms and Conditions.....	66
Section 1: General Terms and Conditions Applicable to All Purchases.....	66
Section 2: Terms and Conditions Applicable to Information Technology Goods and Services.....	77
Section 3: Terms and Conditions Applicable to Personnel and Personal Services.....	80
Section 4: Software as a Service (SaaS) Terms and Conditions.....	82
Attachment C: Agency Terms and Conditions.....	91
Section 1: DHHS Department of Health Benefits (DHB).....	91
Section 2: DHHS Privacy and Security Office (PSO).....	102
Section 3: NCDHHS Development of Artificial Intelligence Systems.....	106
Attachment D: Description of Offeror.....	111
Attachment E: Cost Form.....	112
Attachment F: Vendor Certification Form.....	122
Attachment G: Location of Workers Utilized by Vendor – Disclosure Statement.....	123
Attachment H: Vendor References/Past Performance.....	125
Attachment I: Financial Review Form.....	130
Attachment J: Enterprise Architecture.....	132
Attachment K: Vendor Key Personnel.....	134
Attachment L: Service Level Agreements.....	137
Attachment M: Contract Administrators.....	144
Attachment N: Deliverables And Milestones Schedule.....	146
Attachment O: Business Continuity Plan.....	153
Attachment P: Disaster Recovery Plan.....	155
Attachment Q: State Certifications.....	158
Attachment R: Federal Certifications and Disclosures.....	160
Attachment S: Business Associate Agreement.....	167
Attachment T: Technical / Management Proposal.....	171
Attachment U: Conceptual Architectural Diagrams.....	173
Attachment V: Medicaid Integration Services Core Capabilities.....	174
Attachment W: Work Products.....	179
Attachment X: Request for Proposed Modifications to The Terms and Conditions.....	184
Attachment Y: Minimum Qualifications.....	185
Attachment Z: Subcontractor Identification Form.....	187
Attachment AA: Acquisition Lifecycle Reports.....	189
Attachment AB: Interfaces – RESERVED.....	191
Attachment AC: GenAI Disclosure and Fact Sheet.....	192

1.0 GENERAL PROCUREMENT INFORMATION AND NOTICE TO OFFERORS

1.1 IMPORTANT NOTICES

Offerors are Cautioned to Read Carefully

1.1.1 READ, REVIEW, AND COMPLY

It shall be the Offeror's responsibility to read this entire document, review all enclosures and attachments, and any addenda thereto, and comply with all requirements specified herein, regardless of whether appearing in these Instructions to Offerors or elsewhere in this RFP document.

1.1.2 EXECUTION OF PROPOSAL

Failure to sign the Execution Page in the indicated space and return all attachments, tables, charts, exhibits, diagrams, and appendices completed and signed where required shall render the proposal non-responsive.

1.1.3 RESULTING CONTRACT

Under the State's procurement process, any contract resulting from this RFP will consist of the RFP and the Offeror's response, along with any addenda to the RFP, written Clarifications, System Demonstration, Best and Final Offers (BAFO), and negotiation documents. The Contractor will be obligated to perform services as proposed in its offer, unless otherwise modified by Clarification, BAFO, negotiation, or Contract amendment, or superseded by a document with higher order of precedence. See *Attachment C: Agency Terms and Conditions, Section 1, Paragraph 14 Entire Agreement and Order of Precedence*, of this document for more information and the order of precedence of the contract documents. See section 1.3 Request for Proposal Functionality and Related Notices in this section for more information on the RFP, changes in specifications, and instructions regarding modifications to the terms and conditions.

1.1.4 POTENTIAL NEGOTIATIONS

The Department reserves the right to enter into negotiations with one or more Offerors to establish a contract that is in the best interest of the Department. Negotiations are specific to each Offer and shall be conducted to maximize the State's ability to obtain the most advantageous offer based on the evaluation factors set forth in the RFP. Such negotiations are at the Department's sole discretion and may result in modifications to the RFP and/or Offeror's proposal/response to the RFP.

1.1.5 EVENTS AND DEADLINES

- a. **Pre-proposal Conference** will be hosted by the Department on the date and time indicated in the RFP Schedule in Section 1.4.1.
- b. **Questions** concerning this RFP must be submitted in writing by the date and time indicated in the RFP Schedule in Section 1.4.1.
- c. **Submission of Proposals** will be accepted until the date and time indicated in the RFP Schedule in Section 1.4.1.

1.2 PROCUREMENT INFORMATION

1.2.1 INFORMATION AND DESCRIPTIVE LITERATURE

The Offeror shall furnish all information requested as part of this RFP. Each Offeror shall submit detailed information with their proposal (e.g., narratives, diagrams, exhibits, examples, sketches, descriptive literature, complete specifications) to support the services and products offered

1.2.2 MISCELLANEOUS

Pronouns, whether masculine, feminine, or gender-non-specific, shall be read to be inclusive of all genders and shall be read to include the plural and vice versa.

1.2.3 INFORMAL COMMENTS

The Department shall not be bound by informal explanations, instructions or information given at any time by anyone on behalf of the Department prior to or during the competitive process or after award, including but not limited to policy papers or any written or verbal statements whatsoever made outside of this RFP and any formal Addenda issued herewith. The Department is bound only by information provided in this RFP and in formal Addenda issued

1.2.4 OFFEROR'S REPRESENTATIVE

Each Offeror shall submit with its proposal the name, title, email address, physical address, and telephone number of the person(s) with authority to bind the Offeror and answer questions or provide clarification concerning the Offeror's proposal. This information must be included in the Offeror's proposal and response

1.2.5 INSPECTION AT OFFEROR'S SITE - RESERVED

1.3 REQUEST FOR PROPOSAL FUNCTIONALITY AND RELATED NOTICES

1.3.1 RFP FUNCTIONALITY

- a. This RFP serves two functions:
 - i. Define the specifications of the Solution sought by the Department; and
 - ii. Provide the requirements and terms and conditions of any contract resulting from this procurement.
- b. All Terms and Conditions in this RFP shall be enforceable. The use of phrases such as "*shall*", "*will*", "*must*", "*required*", and "*requirements*" are intended to create enforceable Contract conditions. In determining whether proposals should be evaluated or rejected, the Department will take into consideration the degree to which the Offeror has proposed or failed to propose solutions that are responsive to the Department's needs as described in this RFP.

1.3.2 NOTICES REGARDING RFP AND TERMS AND CONDITIONS

- a. It is the Offeror's responsibility to read all instructions, terms and conditions, specifications, requirements, attachments and appendices, and any other components made a part of this RFP and comply with all instructions and directives. The Offeror is responsible for obtaining and complying with all addenda and other changes that may be issued relating to this RFP.
- b. All questions and issues regarding any term, condition, instruction, or other component within this RFP must be submitted in accordance with Section 6.2.2. Questions Regarding this RFP. If the Department determines that any changes will be made because of the questions asked, then such decisions will be communicated in the form of an Addendum posted on the North Carolina electronic Vendor Portal (NC eVP). The Department may also elect to leave open the possibility for later negotiation and amendment of specific provisions of the Contract that have been raised during the question-and-answer period. Other than through this process, and except as provided in Section 1.3.3 Proposed Modifications to Terms and Conditions, the Department rejects and will not be required to evaluate or consider any additional or modified terms and conditions submitted with Offeror's proposal. This applies to any language appearing in or attached to the RFP document as part of the Offeror's proposal that purports to vary any terms and conditions, or Offeror's Instructions therein to render the proposal non-binding or subject to further negotiation.

- c. The Offeror's proposal to this RFP shall constitute a firm offer. **By execution and delivery of a proposal to this RFP, the Offeror agrees that any additional or modified terms and conditions, whether submitted purposely or inadvertently, or any purported condition to the offer, shall have no force or effect, and will be disregarded. Noncompliance with, or any attempt to alter or delete, this paragraph shall constitute sufficient grounds to reject the Offeror's proposal.**

1.3.3 PROPOSED MODIFICATIONS TO TERMS AND CONDITIONS

- a. Offerors are urged and cautioned to inquire during the question period, in accordance with the instructions in this RFP, about whether specific language proposed as a modification is acceptable to or will be considered by the Department.
- b. Identification of objections or exceptions to the terms and conditions in the proposal itself shall not be allowed and shall be disregarded or the proposal rejected.
- c. If the Offeror wishes to suggest changes to any of the terms and conditions included In Attachments B and C of this RFP, those must be submitted in Attachment X: Request for Proposed Modifications to the Terms and Conditions. The Department, in its sole discretion, may consider any proposed modifications identified by the Offeror. Where necessary, any modification(s) to the terms and conditions agreed upon by the Department may be incorporated as part of an Addendum to the RFP, BAFO, negotiation document, Execution of Contract, or Contract Amendment after award. Other than through this process, the Department rejects and shall not be required to evaluate or consider any additional or modified terms, conditions, or instructions included in the Offeror's proposal.

1.3.4 CHANGES IN REQUIREMENTS AND SPECIFICATIONS

- a. The Offeror is cautioned that the requirements of this RFP can only be altered by written Addendum issued or other documents issued by the Department as described in this RFP, and that oral or emailed communications from whatever source(s) are of no effect.
- b. Any modification to specifications will be specified in an Addendum which shall be posted to the NC eVP prior to the opening of proposals or through Negotiation after opening the proposals.

1.4 SCHEDULE AND IMPORTANT EVENTS

1.4.1 ANTICIPATED PROCUREMENT SCHEDULE

The Department will make every effort to adhere to the schedule detailed below in Table 1 – RFP Schedule. The Department reserves the right to adjust the schedule and will post an Addendum on the NC eVP website for any schedule changes occurring prior to the opening of proposals.

Action	Responsible Party	Due Date	Time (ET)
RFP Issued	Department	August 19, 2026	
Register for Pre-Proposal Conference	Offeror(s)	August 21, 2026	10:00 am
Pre-Proposal Conference	Offeror(s) and Department	August 24, 2026	2:00 pm
Written Questions Deadline	Offeror(s)	August 31, 2026	2:00 pm
Agency's Response to Written Questions / RFP Addendum Issued	Department	September 28, 2026	

Action	Responsible Party	Due Date	Time (ET)
Proposals Due	Offeror(s)	October 23, 2026	2:00 pm
Proposals Evaluation Begins	Department	October 26, 2026	
System Demonstrations	Offeror(s)	December 11, 2026	
Estimated Contract Award	Department	March 19, 2026	
Protest Deadline	Responding Vendors	15 days after award	

Table 1 – RFP Schedule

1.4.2 PRE-PROPOSAL CONFERENCE

- a. The Department will hold a Pre-proposal virtual Conference on the date and time indicated in the RFP Schedule in Section 1.4.1 for one hour via Microsoft (MS) Teams. No purchase is required to use the MS Teams app.
- b. The purpose of the conference is to allow the Department to review key priorities and objectives of the RFP and to review the submission requirements and instructions.
- c. While attendees may ask questions at the Pre-proposal Conference, the Department is not required to respond during the conference. The Department will respond to written questions per the process described in this RFP.
- d. Potential Offerors are not required to attend the Pre-proposal Conference in order to submit responses to this RFP; however, they are urged and cautioned to attend the Pre-proposal Conference to apprise themselves of the conditions and requirements of the submission.
- e. To ensure receipt of the video conference invite and instructions for participation, interested parties are required to pre-register for the conference by sending an email to Medicaid.Procurement@dhhs.nc.gov stating the name of the potential Offeror, the names and email addresses of representatives who will attend, the current title or role of each representative, and requests for a sign language interpreter or other accommodations. Interested parties must pre-register at this email address by the date and time indicated in the RFP Schedule in Section 1.4.1.
- f. The Department limits the number of representatives attending on behalf of each Offeror or organization to two (2) representatives to ensure adherence to videoconference capacity limits.
- g. Audio and video recording will not be permitted. Statements and materials discussed at the conference are informational only, are not binding upon the Department and do not replace reading, reviewing and complying with this RFP.
- h. Attendees will be required to announce their name or otherwise confirm their presence via a roll call during the video conference.

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The North Carolina Department of Health and Human Services (“NCDHHS” or “Department”), through its Division of Health Benefits (“DHB”), is seeking to procure a comprehensive Contract Lifecycle Management System (CLMS) software solution, including ongoing support and maintenance. This solution will serve as

a centralized platform for managing the full lifecycle of contracts, from initiation through closeout, while enhancing transparency, accountability, and operational efficiency.

To effectively support the evolving and expanding contracting environment, the Department requires a robust, scalable CLMS that integrates contract management, vendor oversight, and performance monitoring into a unified, interoperable solution. The system must align with existing state technologies and enable efficient, end-to-end contract operations across all phases of the contract and vendor management lifecycles.

The estimated number of associates requiring access to this solution is provided in the following table:

Role	Description	Est. Number
Administrators	Have full control over the system (Configuration and Security setup)	10
Content Editor	Creates, edits, and submits content for review	50
Approver	Reviews and approves content	100
Subscriber	Only views published content	250

2.2 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The initial term shall be five (5) years unless otherwise stated in the Notice of Award or unless otherwise terminated in accordance with the Contract. After the initial term, the State shall have the option to extend the Contract for two (2) additional one-year periods at its sole discretion. Each year that the Contract remains in effect shall be a “Contract Year.” The Department will give the Contractor written notice of its intent whether to exercise each option year no later than thirty (30) Calendar Days before the end of the Contract’s current term.

2.2.1 EFFECTIVE DATE

This solicitation, including any Exhibits or any resulting contract or amendment, shall not become effective nor bind the State until the appropriate State purchasing authority / official or Agency official has signed the document(s), contract, or amendment; the effective award date has been completed on the document(s) by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for goods provided nor Services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.3 CONTRACT TYPE

Definite Quantity Contract - This request is for a closed-ended contract between the awarded Vendor and the State to furnish a predetermined quantity of goods or services during a specified period of time.

The State reserves the right to make partial, progressive, or multiple awards where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; and where other factors are deemed to be necessary or proper to the purchase in question.

2.4 AGENCY BACKGROUND

The North Carolina Department of Health and Human Services (DHHS or the Department) is responsible for the delivery of health and human services to all North Carolinians, with a particular focus on the state’s

most vulnerable populations, including children, older adults, individuals with disabilities, those with behavioral health needs, and low-income families. As one of the largest and most complex agencies in the state, DHHS employs approximately 18,000 individuals and works collaboratively with health care professionals, community leaders, advocacy groups, and local, state, and federal partners to fulfill its mission.

In partnership with these stakeholders, DHHS is committed to protecting the health and safety of all North Carolinians while providing access to essential, individualized, and compassionate care. The Department serves populations with complex needs, including individuals with developmental disabilities, substance use disorders, and serious mental illness, particularly when care needs exceed the capacity of community-based services. DHHS supports these individuals in achieving greater independence and improved quality of life.

Within DHHS, the Division of Health Benefits (DHB or NC Medicaid) administers the state's Medicaid program, providing access to physical and behavioral health services for more than 3.1 million residents across North Carolina. These include low-income parents, children, seniors, and individuals with disabilities. NC Medicaid plays a vital role in improving health outcomes and promoting well-being statewide.

To support this mission, CMPU is responsible for the full lifecycle management of contracts that underpin Medicaid operations. This includes contract development, administration, oversight, monitoring, and eProcurement. The Unit is organized into six functional areas:

1. Medicaid Operational Contracting – Non-IT
2. Managed Care Contracting
3. Technology and Medicaid Enterprise System (MES) Contracting
4. Technology Monitoring and Compliance
5. Contract Monitoring and Oversight – Non-IT
6. eProcurement

These functional areas work in concert with DHB leadership, program teams, and external stakeholders to ensure effective contract execution and vendor performance throughout the contract and vendor management lifecycle. Through its work, CMPU plays a critical role in enabling the delivery of high-quality, efficient, and coordinated services to Medicaid beneficiaries statewide.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 SCOPE OF WORK

The CLMS entity ("Contractor") shall provide a software solution, along with support and maintenance, to implement a comprehensive Contract Lifecycle Management System (CLMS) to support the full lifecycle of contracts managed by CMPU. This system will serve as a centralized solution to improve efficiency, consistency, and transparency across all contracting activities.

3.1.1 OBJECTIVES OF A CLMS

The Department seeks a qualified Contractor with the experience, expertise, and resources necessary to provide a comprehensive CLMS solution. The primary objectives of this procurement are to:

3.1.1.1 Centralize and streamline all contract management activities across the Division of Health Benefits (DHB). The solution includes contract artifacts such as:

- Requests for Proposal (RFP)
- Requests for Information (RFI)
- Requests for Qualification (RFQ)
- Requests for Quote (RFQ)

- Invitations for Bid (IFB)
- Memorandums of Agreement (MOA)
- Memorandums of Understanding (MOU)
- Data Sharing Agreements (DSA)
- Data Use Agreements (DUA)
- Sole Source Agreements
- Non-Disclosure Agreements (NDA)
- Contract Amendments
- Letters of Extension (LOE)
- Notices of Extension (NOE)
- Letters of Intent (LOI)
- Master Service Agreements (MSA)
- Task Orders (TO)
- Notices of Deficiency (NOD)
- Notices of Concern (NOC)
- Other Agreements
- Internal Templates and Forms

3.1.1.2 Improve vendor performance tracking and contract oversight.

3.1.1.3 Enhance interoperability with existing state systems and workflows as outlined in *Attachment U: Conceptual Architectural Diagrams*.

3.1.1.4 Support current and future Medicaid transformation initiatives impacting procurement.

The selected Contractor must deliver a solution that enables greater efficiency, transparency, and accountability throughout the contract and vendor management lifecycle, while aligning with the Department's strategic goals and regulatory requirements.

3.1.2 SOLUTION ARCHITECTURE – CONTRACT DEVELOPMENT, REPOSITORY, AND MONITORING

The following outlines the Department's need for a secure, integrated digital CLMS solution, supporting the full spectrum of contract development, repository management, and post-award contract monitoring. The solution should empower authorized users with advanced tools to streamline workflows, enforce compliance, and increase operational visibility. This solution shall provide a comprehensive, user-friendly, and secure platform to manage all aspects of contract lifecycle management from development and repository storage to post-award monitoring. Through seamless integration, workflow automation, advanced analytics, and compliance tracking, it enhances organizational efficiency, mitigates risk, and supports governance throughout the contracting process.

3.1.2.1 Contract Development

Provide a secure, role-based digital environment for managing the complete contract creation lifecycle, including drafting, redlining, obtaining approvals, and collaboration. Role-based access ensures that contracting, legal, and business stakeholders can engage in contract development based on their responsibilities. The platform supports:

- Real-time collaboration and document versioning with integrated tools such as MS Office, SharePoint, and DocuSign.
- Flexible use of clause libraries and templates, including support for Federal and State-specific language.
- Automated metadata population and change tracking with conformed document views.
- Seamless integration with the central contract repository.

Provide an intuitive user interface to support centralized contract intake, review workflows, template administration, and modular document construction. Dashboards provide real-time contract statuses, notifications, and ad-hoc reporting capabilities. Users can restore previous versions, lock/unlock drafts, compare document versions, and upload multiple artifacts with ease.

To facilitate oversight and accountability, the solution should include full audit trails, change history, and automated alerts tied to key milestones and events. Approvers can view approval chains and access contracts directly from notifications. Additionally, it supports the creation and management of amendments through predefined templates and workflows.

To further enhance contract quality, the solution includes tools to analyze third-party contract language for deviations from standard terms. Risk indicators and PDF scanning capabilities help identify non-compliant clauses and support ingestion of external vendor templates.

3.1.2.2 Contract Repository

Provide a centralized contract repository that delivers secure, role-based access to all current and expired contracts, amendments, and supporting documentation. Users can manage and search contract files in a variety of formats, with support for uploads exceeding 100 MB. Metadata is automatically updated with changes or amendments, and documents can be linked from pre-award to post-award.

A customizable dashboard offers visibility into contract status, key dates, and reporting metrics. Users can upload multiple documents simultaneously and create tailored reports. Advanced search functionality enables clause-level identification of deviations and tracking across multiple file types.

The repository maintains full version control and historical logs of contract activity. Users receive timely alerts for upcoming contract terminations, renewals, or other required actions. Post-award management includes capabilities for contract closeout and lifecycle tracking.

3.1.2.3 Contract Monitoring – Analytics and Reporting

Provide a solution that includes robust contract monitoring features, ensuring visibility and compliance throughout the post-award phase of the contract lifecycle. Authorized users can access monitoring documents and activities, and business users can actively participate in compliance tracking. Integration with external systems, such as SharePoint, enables seamless monitoring and documentation.

- Automated alerts notify users of deliverables, business reviews, SLAs, and other critical events. Direct links within notifications guide users to relevant contract documents.
- Monitoring is supported by interactive dashboards, approval workflows, and performance metrics management. Users can configure and track KPIs, SLAs, and deliverables to evaluate vendor performance. Insights into key contract obligations, milestones, and costs (including invoice tracking and transition costs) are readily available.
- Enables the upload of monitoring plans and status updates, ensuring clear and continuous visibility into contract compliance.

3.1.3 KEY FUNCTIONAL REQUIREMENTS OF CLMS

The Department requires a Contractor with demonstrated experience, knowledge, and resources to provide a robust and scalable CLMS. The solution must support the complex and evolving needs of the DHB and offer comprehensive capabilities across the full contract and vendor management lifecycle. This CLMS solution must be designed to be secure, scalable, user-friendly, and highly integrated, providing end-to-end contract management, vendor oversight, workflow automation, and robust reporting. The solution shall also ensure compliance, streamline contract processes, and

improve contract performance tracking across the entire lifecycle. At a minimum, the CLMS must include the following key functional requirements:

3.1.3.1 Cloud-Based and SaaS Solution

The CLMS shall be delivered as a cloud-based Software-as-a-Service (SaaS) solution to ensure continuous availability, flexible access, and the ability to scale with the Department's operational demands without requiring internal infrastructure management.

3.1.3.2 End-to-End Contract Management

The system shall support the full contract and vendor management lifecycle, including initiation, development, negotiation, execution, amendments, renewals, monitoring, closeout and eProcurement, to enable comprehensive and consistent contract management from start to finish.

3.1.3.3 Scalability and Integration

The CLMS shall be scalable to accommodate increasing contract volume and complexity, and shall integrate with existing systems such as:

- DocuSign
- MS Office 365
- Adobe or equivalent
- MS SharePoint

Additionally, this solicitation includes two separate Options to Award the integration with the following systems:

- ServiceNow: A cloud-based workflow automation platform that enables organizations to streamline and manage digital workflows across departments such as IT, HR, procurement, and finance. Integration with ServiceNow allows for improved ticketing, approval workflows, and process automation related to contract lifecycle activities.
- North Carolina Financial System (NCFS): The State's enterprise resource planning (ERP) system used for financial management, accounting, budgeting, and procurement. Integration with NCFS supports seamless financial data exchange, contract payment tracking, and compliance with State financial reporting requirements.

3.1.3.4 Vendor Management and Oversight

The system shall include tools for vendor performance monitoring, risk assessment, and compliance tracking to support proactive oversight and ensure vendors meet contractual obligations.

3.1.3.5 Workflow Automation

The CLMS shall automate key processes such as approvals, modifications, renewals, and compliance monitoring through configurable workflows to reduce manual effort and promote timely, consistent execution of contract actions.

3.1.3.6 High Availability

The system shall maintain 99.9% uptime and support recovery within one (1) hour to ensure uninterrupted access to contract management functions and minimize operational disruptions.

3.1.3.7 Secure Digital Environment

The CLMS shall provide a secure digital environment with role-based access controls for contract development, approval, and storage to protect sensitive data and maintain compliance with privacy and security standards.

3.1.3.8 Intuitive User Interface (UI)

The system shall feature an intuitive, user-friendly interface that supports contract development, reporting, dashboards, workflows, and document management to promote ease of use and efficient task execution by a diverse user base.

3.1.3.9 Document Change Tracking and Version Control

The CLMS shall include document version control and change tracking, with automated notifications for key milestones and updates, to ensure transparency and accountability throughout the contract lifecycle.

3.1.3.10 Contract Amendment and Collaboration

The system shall support collaborative contract development and approval of contract amendments through built-in workflows, to ensure all stakeholders are engaged and changes are properly documented and authorized.

3.1.3.11 External Party Language Analysis

The CLMS shall analyze third-party contract language for deviations from standard terms and conditions, and flag potential compliance risks to support consistent application of policy and mitigate risks from non-compliant terms.

3.1.3.12 Contract Access and Management

The system shall allow authorized users to access and manage both current and archived contracts in accordance with document retention policies of three to five years, enabling efficient retrieval and audit readiness.

3.1.3.13 Notifications for Key Events and Milestones

The CLMS shall provide automated notifications for key events, milestones, and required actions throughout the contract lifecycle, to ensure timely follow-up and prevent missed deadlines.

3.1.3.14 Post-Award Compliance and Monitoring

The system shall support post-award compliance and monitoring, including tracking of milestones, service level agreements (SLAs), key performance indicators (KPIs), and vendor performance, to enable real-time oversight and ensure adherence to contract terms.

3.1.3.15 Reporting and Analytics

The CLMS shall include customizable dashboards, real-time reporting, and audit trails to support data-driven decision-making, performance monitoring, and compliance tracking, and oversight.

3.1.4 CURRENT CONTRACTING ENVIRONMENT

The Department requires a Contractor with the experience, knowledge, and capacity to support the establishment and management of more than two hundred and fifty (250) active contracts, each with varying scopes, complexities, and financial values. As the Medicaid program continues to evolve, contract volumes are anticipated to increase substantially. This growth is driven by a series of ongoing and forthcoming initiatives, including:

- The transition from fee-for-service to Managed Care
- Implementation of Behavioral Health and Intellectual/Developmental Disabilities (I/DD) Tailored Plans
- Medicaid Expansion
- Modularity and technological enhancements within the Medicaid Enterprise System (MES)
- Continued support for Medicaid Direct, Standard Plans, and the EBCI Tribal Option

The Department also supports vendor performance management and oversight for legacy systems, information technology solutions, automation-related contracts, and the small purchases to support the Medicaid Program. These initiatives will require a flexible, responsive, and well-coordinated contracting approach to ensure timely execution and oversight aligned with DHB's strategic goals.

3.1.5 IMPLEMENTATION AND SUPPORT

The Department requires a CLMS solution that encompasses a full range of services, including system implementation with configuration, data migration, and integration support. The solution must also provide comprehensive training for system users, including CMPU staff and DHB stakeholders, as well as ongoing technical support and system maintenance. Additionally, the Contractor must supply detailed user and administrator documentation to ensure effective system adoption and operation.

3.1.5.1 Business Resource Requirements

The Department will require moderate business involvement during the implementation phase, particularly from CMPU and DHB stakeholders. Key roles will include business analysts for requirements validation, subject matter experts for configuration and testing, and departmental trainers to support end-user adoption. Post-implementation, minimal business resources will be needed for routine usage and system feedback.

3.1.5.2 IT Resource Requirements

Minimal internal IT involvement is expected. The Contractor will manage system deployment, integration, and maintenance. The Department's IT team may be engaged for network access coordination, data migration oversight, and integration validation. Minimal internal IT involvement is expected and no ongoing system administration is anticipated, as these services will be provided by the Contractor. The Contractor will manage system deployment, integration, and maintenance. The Department's IT team may be engaged for network access coordination, data migration oversight, integration validation, and SLA management."

3.1.5.3 Issue Resolution and Escalation

The solution requires a tiered support model with defined escalation procedures. End users will have access to a helpdesk and knowledge base. Unresolved issues will escalate through support, with prioritized response SLAs based on issue severity. Escalation to a dedicated account manager and technical lead is available for high-impact incidents.

3.1.5.4 CLMS Efficiency Gains

The CLMS solution incorporates workflow automation, template-based contract generation, and real-time tracking to streamline contract lifecycle management. Integration with existing systems reduces manual entry and duplication. Built-in analytics and reporting provide actionable insights, promoting continuous improvement and operational efficiency.

3.2 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.2.1 REQUIREMENTS

A requirement is a function, feature, or performance that the system must provide.

3.2.2 SPECIFICATIONS

A specification documents the function and performance of a system or system component. The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, will mean that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the

specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.2.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency with complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor, and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.2.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturer's or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.2.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

<https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts>

- a. Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
- b. Identify and explain any components that are missing from the State's existing license agreement.
- c. If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.
- d. Explain the transportability and transferability of the proposed license agreements.

3.2.6 ENTERPRISE ARCHITECTURE STANDARDS

The vendor shall comply with Attachment J: Enterprise Architecture, including modeling standards (UML2, BPMN; TOGAF-aligned), required artifacts, repository practices, and submission/maintenance during DDI and O&M.

3.3 SECURITY SPECIFICATIONS

3.3.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE – RESERVED

3.3.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The Contract Lifecycle Management System will be required to receive and securely manage data that is classified as *High Risk*. Refer to the North Carolina Statewide Data Classification and Handling

policy for more information regarding this data classification. The policy is located here: <https://it.nc.gov/document/statewide-data-classification-and-handling-policy>.

To comply with the State's Security Standards and Policies, State agencies are required to perform annual security/risk assessments on their information systems using National Institute of Standards and Technology (NIST) 800-53 controls. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

- a. Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located here: <https://it.nc.gov/documents/vendor-readiness-assessment-report>
- b. Vendors shall provide a current independent 3rd party assessment report in accordance with subparagraphs i)-iii) at the time of offer submission.
 - i. Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).
 - ii. A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.
 - iii. An IaaS vendor cannot provide a certification or assessment report for a SaaS vendor UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.
- c. Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

3.3.3 VULNERABILITY RISK RATINGS AND REMEDIATION

Where technically configurable, risk ratings shall be calculated based on active exploit threat, exploit availability, factors from the Common Vulnerability Scoring System (CVSS), and system exposure utilizing a scale of 0 to 10.0 as per the CVSS v3 "Qualitative Severity Rating Scale" for proper prioritization. If the additional combined information above is not available then the CVSS score, exploitability information, or a vendor rating where appropriate risk is reflected may be used. For general vulnerabilities that do not easily relate back to a common vulnerability and exposure, such as unsupported software or encryption versions less than policy requirements, a vulnerability scanner rating that is above "info", or a score of 0, may be used after appropriate review.

The risk ratings and remediation timelines are assigned to vulnerability follows:

- a. Critical-level Risk (Priority/CVSS 9.0-10.0): A vulnerability that could cause grave consequences and potentially lead to leakage of sensitive data, if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions

of the network or IT asset, as identified by the data owner. Critical-level risk vulnerabilities must be, at a minimum, remediated within seven (7) days.

- b. High-level Risk (Priority/CVSS 7.0-8.9): A vulnerability that could lead to a compromise of the network(s) and systems(s) if not addressed and remediated within the established timeframe. High-level risk vulnerabilities must be mitigated or remediated within thirty (30) days.
- c. Medium-level Risk (Priority/CVSS 4.0-6.9): A vulnerability that should be addressed within the established timelines. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner. Medium-level risk vulnerabilities must be mitigated or remediated within sixty (60) days.
- d. Low-level Risk (Priority/CVSS 0.1-3.9): A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Low-level risk vulnerabilities must be mitigated or remediated within ninety (90) days.

3.4 ENTERPRISE SPECIFICATIONS

3.4.1 ENTERPRISE STRATEGIES, SERVICES, AND STANDARDS

Agencies and vendors should refer to the Vendor Resources Page for information on North Carolina Information Technology enterprise services, security policies and practices, architectural requirements, and enterprise contracts. The Vendor Resources Page can be found at the following link: <https://it.nc.gov/vendor-engagement-resources>. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

3.4.2 ARCHITECTURE DIAGRAMS

The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. These diagrams, required at offer submission, can be found at the following link: <https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192>

There may be additional architectural diagrams requested of the Vendor after contract award. This will be communicated to the Vendor by the agency as needed during the project.

Please review *Attachment U: Conceptual Architectural Diagrams* for a detailed architecture of the future state.

3.4.3 IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (ICAM)

Identity and Access Management is a crucial component of modern IT security strategies, providing a robust framework to protect an organization's digital assets while enabling efficient and compliant business operations. The State provides an Identity and Access Management Solution (NCID) and requires all inter-agency and external facing solutions/applications to use NCID. NCID enforces policies for identity management such as:

- a. Common user ID and passwords
- b. Central, delegated ID management
- c. Central repository of IDs and authentication policies
- d. Self-registration and password recovery
- e. Tooltips to verify new passwords meet the State's password policy.

Documentation and resources are available from the State to provide guidance for using the NCID solution to individuals, business users, government employees, and contractors.

- [NCID resources - Individual and Business users](#)
- [NCID resources – Government employees and Contractors](#)

A solution's identify and access management integration to the NCID solution is accomplished by one of the following protocols:

- Security Assertion Markup Language (SAML v2)
- OAuth/OIDC

The State has developed a Medicaid Enterprise System Portal (MES Portal) which provides an entry point into the NC MES Medicaid system and displays the MES modules to which a user has access based on the coarse-grained authorization. When linking and signing into an MES module's application, the MES module will provide fine-grained authorization to give the user the appropriate access within the application.

Multi-Factor Authentication (MFA) will be provided by NCID and will be used when logging in by MES Modules to provide enhanced security in addition to the use of a username and password. The MES Modules will make available to users State documentation and guidance for installing MFA options to work with NCID.

- [NCID MFA Documentation and Guidance](#)

Please review *Attachment V: Medicaid Integration Services Core Capabilities* for additional information on ICAM and the MES Portal.

3.5 BUSINESS AND TECHNICAL REQUIREMENTS

The Vendor must provide a response in their offer to all requirements as part of the technical proposal as defined in *Attachment T: Technical / Management Proposal*. If any of the RFP requirements cannot be met, the State will disqualify the Vendor from further evaluation.

Note: The number assigned to each requirement in the following tables may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

3.5.1 REQUIREMENTS

Table R1. CLMS Functionality Requirements

Requirement #	Requirement Description
CLM-001	The Vendor solution must provide a secure digital environment which allows authorized users to manage, access and view current and expired contracts and supporting documents for Contract Development, Contract Repository, and Contract Monitoring.
CLM-002	The Vendor solution must provide an intuitive graphical user interface functionality to support contract development, dashboards and reporting, workflows and approvals, and file management for Contract Development, Contract Repository, and Contract Monitoring.
CLM-003	The Vendor solution must provide users with a view of document change activities and notifications of key events and milestones throughout the Contract Development and Contract Repository processes.
CLM-004	The Vendor solution must provide contract amendment / modification development and collaboration functionality with associated approval workflows.
CLM-005	The Vendor solution must provide users with notifications of key events and milestones during the Contract Monitoring period.

Table R2. Operations Requirements

Requirement #	Requirement Description
OPS-001	The Vendor must provide system configuration changes to the Department for approval prior to deployment. The Department reserves the right to request changes to the proposed major configuration changes that impact the State.
OPS-002	The Vendor must submit its notice within ninety (90) days of any system upgrades, new versions of product, or new APIs, to the Department for approval. The Vendor must provide an impact analysis to the Department how the changes or upgrades will impact the operation and functionality of the solution and provide the documented testing results without degradation to the solution.
OPS-003	The Vendor must provide a Root Cause Analysis (RCA) of any problems that interrupt or delay online inquiries or data transfers within the solution. The RCA must also include any issue mitigations and corrective actions to prevent future interruptions.
OPS-004	The Vendor must provide system maintenance which will include, at a minimum: service changes, system upgrades, correction of deficiencies, performance enhancements, script changes, system parameters, configuration changes, patching, and other activities required to meet the solution requirements.
OPS-005	The Vendor will be solely responsible for obtaining and maintaining all permits, approvals, licenses, certifications, and similar authorizations required by any local, State, or Federal entities for the project and maintaining them throughout the duration of the Contract.

Table R3. Project Management Requirements

Requirement #	Requirement Description
PROJ-001	The Vendor must organize and participate in project-related meetings with the Department as required by the Department.
PROJ-002	The Vendor must support key project/program milestones, such as but not limited to: User Acceptance Testing (UAT) Sign-Off and Go-Live.
PROJ-003	The Vendor must provide all Deliverables to be approved by the Department in accordance with its formal deliverable review process provided by the Department. The Deliverable review is limited to two (2) iterations for each Deliverable.
PROJ-004	The Vendor must follow the Department processes outlined in Section 7.11 Project Management, for the escalation of risks, issues and decisions during the project implementation and operations phases.
PROJ-005	The Vendor must manage, maintain (i.e., RTM maintenance), and demonstrate requirements traceability throughout the life of the contract, to include providing product demonstrations and post-configuration reviews, to support project implementation, operations, and audits.
PROJ-006	The Vendor must conduct a weekly status meeting, during the DDI phase, to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and service level agreements), utilizing the Department-provided status deck template.

Table R4. Security Requirements

Requirement #	Requirement Description
SEC-001	The Vendor shall provide and require encryption for the transmission of email and attached data that is sensitive relative to confidentiality.
SEC-002	The Vendor shall ensure all appropriate measures are in place for minimal use and protection per applicable regulations for the data types and classifications. Policies, procedure and related controls around the use of sensitive data and segregation of duties as required by NC DHHS security or audit staff.

Requirement #	Requirement Description
SEC-003	The Vendor shall certify that any and all Department data will reside in data centers located in the continental United States. Additionally, this data will only be accessible by resources within the continental United States that have completed the necessary HIPAA and PHI training. Any data that will be accessed by resources that are not physically located in the United States will be masked or scrambled.
SEC-004	The Vendor must perform functions, including data and computer processing within the continental United States.
SEC-005	The Vendor's solution must ensure that all data exchanges including inbound and outbound interfaces shall comply with industry standards (e.g., National Institute of Standards and Technology (NIST)), State, and Department requirements.
SEC-006	The disaster recovery site must be geographically separated from the primary site by at least 100 miles and not reliant on the same power or network utilities.
SEC-007	The Vendor must maintain or otherwise arrange for a disaster recovery site for its system operations in the event of a disaster that renders the production site inoperable.
SEC-008	The Vendor must provide back-up processing capability at a DR site such that normal processing can continue in the event of a disaster or major hardware problem at the primary site. All operations at the remote back-up (DR) site must meet established contractual performance and SLA requirements.
SEC-009	If the production site becomes unavailable due to a disaster, the Vendor must move operations to the disaster recovery site and remain operational at the disaster recovery site until the Vendor returns to normal operations.
SEC-010	The disaster recovery environment must fully support production-level availability, capacity, and capabilities while maintaining adherence to all contract SLAs.
SEC-011	The Vendor must determine when the primary production site is inoperable due to a disaster and execute the Disaster Recovery Plan.
SEC-012	The Vendor must submit an After Action Report that includes the DR testing results and issues experienced during DR testing.
SEC-013	As part of Go-Live/Production Readiness Review, the Vendor must execute a disaster recovery test and provide testing results (After Action Report) to the Department that demonstrates the ability to recover the solution in accordance with the Disaster recovery Plan and in support of all Service Level Agreements.
SEC-014	The Vendor must perform DR testing each year at no additional cost to the Department. In the event the Vendor's test is deemed by the Department to be unsuccessful, the Vendor must resolve the identified issues and continue to perform the test, at the Vendor's expense, until satisfactory results are received and approved by the Department.
SEC-015	The Vendor must coordinate disaster recovery activities with the Department.
SEC-016	The Vendor must conduct annual independent third-party penetration testing and submit the test results and reports to the Department.
SEC-017	The Vendor must provide the Department with an annual report, conducted by an external auditor that is accredited by the Association of International Certified Public Accountants (AICPA), on effectiveness of internal controls that is compliant with the current AICPA standard, Reporting on Controls at a Service Organization (SOC 2 – Type 2) includes all five trusted service criteria (i.e., security, availability, confidentiality, process integrity and privacy).
SEC-018	The Vendor must provide Corrective Action Plans (CAPs) to remediate any deficiencies found in any audit or assessment findings such as the SOC 2 – Type 2 audit, HITRUST CSF assessments within 30 days of receiving the report, and must remediate the findings as per the guidelines described in the State Security Policies, and must adapt to evolving controls as standards change, and at no additional cost to the Department.
SEC-019	The Vendor must provide weekly status updates for each Corrective Action Plan (CAP) until the CAP is complete and the finding is remediated in accordance with the State IT Security Policies.
SEC-020	The Vendor must provide access (network connectivity and system credentials) for Department, Federal, and State auditors, including the execution of outside audit tools and audit test software for

Requirement #	Requirement Description
	auditors from the U.S. Department of Health and Human Services (HHS) Office of the Inspector General, the State of NC or DHHS Internal Audit, or any other authorized auditors as determined by Department.
SEC-021	The Vendor must incorporate SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing) in their SDLC and share the security testing results with the Department before implementing any major changes to the system into the production.
SEC-022	The Vendor must implement the risk management framework in compliance with the NIST Risk Management Framework or equivalent.
SEC-023	The Vendor must perform internal risk assessment annually and share the assessment findings and corresponding Plan of Action and Milestones (POA&M) / Corrective Action Plans (CAPS) with the Department.
SEC-024	The Vendor must incorporate other security testing IAST (Interactive application security testing) and RASP (Runtime Application Self Protection) techniques to improve the security posture of the application.
SEC-025	The Vendor must implement the Web Application Firewall (WAF) to mitigate the application security vulnerabilities such as OWASP TOP 10.
SEC-026	The Vendor must implement encryption for data in transit and data at rest using FIPS 140-2 or FIPS 140-3 compliant crypto material.
SEC-027	The Vendor must run weekly vulnerability scans on all Vendor and subcontractor networks and systems that will access State data and information.
SEC-028	The Vendor must provide all vulnerability reports to the Department to track critical and high vulnerabilities in accordance with the Vulnerability Risk Ratings and Remediation State requirements.
SEC-029	The Vendor must review privileged access accounts with the Department and provide the summary report on a quarterly basis.
SEC-030	The Vendor must provide the list of users and their access to the system in a report that Department authorized users can access when needed.
SEC-031	The Vendor must provide at least two Department individuals with administrative accounts to provide continuity of operations.
SEC-032	The Vendor must implement the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks.
SEC-033	The Vendor must conduct Business Impact Analysis (BIA) to identify hierarchy of critical services and infrastructure to determine the order that services will be restored for developing the detailed Business Continuity and Contingency Plan (BCP) and Disaster Recovery Plan (DRP).
SEC-034	The DRP must include (but is not limited to) detailed procedures to address the following potential events: natural disasters (e.g., earthquake, fire, flood, storms), terrorist acts, power disruptions or power failure, computer software or hardware failures, computer shutdown due to cyberattacks (e.g., hacking, malware, and ransomware).
SEC-035	The Vendor must comply with the applicable Federal, State and Department Security Policies and Standards as outlined in the RFP.
SEC-036	The Vendor must provide the necessary access to their systems and the required support to the Department or its authorized contractors to conduct an annual third-party privacy and security assessment including whitebox penetration testing.
SEC-037	The Vendor must maintain dedicated test environments adequate to support multiple testing workstreams concurrently, for example multiple concurrent cycles of internal testing and end-to-end testing. In addition, for the end-to-end environment and testing specifically, the Vendor must maintain a test environment provisioned with the same privacy & security controls that are required by the Federal, State, and Department privacy and security requirements. As part of end-to-end testing, this environment must support and secure production data including production volumes.

Requirement #	Requirement Description
SEC-038	The Vendor must obtain approval from the Department's Privacy and Security Office before storing or processing production data in lower and non-production environments such as development, user acceptance testing, and end-to-end.
SEC-039	The Vendor must pass privacy and security related assessments or audits conducted by DHHS, the State of NC, and Federal, including security audits, third party security assessments, and annual audits.
SEC-040	The Vendor must restore the Solution availability, in the event of unscheduled downtime, following the protocols and timing provided in the Disaster Recovery Plan.
SEC-041	The Vendor's solution services and infrastructure shall adhere to best practices and use open security standards and frameworks, such as but not limited to: i. Policy: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL) ii. Federation: WS-Secure Conversation, WS-Federation, WS-Authorization, XML Key Management (XKMS) iii. Mechanism: Extensible Access Control Markup Language (XACML), XML Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML), X.509 certificates
SEC-042	The Vendor shall provide different access levels using role-based access controls. The access levels shall be configurable by the Vendor.
SEC-043	The Vendor solution must maintain and operate a secure web-based CLMS solution that utilizes Internet/Cloud-based applications and complies with State and Federal Security standards.
SEC-044	The Vendor solution must provide and support multifactor authentication.
SEC-045	The solution shall provide Single Sign-On (SSO) capability using Department standards using NCID and authentication.

Table R5. Testing Requirements

Requirement #	Requirement Description
TEST-001	The vendor must coordinate testing processes, activities, and schedules with the State.
TEST-002	The Vendor must document test results and provide them to the Department prior to implementing any changes in the production environment.
TEST-003	The Vendor must ensure that UAT is conducted on a fully tested and operations-ready module component, including all software features.
TEST-004	The Vendor must have the capability to mask, sanitize, scramble, and / or desensitize procurement sensitive data when extracting data from the production environment for use in non-production environments.
TEST-005	The Vendor must implement version control in all environments.
TEST-006	The Vendor must make recommendations concerning test correction / remediation execution activities based on the results of testing.
TEST-007	The Vendor must obtain Departmental approval of test results for all standard North Carolina testing phases before testing is considered complete.
TEST-008	The Vendor must perform Production Readiness Testing that includes a test of actual data processing in a fully operational environment.
TEST-009	The Vendor must plan and manage all required testing phases such as unit, integration, user acceptance, and end-to-end Testing for their solution.
TEST-010	The Vendor must provide authorized users access to necessary testing environments as required for testing during DDI and throughout the life of the Contract.

Requirement #	Requirement Description
TEST-011	The Vendor must provide training for all testing participants that includes: the system, processes, procedures, and tools used to execute testing.
TEST-012	The Vendor must support the State in all testing activities by providing support staff and technical expertise.
TEST-013	Test cases must include positive and negative scenarios, and the negative scenarios must include error handling and stressing the system with bad or invalid data to ensure it is rejected correctly. Test scripts must provide step-by-step instructions for executing test cases, including the expected results.
TEST-014	All test cases must be reviewed and approved by the Department prior to the start of testing execution. The Department may provide additional test cases as agreed to by both parties.
TEST-015	For end-to-end testing, the test environment(s) data refresh must be scheduled per Department approval.
TEST-016	The Vendor must develop and maintain a Master Test Plan (i.e., living document) throughout all DDI phases, including testing phases (Unit/Assembly, System Integration/Regression Testing, Performance/Security Testing, and UAT Testing as applicable) as described in Section 7.17 of the RFP. Updates must be made by the vendor within 30 calendar days of a change being implemented prior to SIT, a change in scope, and any changes to access to testing tools. The Master Test Plan shall be submitted to the Department per the project schedule or upon request by the Department and shall include: i. High level description of the scope of each testing phase; ii. Applications or Systems that are part of the testing; iii. Integrations that are part of the testing; iv. Testing techniques or tools that will be used for testing; v. Test Environment; and vi. Test Metrics and Reporting of Defects.
TEST-017	The Vendor must design and document detailed test cases for each phase of testing.
TEST-018	The Vendor shall plan for and include State participation and involvement in all testing efforts throughout DDI and O&M, where applicable.
TEST-019	The Vendor must manage the process of test execution and processes; and provide automated test reports on a weekly basis as part of project status updates. The reports must include at a minimum test case statistics, test case execution, screen shots, and defect statuses.
TEST-020	The Vendor must build and maintain a testing schedule as part of the overall project schedule that accurately reflects all testing activities linked with the appropriate dependencies between predecessors and successors.
TEST-021	The Vendor must propose solutions for all issues, problems, and defects for the Vendor's solution identified through Production Readiness Review.
TEST-022	The Vendor must be responsible for scheduling, coordinating, and supporting all testing activities to ensure that each test is prepared and performed in accordance with the Master Test Plan.
TEST-023	The Vendor must document and communicate the progress of all testing efforts through a regular progress report to include test case execution status and defect status. This report must address all test scenarios and test cases and report the status of the test effort relative to the test schedule.
TEST-024	The Vendor must provide a functional demonstration of the system including any changes or enhancements prior to user acceptance testing.
TEST-025	The Vendor must perform periodic demonstrations at the completion of each major component during the testing phase to the Department. Additional demos can be requested, as needed.
TEST-026	The Vendor must provide test cases that include identifications, detailed steps, expected results, and actual results.
TEST-027	The Vendor must track and report defects at a minimum weekly, or as requested by the Department, on the defects identified and the progress made toward resolution of the defects during SIT.
TEST-028	The Vendor must identify test configurations and environment.

Requirement #	Requirement Description
TEST-029	The Vendor must lead planning, execution, and reporting of system/user testing.
TEST-030	For State-led testing, the Vendor must support all aspects, including resources, scheduling, data, environments, and defect remediation, as appropriate.
TEST-031	The Vendor must utilize a Department-approved automated testing tool.
TEST-032	The Vendor's solution must provide the ability for the tester to perform Temporal testing within all testing environments by manipulating the system date.
TEST-033	The Vendor must support all testing efforts with other platforms (both internal and external).
TEST-034	The Vendor must test all data transmissions with the Department and other State systems to validate connectivity, format, and data. This includes data exchanges between the Department and other systems (see <i>Attachment U: Conceptual Architecture Diagram</i>).
TEST-035	The Vendor must provide a training environment for use in training staff for pre and post-production.
TEST-036	The Vendor must thoroughly test the solution and demonstrate proof of successful Vendor testing for each testable requirement by providing all Vendor test results for State review and approval.
TEST-037	The Vendor must provide regression results to the State at agreed-upon intervals.
TEST-038	The Vendor's system improvements or enhancements must be deployed to test environments before they are deployed to the production environment.
TEST-039	The Vendor must outline its testing escalation process in the Master Test Plan that describes how testing issues and defects will be managed according to criticality (e.g., identification through resolution) and how this will be reported to the State.

Table R6. Staffing Requirements

Requirement #	Requirement Description
STAF-001	The Vendor must provide written notice within thirty (30) Calendar Days of any decision by the Vendor or by any of the Vendor's subcontractors to relocate the performance of any work under the Contract from a location within the United States to a location outside the United States. The Vendor must obtain written approval from the State prior to relocating the performance of any work to a location outside the United States.
STAF-002	The Vendor must provide technical support every State Business Day from 8:00 A.M. - 5:00 P.M. ET, unless otherwise agreed upon by the Department.

Table R7. Reporting Requirements

Requirement #	Requirement Description
REP-001	The Vendor solution must accept all individual queries and batch queries without any limitation on query volume or frequency to include ad hoc request.

Table R8. Training Requirements

Requirement #	Requirement Description
TRAIN-001	The Vendor must provide training, education, and technical assistance to the CMPU and other relevant stakeholders pre and post implementation.
TRAIN-002	The Vendor must conduct training at times and locations mutually agreed upon between Department and Vendor, which may include virtual options when approved by the Department.
TRAIN-003	The Vendor must provide a development environment to design training and conduct training of each associated user, role, and group.

Requirement #	Requirement Description
TRAIN-004	The Vendor must conduct surveys and monitor training effectiveness among all user groups and prepare corrective action(s) for process improvement where indicated. All findings, corrective actions, and recommendations will be documented in the Training Evaluation Report.

Table R9. Turnover Requirements

Requirement #	Requirement Description
TURN-001	The Vendor shall provide a Turnover Plan within 30 days of the Turnover Notification Letter. The plan shall include: Data Turnover tasks, Custom interface Turnover tasks, Reusable code Turnover tasks, Documentation regarding products (with versions), files, interfaces, and work flows not considered to be part of the COTS proprietary documentation tasks, A timeline with milestones for the Turnover to include planning, execution, and implementation approval.
TURN-002	The Vendor shall provide Turnover deliverables as part of the Turnover tasks to include: All product documentation (with versions), files and data, Reusable code Turnover, Customized ad-hoc reporting specifications, Documentation regarding files, interfaces, and work flows not considered to be part of the COTS proprietary documentation, A timeline with milestones and a Work Breakdown Structure (WBS) for the Turnover to include planning, execution, and implementation approval, A description of post turnover support for up to 90 business days.
TURN-003	The Vendor shall provide a security profile of Department users in a Microsoft Word document or Microsoft Excel spreadsheet format.
TURN-004	The Vendor shall carry out an orderly, cooperative, comprehensive, and controlled transition to the Department or to a Department's vendor.

Table R10. Audit Requirements

Requirement #	Requirement Description
AUD-001	The Vendor must cooperate fully and completely with all Quality Assurance audits, evaluations, studies, investigations, surveys, reviews, and findings conducted by the Department, Federal, State, or other auditing entities.
AUD-002	The Vendor must produce and maintain robust audit trails and audit logs of all applications and engineering activities (including inquiry transactions) on the environments wherever the production data is accessible. Audit trails/logs must be maintained throughout the life of the contract and all data be turned over to the State within 90 days of contract expiration or termination.
AUD-003	Audit logs must be maintained online, behind a front-end presentation toolset that is accessible by the Department (or Department authorized users) and provides queries, reports and analytics on any log, in support of typical control questions required by the latest NIST 800-53.
AUD-004	The Vendor must retain all records and reports relating to this Contract for a period of three (3) years after final payment is made under this Contract and in alignment with our Retention Policy.

Table R11. Integration Requirements

Requirement #	Requirement Description
INT-001	The Vendor solution must use Microsoft SharePoint to support document and file management activities (e.g., filing, storing, archiving, retrieving, sharing, securing, and collaborating).
INT-002	The Vendor solution must use "DocuSign" or equivalent product to support contract documents for routing (e.g., signature process, etc.).
INT-003	The Vendor solution must support the use of "Adobe" or similar products related to PDF file activities, including document conversion.
INT-004	The Vendor solution must use Microsoft 365 products to support solicitation and contract document activities (e.g., creating, editing, analyzing, reporting, etc.).

3.6 BUSINESS AND TECHNICAL SPECIFICATIONS

The Vendor must provide a response in their offer to all specifications as part of the technical proposal as defined in *Attachment T: Technical / Management Proposal*.

Note: The number assigned to each specification in the following tables may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional. **Specification categories are listed in descending order of importance.**

3.6.1 SPECIFICATIONS

Table S1. CLMS Development Specifications

Specification #	Specification Description
CLMD-001	Describe how the solution provides role-based access that allows authorized contracting and legal users to access and manage contract development activities.
CLMD-002	Describe how the solution provides the ability for additional approvers, such as business owners, to review/redline/approve draft solicitation documents.
CLMD-003	Describe how the solution provides integration with MS Office, collaboration tools such as SharePoint, and approval tools such as DocuSign.
CLMD-004	Describe how the solution implements different template structures and clause libraries for different contract types to include State and Federal clauses provided by the State.
CLMD-005	Describe how the solution provides Contract meta-data properties that are updated automatically.
CLMD-006	Describe how the solution provides the capability to track every change made to contracts within a conformed document.
CLMD-007	Describe how the solution provides centralized contract processes like intake, review, and approval routing.
CLMD-008	Describe how the solution provides the ability to develop and administer automated workflows to streamline the contract creation, review, and approval processes.
CLMD-009	Describe how the solution provides locking/unlocking current versions during contract development with the ability to look at and restore previous drafts.
CLMD-010	Describe how the solution provides comparison of different versions to identify changes.
CLMD-011	Describe how the solution provides contracts to be constructed using modular parts and attachments, with functionality to manage how they are collated.
CLMD-012	Describe how the solution provides a graphical method to upload multiple contract artifact files.
CLMD-013	Describe how the solution provides a dashboard configured to show elements such as contract status, notifications, and reports.
CLMD-014	Describe how the solution provides ad-hoc reporting.

Specification #	Specification Description
CLMD-015	Describe how the solution provides reporting and analytics tools for generating reports and analyzing contract data for the Development, Repository, and Monitoring.
CLMD-016	Describe how the solution provides a historical log of document change activities, archiving, version control, reviews and approvals, and alerts and notifications delivered to users for key milestones such as renewals or expirations.
CLMD-017	Describe how the solution notifies the user(s) and if it provides a link directly to the contract or document needing attention.
CLMD-018	Describe how the solution provides approvers the capability to view the contract approval record, including other approvals or dissents, and provide their approval.
CLMD-019	Describe how the solution creates and manages pre-approved templates such as Amendments.
CLMD-020	Describe how the solution manages the contract amendment development process.
CLMD-021	Describe how the solution provides the capability to scan a PDF or other text document and identify language in the document that correlates to, or deviates from standard terms and conditions.
CLMD-022	Describe how the solution provides the capability to ingest standard and customized templates electronically in various formats.
CLMD-023	Describe how the solution provides functionality to analyze external party language for deviations to contract standards.

Table S2. CLMS Repository Specifications

Specification #	Specification Description
CLMR-001	Describe how the solution provides a centralized contract repository for all contracts and other documents related to contracts.
CLMR-002	Describe the solutions size limitations associated with storing and supporting documents. Include in your narrative how the solution handles large files using multi-part upload.
CLMR-003	Describe how the solution provides role-based access that allows authorized users to access and view contracts.
CLMR-004	Describe how the solution provides contract meta-data properties with automatic updates through amendments.
CLMR-005	Describe how the solution provides the ability to link pre-award solicitation documents with resulting contract and amendments.
CLMR-006	Describe how the solution provides a dashboard that can be configured to show elements such as contract and workflow status, notifications and reports. Include in your narrative how the solution dashboard can be configured or customized by user, role, or group.
CLMR-007	Describe how the solution provides the ability for users to create customized reports pertaining to contracts and supporting documents meta-data properties.
CLMR-008	Describe how the solution provides a graphical method to upload contract artifacts and allow for the selection of multiple files to be uploaded at one time.
CLMR-009	Describe how the solution provides search capability for key words and clauses across all contracts and associated artifacts in any type of file (PDF, Word, Excel).
CLMR-010	Describe how the solution provides notifications with links that allow users to link directly to the contract or document needing attention.
CLMR-011	Describe how the solution provides management of contract terminations and closeout activities.

Table S3. CLMS Monitoring Specifications

Specification #	Specification Description
CLMM-001	Describe how the solution permits users to perform contract monitoring / post-award activities.
CLMM-002	Describe how the solution will integrate with the State systems. Include in your narrative how APIs are used for integration with State systems.
CLMM-003	Describe how the solution provides alerts and notifications delivered to users for key dates, contract monitoring events such as deliverables, SLAs, reporting, etc., and business reviews.
CLMM-004	Describe how the solution provides notifications with links that allow users to link directly to the contract or document needing attention.
CLMM-005	Describe how the solution provides the capability to develop and administer customized approval workflows for contract monitoring activities.
CLMM-006	Describe how the solution provides the capability to configure, monitor, and analyze metrics such as deliverables, SLAs, KPIs, etc.
CLMM-007	Describe how the solution provides a dashboard that allows for performance tracking to monitor and report on contract performance against agreed-upon metrics and deliverables.
CLMM-008	Describe how the solution provides enhanced visibility to offer insights into contract performance, key dates (deliverables, renewals and expirations), and obligations (SLAs).
CLMM-009	Describe how the solution provides cost management associated with contracts, including tracking expenses, invoice burndown, and transition period costs such as on-boarding and off-boarding.
CLMM-010	Describe how the solution provides the functionality to upload the contract monitoring plan and other monitoring documents and provide status updates on the monitoring activities.

Table S4. Business Specifications

Specification #	Specification Description
BUS-001	Describe your approach to support custom label changes and/or system branding (e.g., NC DHHS logos, etc.).
BUS-002	Describe your solution by providing screen shots (e.g., up to ten (10) screen shots for Contract Development, Contract Repository, and Contract Monitoring) to effectively represent the solution components.
BUS-003	Describe how the solution supports the reports identified in <i>Attachment AA: Reports</i>. Include in your narrative use of AI, self-service capabilities, and how these reports are generated: Pre-Award Reports: 1. RFx-to-Contract Conversion 2. Cost and Savings 3. RFx Lifecycle 4. Compliance and Risk 5. Audit and Version Control 6. Vendor Response Analysis Post-Award Reports: 1. Contract Status 2. Expiring Contracts 3. Vendor Performance Metrics 4. Financial 5. Compliance 6. Lifecycle 7. Customizable 8. Analytics

Table S5. Operations Specifications

Specification #	Specification Description
OPS-001	Describe how the solution will provide the Department with system flexibility, security and automation to manage and act upon errors identified by the Vendor solution, in a timely manner.
OPS-002	Describe the approach to ensure the Vendor solution meets 99.9% uptime.
OPS-003	Describe the level of business resources the Department would need to implement, support, and maintain the solution.
OPS-004	Describe the level of IT resources the Department would need to implement, operate, and maintain to support the solution.
OPS-005	Describe the solution's capability to provide issue resolution as an escalation strategy.
OPS-006	Describe your approach to provide customer and technical support services, beyond automated help responses, that will be available to the State, including hours of operations and time resolution.

Table S6. Compliance Specifications

Specification #	Specification Description
COMP-001	Describe any performance or compliance issues that have occurred in any Contract held by the Vendor in the past five (5) years, if any, and how it was resolved and in what timeframe.
COMP-002	Describe any incidents where a contract was terminated due to a contractual breach or insufficient performance within the past five (5) years. If any such incidents have occurred, explain the circumstances or reasons surrounding the terminations. Respond if no such contract terminations or breach incidents have occurred.

Table S7. Security Specifications

Specification #	Specification Description
SEC-001	Describe your approach to maintaining data security during an event that causes the implementation of the Business Continuity Plan.
SEC-002	Describe your approach to address and resolve customer support and technology disruption impacting the CLMS services. Include in your narrative the resolution time frame and communication strategy.
SEC-003	Describe how your proposed solution complies with applicable security standards identified by the State in this document; and describe how compliance can be achieved and verified during Design, Development, and Implementation (DDI) and Operations of the solution.
SEC-004	Describe if the solution provides a portal and, if so, how the Department would access the solution while maintaining security measures.

Table S8. Enterprise Architecture Specifications

Specification #	Specification Description
ARC-001	Describe the solution roadmap for your product. Include content on release strategies for functionality, roadmap for technical architecture, and address the scalability of the solution.
ARC-002	Describe how your solution supports the State's Identity and Access Management protocols referenced in Section 3.4.3 of the RFP, as well as making them available for application integration/consumption.
ARC-003	Describe the proposed solution capabilities to interoperate with other solutions. Identify the standards supported, integrations platforms, adaptors, APIs and other similar standards. Identify the standards supported and the standards for data exchange (e.g., EDI).
ARC-004	Describe how proposed solution's Disaster Recovery Plan (DRP) supports Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) metrics.

Specification #	Specification Description
ARC-005	Describe the solution's backup plan and contingency planning capabilities, to include rollback functionality.
ARC-006	Describe the frequency and test procedures for end-to-end disaster recovery testing.
ARC-007	Describe the capabilities of the proposed solution to support the agency's continuity of operations and incident responses.
ARC-008	Describe approaches available for data conversion and/or data migration to load current and historical data into proposed solution.
ARC-009	Describe how the proposed solution monitors and reports the metrics on system performance.
ARC-010	Describe how the proposed solution manages user administration.
ARC-011	Describe how the proposed solution provides application audit functionality or supports application audits. Areas of support may include: - Security audits - Performance monitoring - Compliance management - Issue management - Change management - Access control - Log management and analysis - Reporting
ARC-012	Describe how the proposed solution complies with industry accessibility standards.
ARC-013	Describe how the proposed solution is digitally accessible or if not fully accessible, provide the roadmap with timeline for remediation. Provide product documentation that demonstrates if the solution is digitally accessible.
ARC-014	Describe how the Vendor solution will be delivered and supported (e.g. on premises, cloud-based, or cloud-agnostic).
ARC-015	Describe how the Vendor solution will integrate with other systems. Provide detailed data, data flow diagrams with descriptions, network and application architecture diagrams. Include a list of proposed API's that will be used to interface with other systems and the objective of each API.

Table S9. Testing Specifications

Specification #	Specification Description
TEST-001	Describe how you conduct testing using automation testing tools, level of test automation, interactive testing, and interactive debugging available in the test environment.
TEST-002	Describe your approach to the design and documentation of a combination of positive and negative test case scenarios, including such items as identification, detailed steps, expected results, and actual results for each phase of testing.
TEST-003	Describe your solution's approach to providing a functional demonstration to the Department to show any changes or enhancements to the solution, prior to user acceptance testing.
TEST-004	Describe how the Vendor solution will create and load test data and utilize it during the testing process. Include how confidential data is protected or masked during testing and how participants are notified if testing involves confidential data.
TEST-005	Describe the defect management process and how abnormal results that arise during the execution of identified test cycles (e.g., DDI, Operations, UAT) are resolved.
TEST-006	Describe the testing environments your solution will support such as: Unit Testing, System Testing, Integration Testing, Interface Testing, Performance Testing, Regression Testing, User Acceptance Testing, and Production Readiness Tests.
TEST-007	Describe how your solution's test environment mirrors the production environment in its size, files, databases, processing, data protection, and reporting.

Specification #	Specification Description
TEST-008	Describe how your testing protocols avoid testing conflicts of interest between solution developers and the testing team such as a clear separation of duties from the development and implementation team versus the team performing testing.
TEST-009	Describe how your solution provides performance tests and reporting of a simulated load consistent with the actual load projected or used in production.

Table S10. Quality Assurance Specifications

Specification #	Specification Description
QUA-001	Describe your internal quality process to measure, track, and document the quality of deliverables.
QUA-002	Describe the Vendor's quality assurance policies, procedures, and practices they will implement to ensure completion and validation of the accuracy of the services required in the RFP.
QUA-003	Describe the approach for participation in Department initiated reviews and incorporation of feedback and recommendations.

Table S11. Training Specifications

Specification #	Specification Description
TRAIN-001	Describe the type of training offered in your training program to meet the needs of users with different learning styles. Include how you determine the effectiveness of your training via such methods as surveys and real-time feedback sessions.
TRAIN-002	Describe the curriculum and training documents used for training. Include in your narrative help screens, descriptions of online or printable materials, use of knowledge bases, etc.

3.7 OPTION REQUIREMENTS AND SPECIFICATIONS

This RFP contains an option to purchase functionality for integration with ServiceNow and the North Carolina Financial System (NCFS) as part of the Contract Lifecycle Management System (CLMS) solution. The State may elect to exercise either of the Options during the term of the contract at its sole discretion. The Vendor must include a response to the required information associated with the Options as part of their proposal.

3.7.1 Option to Award – Requirements

Table OR1. ServiceNow Integration Requirements

Number	Requirement Description
OPT-SNOW-01	The Vendor solution must retrieve and display near real-time ServiceNow data related to vendor performance (e.g., Notice of Deficiencies (NOD)) through the Medicaid Integration System (MIS) Platform.

Table OR2. NCFS Integration Requirements

Number	Requirement Description
OPT-NCFS-01	The system must retrieve and display near real-time North Carolina Financial System data related to contractual obligations, budget encumbrances, and expenditures to ensure end-to-end workflow continuity.

3.7.2 Option to Award – Specifications

Table OS1. ServiceNow Integration Specifications

Specification #	Specification Description
OPT-SNOW-02	Describe the technical approach for integrating with ServiceNow, including use of APIs, data exchange formats, and authentication methods.
OPT-SNOW-03	Identify any dependencies, assumptions, or prerequisites for enabling the ServiceNow integration and describe how the ServiceNow integration will be maintained and supported throughout the contract term, including version compatibility and updates.
OPT-SNOW-04	Describe how the solution will retrieve and display ServiceNow data in the CLMS user interface, including dashboards or reports.
OPT-SNOW-05	Describe how the integration will support audit trails and traceability for ServiceNow-sourced data.

Table OS2. NCFS Integration Specifications

Specification #	Specification Description
OPT-NCFS-02	Describe how the solution will interface with NCFS using secure APIs or data exchange protocols to synchronize contract and financial data.
OPT-NCFS-03	Describe how the solution supports automated data validation to ensure consistency between contract terms and financial records.
OPT-NCFS-04	Identify any dependencies, assumptions, or prerequisites for enabling the NCFS integration and describe how the NCFS integration will be maintained and supported throughout the contract term, including version compatibility and updates.

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must provide a complete cost proposal that is inclusive of all costs associated with the solution and services outlined in this RFP, including all direct and indirect costs. The Cost Proposal must be submitted using the Microsoft Excel Cost Proposal Workbook referenced in *Attachment E: Cost Form*. The Cost Proposal will contain the following:

Total Implementation Costs: The deliverables associated with planning, development, and implementation effort necessary to deliver the solution and services outlined in this RFP.

In addition to the Total Implementation Costs, describe how the Vendor can also provide a schedule reflecting a request for payment for satisfactory performance of the remaining scope (Non-Implementation or Steady State) of the contract.

Each deliverable within a phase must have a cost unless otherwise noted by the Department within the Cost Proposal Workbook.

Operations and Maintenance Costs: The ongoing services, support, deliverables, and cloud hosting necessary to provide the solution and services outlined in this RFP after the initial implementation.

- a. Costs must be provided for each year of the Contract term.
- b. Operations and Maintenance Costs will begin after Solution Implementation is complete and approved by the Department.
- c. Operations and Maintenance Costs will be billed monthly:
 - i. Services and Support for the functionality of Items in *Attachment E: Cost Form* will be billed as one-twelfth (1/12th) of the annual cost for the item for the upcoming month.

- ii. Ongoing Maintenance deliverables will be billed by the Vendor upon delivery and approval by the Department.
- iii. Cloud Hosting and software related O&M costs will be billed as one-twelfth (1/12th) of the annual cost for the upcoming month.
- d. Fully Burdened Off-Site Hourly Labor Rates for all Key Personnel and other project staff must be provided.
- e. Additional Costs – The Vendor may provide any additional costs that are specific to the implementation of their solution that are not outlined in the Cost Proposal Workbook referenced in *Attachment E: Cost Form*.
- f. Assumptions – The Vendor must provide any assumptions made in their cost proposal.

Cost Option: The functionality of ServiceNow integration and NCFS integration are options to award. The completed cost form must provide all costs including options in the respective tables within the selected cost form. The total cost of ownership, inclusive of all options, will be considered for evaluation and award purposes.

For additional information regarding the Cost Proposal content, see *Attachment E: Cost Form*. To obtain an electronic version of the Cost Proposal Workbook in Excel format, please contact the Contract Specialist listed on the first page of this document.

4.2 PAYMENT SCHEDULE

The Vendor must propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables.

5.0 EVALUATION

5.1 SOURCE SELECTION

A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value to the State, recognizing that Best Value may result in an award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when price is considered with, or traded off against, non-price factors.

- a. Evaluation Process Explanation: The State will establish an evaluation committee to review each Vendor's response to this RFP and make award recommendations. The State will designate employees, independent contractors, or other individuals to serve on the evaluation committee or assist the evaluation committee as a subject matter expert during the evaluation process. The State reserves the right to alter the composition of the evaluation committee and to designate individuals and subject matter experts to assist in the evaluation process. All offers will be initially classified as being responsive or non-responsive. If an offer is found to be non-responsive, it will not be considered further. All responsive offers will be evaluated based on the stated evaluation criteria.
- b. To be eligible for consideration, the Vendor's offer must conform to all requirements and must substantially conform to the specifications provided in this RFP. Compliance with requirements and specifications will be determined by the State. Offers that do not meet all requirements listed in this RFP may be deemed deficient.
- c. The State reserves the right to reject any offer if the evidence submitted by, or investigations, reviews or validations of, the Vendor and its proposal fail to satisfy the State that the Offeror is

properly qualified to carry out the obligations of the Contract and to provide the required services.

- d. The evaluation committee may request clarifications or presentations from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or in part, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer as part of the negotiation process, if applicable.
- e. Vendors are advised that the State will not ask for or accept data that is essential for a complete and thorough evaluation of the offer after the closing date for receipt of offers.
- f. The evaluation committee will make a recommendation to award to the Vendor meeting the RFP requirements and whose offer is determined to be most advantageous and provide the Best Value in accordance with N.C.G.S. § 143-135.9, to the State, based on the evaluation criteria described in the RFP, and the evaluation committee's ranking of proposals and the basis and reasons for the selection decision. Upon approval of the recommendation by the State, the notice of award will be issued, with the State executing a Contract with the successful Vendor.

5.2 EVALUATION CRITERIA

Evaluation shall include best value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in descending Order of Importance.

- a. Business and Technical Specifications of this RFP. Within the business and technical specifications listed in Section 3.6.1 the major categories listed by table are further listed in descending order of importance as provided in *Attachment T: Technical / Management Proposal*. For example, the CLMS Functionality category is more important than the Security category. The specifications listed within a major category, such as CLMS Functionality, are all of equal importance. In addition to the business and technical specifications, vendors within the competitive range will be required to perform a system demonstration based on use cases provided by the Department once a competitive range has been established.
- b. Corporate background and experience, and strength of references (see *Attachment H: Vendor References/Past Performance*), relevant or material to technology area(s) or Specifications. The Vendor may be disqualified from any evaluation or award if the Vendor or any Key Personnel proposed (see *Attachment K: Vendor Key Personnel*), has previously failed to perform satisfactorily during the performance of any contract with the State (e.g., unresolved vendor complaint forms on file with the State or contracts terminated for default) or violated rules or statutes applicable to public bidding in the State;
- c. Cost: Total Cost of Ownership, inclusive of Options to Award, in the formatted cost tables provided in this RFP.

Only those proposals that substantially conform to the RFP will be considered for award.

5.2.1 EVALUATION OF OPTIONS

This solicitation contains optional functionality. The State will evaluate proposals for award purposes, based on the total cost of ownership, inclusive of all options. Evaluation of options will not obligate the State to exercise these options at the time of award or during the contract term.

5.3 BEST AND FINAL OFFERS (BAFO)

The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendor(s) within this range; e.g., "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers consistent with the stated evaluation criteria to determine the final rankings.

5.4 POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, and to the committee responsible for participating in the evaluation. The Vendor submitting a proposal (including its representatives, subcontractors, and suppliers or other pilot partners or affiliates) is prohibited from having any communications with any person inside or outside the using agency, issuing agency, other government agency office, or body (including the purchasing agency, department secretary, agency head, members of the General Assembly and Governor's office), or private entity, if the communication refers to the content of Vendor's proposal or qualifications, the content of another Vendor's proposal, another Vendor's qualifications or ability to perform the contract, and/or the transmittal of any other communication of information that could be reasonably considered to have the effect of directly or indirectly influencing the evaluation of proposal and/or the award of the contract. Vendors who attempt to gain privileged information, or to influence the evaluation process will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 must be clearly marked as such in the offer when submitted.

5.5 COMPETITIVE RANGE

Following the initial evaluation of proposals, the Department will establish a competitive range composed of the highest-ranked Offerors whose proposals are determined to be reasonably susceptible of being selected for award. Only those Offerors within the competitive range will be invited to participate in additional evaluation activities, to include a solution demonstration.

The Department reserves the right to limit the number of Offerors in the competitive range based on the evaluation results, inclusive of Total Cost of Ownership, and the Department's determination of the most advantageous proposals.

5.6 SOLUTION DEMONSTRATIONS

Solution demonstrations will be conducted only with Offerors in the competitive range. Demonstrations will be based on use cases provided by the Department and will be limited to two (2) hours. Demonstrations must be conducted by the proposed project team members who will be responsible for day-to-day operations, not sales or marketing personnel. Demonstrations will be evaluated and scored as part of the Business and Technical Specifications criteria in section 5.2 and will influence final rankings. Details and demonstration guidelines will be provided once a competitive range has been established.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

- a. The Offeror must meet all the minimum qualifications of this RFP, as provided in *Attachment Y: Minimum Qualifications*, for its proposal to be evaluated.
- b. It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications, requirements and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person.
- c. The Vendor will be responsible for investigating and recommending the most effective and efficient solution. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the recommended approach is not short lived. Several approaches may exist for hardware configurations, other products and any software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

- a. The Offeror is made aware, pursuant to 01 NCAC 05B .0501, that in soliciting offers, any or all offers received may be rejected. The basis for rejection may include, but not be limited to the following:
 - i. The offer is deemed unsatisfactory as to quantity, quality, delivery, price or service offered;
 - ii. The offer fails to comply with conditions of the solicitation document or with the intent of the proposed contract;
 - iii. The Department determines there is a lack of competition;
 - iv. error(s) in specifications or indication that revision(s) would be to the State's advantage;
 - v. Cancellation of or changes in the intended project or other determination that the proposed requirement is no longer needed;
 - vi. Limitation or lack of available funds;
 - vii. Circumstances which prevent determination of the most advantageous offer and selection in accordance with N.C.G.S. § 143-135.9; or
 - viii. Any determination that rejection would be to the best interest of the State.
- b. If all offers are rejected, the solicitation may be cancelled in its entirety, or the Department may negotiate with one or more sources of supply that may be capable of satisfying the requirements.
- c. The Offeror is cautioned that this is a Request for Proposal, not a request to contract, and the Department reserves the unqualified right to reject all offers deemed failing to meet minimum qualifications, not responsive, incomplete, or non-compliant with the requirements described herein; or when such rejection is deemed to be in the best interest of the Department or the State of North Carolina.
- d. The Department may also:
 - i. Modify provisions of this RFP in response to changes in law or as required by CMS;

- ii. Waive any formality or informality;
 - iii. Waive a specification or requirement of the RFP if it is in the best interest of the Department;
 - iv. Waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
 - v. Negotiate directly with one or more Offerors, to achieve a contract that is in the best interest of the Department, if the responses to this solicitation demonstrate a lack of competition, or offers are found non-responsive; and/or
 - vi. Cancel this RFP at any time. Notice of Cancellation will be posted on the NC eVP website.
- e. In the event all proposals are rejected, and the Department enters into negotiation, pursuant to 01 NCAC 05B .0503, the Department reserves the right to award a contract to the Offeror or Offerors, which, in its opinion, has (have) made the best proposal through the negotiation process.

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

Any and all amendments or revisions to this document shall be made by written addendum from the Agency Procurement Office. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendors contact regarding this RFP with anyone other than the State's contact person may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.

6.1.5 E-PROCUREMENT

This is an E-Procurement solicitation. Sub-Paragraph #38 of *Attachment B: Department of Information Technology Terms and Conditions* applies to this solicitation.

6.1.6 ELECTRONIC VENDOR PORTAL

The State has implemented the NC eVP that allows the public to retrieve award notices and information on the Internet at <https://evp.nc.gov>. Results may be found by searching by Solicitation Number or agency name. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

When a Vendor protests a contract awarded by the agency, the agency and Vendor shall comply with the following:

- a. The Vendor shall deliver a written request for a protest meeting to the agency head or the agency head's designee within fifteen (15) calendar days from the date of contract award. The Vendor's request shall contain specific reasons and any supporting documentation regarding why there is a concern with the award. If the request does not contain this information or the agency head determines that a meeting would serve no purpose, then the agency head, within ten (10) calendar days from the date of receipt may respond in writing to the offeror and refuse the protest meeting request. **Note:** Contract Award notices are sent only to the Vendor awarded the Contract, and not to every person or firm responding to a solicitation. Proposal status and Award notices are posted at <https://evp.nc.gov/>. If the protest letter contains or points to anything deemed or marked confidential and/or proprietary, Protester must include a redacted copy of the protest letter in accordance with Section 7.10 Confidentiality of Offers of this RFP.
- b. If the protest meeting is granted, the agency head shall schedule the meeting within thirty (30) calendar days after receipt of the letter, unless a later date is accepted by the protesting party

and the agency. The agency shall provide written notice of the date and time of the protest meeting to any awarded vendor. The awarded Vendor may attend the protest meeting and provide a response to the protest allegations, but is not required to do so. If the awarded Vendor submits a response in writing, it shall be provided to the protester by the Department before the protest meeting. Each party will be given a set period of time in which to present their side. The protester and awarded Vendor (if attending) may be represented by legal counsel of their own choosing and at their own expense. Within ten (10) calendar days from the date of the protest meeting, the agency head or their designee, shall respond to the protesting Vendor in writing with a final agency decision.

- c. If a protest is determined by the agency head or their designee to be valid then the following outcomes may occur:
 - i. The award and issued purchase order shall be canceled and the solicitation for offers to contract is not re-bid;
 - ii. The award and issued purchase order shall be canceled and the solicitation for offers to contract is re-bid;
 - iii. The award and issued purchase order shall be canceled and the contract shall be awarded to the next lowest priced, technically competent, qualified Vendor, if that Vendor agrees to still honor its submitted bid.
- d. If the Vendor desires further administrative review after receiving a decision under paragraphs a. or b., the protesting party may, within sixty (60) days from the date such decision is received, file a contested case petition with the Office of Administrative Hearings (OAH) in accordance with N.C.G.S. §150B-23.

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 SITE VISIT OR PRE-OFFER CONFERENCE - RESERVED

6.2.2 QUESTIONS CONCERNING THE RFP

Vendors contact regarding this RFP with anyone other than the contact person listed on Page One of this RFP may be grounds for rejection of said Vendor's offer.

Written questions concerning this RFP must be received by the stated deadline. They must be submitted via the Ariba Sourcing Tool's message board. Please enter "Questions Solicitation RFP" as the subject for the email. Questions should be submitted in the following format:

Question #	RFP Section	RFP Page Number(s)	Vendor Question
1	(Example: 5.4.a)	64	Question regarding specific issue?
2			

6.2.3 ADDENDUM TO RFP

If a Pre-Proposal Conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State will be posted to the Ariba Sourcing Tool and shall become an Addendum to this RFP. Vendors' questions posed orally at any Pre-Proposal Conference must be reduced to writing by the Vendor and submitted via the Ariba Sourcing Tool's message board. Oral answers are not binding on the State.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State Ariba Sourcing Tool for any and all Addenda that may be issued prior to the offer opening date.

6.2.4 COSTS RELATED TO OFFER SUBMISSION

Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.

All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.

6.2.5 VENDOR EXCEPTIONS – RESERVED

6.2.6 ALTERNATE OFFERS

The Vendor may submit alternate offers for various levels of service(s) or products meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s) addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services or products and offer at specific pricing. If a Vendor chooses to respond with various service or product offerings, each must be an offer with a different price and a separate RFP offer. Vendors may also provide multiple offers for software or systems coupled with support and maintenance options, provided, however, all offers must satisfy the specifications.

Alternate offers must be submitted in accordance with the proposal submission instructions and clearly labelled “**RFP 30-2025-037-DHB, Alternate Offer, Name of Vendor**” and numbered sequentially with the first offer if separate offers are submitted. The legend “**Alternate Offer for ‘Name of Vendor’**” must be in bold type of not less than 14-point type on the face of the offer and on the text of the alternate offer.

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

6.2.9 NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- “This offer does not constitute a binding offer”;
- “This offer will be valid only if this offer is selected as a finalist or in the competitive range”;
- “The Vendor does not commit or bind itself to any terms and conditions by this submission”;
- “This document and all associated documents are non-binding and shall be used for discussion purposes only”;

- “This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties”; or
- A statement of similar intent.

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Learn how to register a business in the state of North Carolina at: <https://www.nc.gov/working/business-nc/start-my-business>

6.2.11 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC eVP allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the at the following website: <https://evp.nc.gov>.

This RFP is available electronically on the electronic NC eVP at the following website: <https://evp.nc.gov>.

6.2.12 VENDOR POINTS OF CONTACT

POINT OF CONTACTS AFTER CONTRACT AWARD:

Below are the Vendor Points of Contact to be used after award of the Contract.

VENDOR CONTRACTUAL POINT OF CONTACT	VENDOR TECHNICAL POINT OF CONTACT
[NAME OF VENDOR]	[NAME OF VENDOR]
[STREET ADDRESS]	[STREET ADDRESS]
[CITY, STATE, ZIP]	[CITY, STATE, ZIP]
Attn: Assigned Contract Manager	Attn: Assigned Technical Lead

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:

- Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.
- Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
- Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.
- Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services

and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.

- e. Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.
- f. Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.
- g. **Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not be considered as a response to this solicitation.

6.3.2 OFFER ORGANIZATION

Within each section of its offer, Vendor should address the items in the order in which they appear in this RFP. Forms, or attachments or exhibits, if any provided in the RFP, must be completed, and included in the appropriate section of the offer.

- a. **Contents of Proposal:** This section should contain all relevant and material information relating to the Vendor's organization, personnel, and experience that would substantiate its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If any relevant and material information is not provided, the offer may be rejected from consideration and evaluation. Offers will be considered and evaluated based upon the Vendor's full completion and response to the following, and any additional requirements herein, or stated in a separate Exhibit.
- b. **Offer Format:** The proposal must contain the entire completed and signed Execution page of this RFP must be placed at the front of the proposal. Each page must be numbered. The proposal should contain a table of contents, which cross-references the RFP requirement and the specific page of the response in the Vendor's offer.
- c. **Proposal Content:** This Section lists the required content for completion of this RFP. Vendor shall populate all attachments of this RFP that require the Vendor to provide information and include an authorized signature where requested. The RFP response should be arranged in the following order:
 - 1. Letter of Transmittal to include:
 - i. the submitting organization's legal name and employer identification number (EIN);
 - ii. the name, title, telephone and fax number, and e-mail address of the person authorized to negotiate the Contract on behalf of the organization;
 - iii. the name, title, telephone and fax number, and e-mail address of the person to be contacted for clarification;
 - iv. **Completed Attachment D** along with detailed description of the Vendor's organization to include the following:
 - Date Established;
 - Ownership (public company, partnership, subsidiary, etc.);
 - If incorporated, state of incorporation must be included;
 - Background of the organization (not to exceed three (3) pages);

- Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's organization has been in business, whichever is less.
2. **Completed and Signed** version of the **Execution Page**, along with the body of the RFP and signed receipt pages of any addenda released in conjunction with this RFP;
 3. **Completed Cost Proposal Workbook**: Cost form to be completed in accordance with **Section 4** and instructions found in **Attachment E**;
 4. **Completed** and **signed Attachment F**: Vendor Certification Form;
 5. **Completed Attachment G**: Location of Workers Utilized by Vendors;
 6. **Completed Attachment H**: Completed Past Performance Questionnaires from References in accordance with instructions provided for completion;
 7. **Completed Attachment I**: Financial Review Form and copies of Financial Statements as further described in Section 7.2;
 8. **Confirm Acceptance of Attachment J**: Enterprise Architecture. Vendor must confirm acceptance to adhering to the Department's requirements regarding developing and maintaining enterprise architecture information and artifacts using the tools and processes established by the Department.
 9. **Completed Attachment K**: Key Personnel in accordance with the Instructions provided for completion;
 10. **Completed Attachment M**: Contract Administrators;
 11. **Completed Attachment N**: Deliverables and Milestones Schedule in accordance with the instructions provided for completion in paragraph 2.0 Milestones;
 12. **Completed Attachment O**: Business Continuity Plan in accordance with the Instructions provided for completion;
 13. **Completed Attachment P**: Disaster Recovery Plan in accordance with the Instructions provided for completion;
 14. **Completed** and **signed** version of **Attachment Q**: State Certifications;
 15. **Completed** and **signed** version of **Attachment R**: Federal Certifications;
 16. **Completed** and **signed** version of **Attachment S**: Business Associate Agreement;
 17. **Completed** and **signed** version of **Attachment T**: Technical / Management Proposal to be provided in accordance with the instructions provided for completion;
 18. **Completed** and **signed** version of **Attachment X**: Request for Proposed Modification To The Terms and Conditions;
 19. **Completed** and **signed** version of **Attachment Y**: Minimum Qualifications;
 20. **Current** independent 3rd party assessment report in accordance with Section 3.3.2, paragraph b, subparagraphs i)-iii);
 21. **Completed** Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") in accordance with Section 3.3.2, paragraph a.;
 22. **Completed** Privacy Threshold Analysis (PTA) in accordance with the description of the deliverable DEL-SEC-002 in Attachment N: Deliverables and Milestones Schedule; and

23. **Completed and signed** version of **Attachment AC: GenAI Disclosure and Fact Sheet**

ADHERENCE TO INSTRUCTIONS: Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.

6.3.3 OFFER SUBMITTAL

The Vendor's proposal is subject to the conditions made a part hereof and the receipt requirements described herein, must be submitted as indicated below.

- a. **Vendor must submit its proposal in response to this solicitation to the Ariba Sourcing Tool. Paper and email copies will be deemed non-responsive, and the proposal will not be considered. Proposals submitted by physical mail delivery or in person delivery in response to this solicitation will be deemed non-responsive and will not be considered further. Files must not be password-protected and must be capable of being copied to other media.**
- b. **INSUFFICIENCY OF REFERENCES TO OTHER DATA:** Only information that is received in response to this RFP will be evaluated. Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation. The Department will not click on any links to access information.
- c. **It is the responsibility of the Vendor to submit their proposal in accordance with these instructions to the Ariba Sourcing Tool by the specified time and date of opening. All electronic proposal submissions are subject to the conditions made a part hereof. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues.**
- d. **Proposal and Cost Proposal Workbook must be submitted to the Ariba Sourcing Tool.**
- e. Vendor's Proposal and Cost Proposal Workbook must be separate files and clearly named (e.g. **RFP 30-2025-037-DHB, Vendor's Name, Proposal**) and (e.g. **RFP 30-2025-037-DHB, Vendor's Name, Cost Proposal**).
- f. If your proposal is being submitted as multiple files, then the file names must be clearly **noted**. **For example: RFP 30-2025-037-DHB, Vendor's Name, Proposal 1 of 2; RFP 30-2025-037-DHB, Vendor's Name, Proposal 2 of 2.**
- g. Vendor must submit **one (1) executed (signed) electronic copy of its proposal**.
- h. Proposals must be submitted with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to submit a signed proposal shall result in disqualification. All proposals must comply with *Section 6.3.1 General Instructions for Offer and Section 6.3.2 Offer Organization*.
- i. Vendor must submit one (1) electronic copy of Vendor's **redacted proposal** to the Ariba Sourcing Tool in accordance with Chapter 132 of the General Statutes, Public Records, identified as **RFP 30-2025-037-DHB, Vendor's Name, Proposal Redacted**. For the purposes of this RFP, redaction means to edit a document by obscuring or removing information that is considered confidential and/or proprietary by Vendor and that meets the definition of Confidential Information set forth in G.S. 132-1.2. If Vendor's proposal does not contain Confidential Information, Vendor must submit a signed statement to that effect as **RFP 30-2025-037-DHB, Vendor's Name, Statement of Confidential Information**. If no redacted proposal is submitted by the Vendor, then the Department may use the unredacted proposal for any public record requests. Redacted copies provided by the Vendor to the Department may be released in response to public record requests without notification to the Offeror.

- j. This RFP is available electronically on the NC eVP at the following website: <https://evp.nc.gov>
- k. Proposal documents as submitted must include the entire RFP, proposal, and all addenda. Linked or referenced documents from web or other locations cannot be included and will not be considered or evaluated. Hyperlinks and uniform resource locators (URLs) are not permitted in any of the proposal documents.

For Vendor training on how to use the Ariba Sourcing Tool to view solicitations, submit questions, develop responses, upload documents, and submit offers to the State, Vendors should go to the following site: <https://eprocurement.nc.gov/training/vendor-training>.

Questions or issues related to using the Ariba Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM EST to 5:00 PM EST.

6.3.4 FALSIFIED INFORMATION

The Department may initiate proceedings to debar an Offeror from participation in the offer process and from Contract Award as authorized by North Carolina law if it is determined that the Offeror has withheld relevant or provided false information.

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer.

Complete Attachment G: Location of Workers Utilized by Vendor and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (*Attachment I*), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

- a. For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.
- b. For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.
- c. The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

- a. Pursuant to N.C.G.S. §143B-1350(h)(1), Agencies must conduct a risk assessment, including whether the Vendor has sufficient financial resources to satisfy the agreed upon limitation of liability prior to the award of a contract with Vendor.
- b. Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
- c. Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

Vendor should present its license or support agreements for review and evaluation. Terms offered for licensing and support of Vendors' proprietary assets will be considered.

The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees or other similar costs.

7.5 RESELLERS - RESERVED

7.6 DISCLOSURE OF LITIGATION

The Vendor's failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Agreement.

- a. The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or Key Personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. The Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.
- b. The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or

subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.

- c. All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the DIT Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.

7.7 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or Services with any Department, institution or agency of the State.

7.8 SECURITY AND BACKGROUND CHECKS

All Vendor personnel who need access to project resources must have a security background check performed by their vendor prior to onboarding. Upon State's request, the Vendor must provide the background check reports of the personnel.

The State reserves the right to conduct a security background check or otherwise approve any employee or agent provided by the Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the State's security or other similar requirements.

7.9 ASSURANCES

In the event that criminal or civil investigation, litigation, arbitration, or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of the Agreement, causes the State to be reasonably concerned about:

- a. the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions; or
- b. whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

All offers and any other RFP responses shall be made public as required by the NC Public Records Act and GS 143B-1350. Vendors may mark portions of offers as confidential or proprietary, after determining that such information is excepted from the NC Public Records Act, provided that such marking is clear and unambiguous and preferably at the top and bottom of each page containing confidential information. Standard restrictive legends appearing on every page of an offer are not sufficient and shall not be binding upon the State.

Certain State information is not public under the NC Public Records Act and other laws. Any such information which the State designates as confidential and makes available to the Vendor in order to respond to the RFP or carry out the Agreement, or which becomes available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.

7.11 PROJECT MANAGEMENT

All project management and coordination on behalf of the Agency shall be through a Single Point of Contact (SPOC) designated as the MES Program Project Manager. The Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor's work. All work performed pursuant to the Agreement shall be coordinated between the MES Program Project Manager and the Vendor Project Manager.

The Vendor shall employ a robust project management methodology tailored to the scope of work and complexity of the engagement described in the RFP. The Vendor shall provide project management services that align with the Department processes and tools, including the development and maintenance of a detailed Project Work Plan (PWP) that supports transparent reporting, tracks milestones and dependencies, and integrates with the Department's Integrated Master Schedule (IMS).

The Vendor shall describe and provide the project management methodology (waterfall, agile, hybrid, or others) and sequencing that will be used to implement the project.

7.11.1 RISK AND ISSUE MANAGEMENT PROCESS

Vendor must align its Risk and Issue Management Process with the Department, which describes the processes to be employed by the Department and Vendor to ensure that risks and issues are identified, classified, monitored, and mitigated in a visible fashion. The Risk and Issue Management Process establishes procedures for documenting and updating risks and issues to ensure that all items are:

- i. Clearly identified and categorized based on severity, likelihood, and potential impact
- ii. Assigned to responsible owners for tracking and resolution
- iii. Logged in the Department's centralized repository for visibility and auditability
- iv. Regularly reviewed and updated to reflect current status and any changes in mitigation or resolution plans
- v. Escalated appropriately when thresholds are exceeded or resolution is delayed
- vi. Linked to mitigation strategies and contingency plans to minimize disruption

- vii. Closed formally with documented outcomes and lessons learned following the Department Risk and Issue Management Process.
- a. The Risk and Issue Management Process includes procedures where the Parties interact to progressively reduce the program's exposure to events that threaten accomplishment of its objectives. The Vendor shall comply with the following:
 - i. In coordination with the Contract Administrator, Vendor must promptly identify, categorize, and report risks and issues to mitigate potential impact. Categorization of risks and issues should follow the Department's severity, occurrence, and risk score metrics. Reporting of the risks and issues should occur within the Department defined tools.
 - ii. The Business Owner and Contract Manager will review this information within the Department defined tool to confirm if the risk or issue requires modifications.
 - iii. The risk and issue information should be presented through the Vendor's weekly status meeting. As applicable, the risks and issues should be presented through a weekly RAID meeting as well.
 - iv. The risks and issues should be reviewed at least weekly to ensure they reflect current status and any changes in mitigation or resolution plans. The Vendor shall promptly notify the Department when a threshold is exceeded or resolution is delayed.
 - v. The Vendor shall formally close all risks and issues with documented outcomes and lessons learned.
- b. The Risk and Issue Management Process shall apply to all risks and issues identified by the Vendor, the Department, and any impacted parties.
- c. The Vendor's approach to risk and issue management will be subject to review as part of the Risk & Issue Management Plan deliverable. Additional contract requirements outline the Department's expectations for ongoing risk and issue management beyond this deliverable.

7.12 MEETINGS

The Vendor is required to lead and/or participate in a weekly status meeting during the DDI/Implementation/Closeout and applicable Operations & Maintenance (O&M) Phases of the project.

- a. These meetings will include an agenda containing updates, including but not limited to status, implementation, schedule, testing, training, risks, issues, actions, decisions, defects, and change management functions.
- b. The Vendor is required to lead and/or participate in stand-up meetings with the project team to address progress, risks, issues, and roadblocks to ensure the project deliverables and milestones are met as outlined in *Attachment N: Deliverables and Milestones Schedule*.
- c. Failure to participate in weekly status and/or stand-up meetings, two (2) consecutive or rescheduled meetings, may result in termination of the Contract.
- d. The Vendor is required to meet with State personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Contract. Meetings will occur as problems arise and will be coordinated by the State. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract.

7.13 RECYCLING AND SOURCE REDUCTION - RESERVED

7.14 SPECIAL TERMS AND CONDITIONS

7.14.1 PERFORMANCE BOND – RESERVED

7.14.2 CHANGE MANAGEMENT REQUEST PROCESS

Vendor must align its Project Change Request Management Process with the Department, which describes the processes to be employed by the Department and Vendor to ensure that changes are captured, planned, and implemented in a visible, controlled, and orderly fashion. The Change Request Management Process establishes procedures for documenting and controlling contract changes to ensure that all contract changes are:

- i. Necessary.
 - ii. Documented correctly in the Change Request Form (to be provided to the Vendor upon contract award) and include a detailed description of the impact to the project describing its severity and criticality.
 - iii. Evaluated to consider interfaces and IT environments.
 - iv. Evaluated against available resources.
 - v. Evaluated for cost reasonableness versus benefit, schedule, and performance trade-offs.
- a. The Change Request Management Process includes procedures where the Parties interact to propose, refine and if agreement is reached, sign off on the Project Change Request forms after approval by the Division's Governance Process. The Vendor shall comply with the following:
- i. In coordination with the Contract Administrator, Vendor must provide supporting information through the use of the change request management process as outlined herein. Completion of the Change Request Form includes a complexity assessment and the development of a level of effort (LOE).
 - ii. The Business Owner and Contract Manager will review this information to determine if the CR requires a new funding request or can be accommodated through funding set aside and approved for Necessary System Changes. Changes that have no impact to cost, schedule, scope or performance are administrative. Administrative changes, inclusive of those that may have a cost impact, but are determined to be within the scope of the contract, can be funded through the NSC. If a change is not administrative, it requires a contract amendment.
 - iii. The CR information will be presented through the Division's Governance Process. Vendors must allow a minimum of fourteen (14) days for approval. The Division's assigned project manager will determine the appropriate governance committee and present the CR information.
 - iv. Change Requests of an administrative nature (not resulting in a Contract Amendment) do not require approval by the Centers for Medicare and Medicaid Services (CMS). All Contract Amendments require CMS approval prior to execution. Contract amendments require an additional sixty (60) calendar day review/approval cycle from CMS.
 - v. Any new solution scope changes from approved change requests, resulting in either administrative changes or amendments, must be added to the solution project timeline.
- b. The State's Change Request Management Processes will not define or direct the manner in which each Party seeks internal approval of changes within that Party's decision-making hierarchy.
- c. Vendor shall not be entitled to compensation for any Services performed unless the Change Request Management Process is followed and approved by the governance committees in which all changes will be evaluated.

- d. The Change Request Process shall apply to all proposed Changes to the Services provided by the Vendor.
- e. Changes deemed reasonable, necessary, or proper that are made in the ordinary course of the Vendor's provision of Services that do not affect service levels, scope or time frames shall be made at no additional cost to the State.

7.14.3 MITA FRAMEWORK AND TECHNICAL ARCHITECTURE SEVEN STANDARDS AND CONDITIONS – RESERVED

7.14.4 PERFORMANCE MANAGEMENT

The Vendor is responsible for the performance and quality of all contracted work required by the Contract. DHHS will monitor the vendor's performance, review reports furnished by the Vendor, and review any available data to the State to determine how the Vendor is performing against the contractual performance objectives. If the Vendor does not meet a performance objective in this RFP or standard outlined in the Service Level Agreements (SLAs) DHHS requires that the Vendor develop a Corrective Action Plan (CAP). The CAP should describe the issue, what action the Vendor is taking to correct the issue, and the anticipated timeframe to return performance to contractually obligated levels.

The State will monitor and manage the Vendor performance through the following metrics and reports, including but not limited to:

- a. Service Level Agreements (SLAs)
- b. Monthly reports such as:
 - i. Backup Reports (detailing failed backups and subsequent remediation)
 - ii. Patching Reports (detailing failed patching efforts and subsequent remediation)
 - iii. Security Reviews
- c. Review of contract deliverables
- d. Approval of contract deliverables
- e. Operations Reviews
- f. Comprehensive Business Reviews
- g. Compliance Audits

7.14.5 RETAINAGE

N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts.

- a. For this procurement, this will include withholding a retainage of 10% of each invoice, less any accrued service credits, and will be paid upon confirmation by the Contract Administrator that the Vendor has delivered services in accordance with the specifications and SLAs.
- b. The State will also withhold the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4).
- c. The services herein will be provided consistent with and under these services performance review and accountability guarantees.

7.14.6 CMS CERTIFICATION – RESERVED

7.14.7 FUNDING TO IMPLEMENT NECESSARY SYSTEM CHANGES (NSC) - RESERVED

7.14.8 ESCROW AGREEMENT – RESERVED

7.14.9 STATE CONTRACT REVIEW

This RFP and subsequent contracts are exempt from the State contract review and approval requirements pursuant to G.S § 143B-216.80(b)(4).

7.14.10 TECHNICAL SOFTWARE CHANGES / UPDATES

The Vendor will notify DHHS of any changes to the technical platform including but not limited to software updates, platform changes, hosting changes, or functional updates. The Department categorizes changes as Routine Operational Changes, Functional Changes, or High impact Changes and will categorize a change at the Department's discretion. Descriptions of the changes with examples and required action are as follows:

- a. Routine Operational Changes – Routine operational changes are generally accepted to be changes to the platform that do not impact the functionality of the software or system but may impact the availability of the system. Examples could be security patching, changes to adjacent systems that impact availability, or routine operational processes such as server reboots. For these events the Vendor must use the existing Tech Ops release processes to notify DHHS.
- b. Functional Changes – Functional changes include any updates to the software or technical platform that will impact the functionality of the system. Functional changes must be approved using the DHHS Medicaid governance processes prior to initiating the development and testing of the new or changing functionality. In addition, other Departmental processes such as end-to-end testing, readiness, and deployment may also apply at the Department's discretion. Once these changes have completed development and are ready for deployment, the Vendor must use the existing Medicaid deployment processes and Tech Ops release processes.
- c. High Impact Changes – High impact changes are any modifications to the system or technical platform that result in materially significant changes to the functionality of the system, or significant changes to the technical platform. Examples of high impact changes are major software version upgrades, hosting platform changes such as migrating the technical platform from an on prem data center to the cloud, or changes to the underlying software or platform sub systems. Changes in this category must be presented to the Department in writing and approved by the Department before any work commences. The Department will define the appropriate executive governance venues for the Vendor to present the project.

A document describing the changes should include at a minimum a description of the full scope of the work, costs, risks, schedule, where the work is being performed, impacted deliverables, system availability impacts, and contingency plans. At the Department's discretion additional information may be requested. In addition, these changes must be approved through the DHHS Medicaid governance processes prior to initiating the development and testing of the new or changed functionality. Other Departmental processes such as end to end testing, readiness, and deployment may also apply at the Department's discretion. Once these changes have completed development and are ready for deployment, the Vendor must use the existing Medicaid deployment processes and Tech Ops release processes.

7.15 TECHNICAL OPERATIONS

- a. Processes - The Vendor must comply with all DHHS Technical Operations (Tech Ops) team processes and procedures included herein. The Tech Ops processes may change over time,

and any changes to these processes shall be mutually agreed upon between the Vendor and the Department. Any Tech Ops processes that impact the cost or scope will be managed through the Change Request Management Process as described in section 7.14.2. Upon contract execution and prior to implementation, the Tech Ops team will provide an onboarding process which will detail all specific processes and procedures the Vendor will follow.

The Department, at its discretion, will track issues reported by the Vendor and may require a more comprehensive corrective action plan if the Department identifies trends in the Vendor's performance.

- b. Retransmissions – If the Vendor receives an Unintelligible Transmission from the Department, the Vendor will immediately notify the Department via the Tech Ops team and the Department shall retransmit as soon as the errors are remediated. If the Vendor is notified by the Department or the Department's vendor of the receipt of an unintelligible transmission, the Vendor shall retransmit as soon as the errors are remediated.
- c. Test Data Transmissions - The Vendor will be required to test all data transmissions with the Department and the Department's agents and subcontractors to validate connectivity, format, and data. This may include data exchanges between the Department and the Vendor, or between the Vendor and other Department subcontractors. The Department will oversee any testing and review results. If the testing is not successful, the Department will define an appropriate remediation period if not defined in other sections of this RFP.

7.16 HELP CENTER

- a. Processes - The Vendor must comply with all DHHS Help Center processes and procedures included herein. The Help Center processes may change over time, and any changes to these processes shall be mutually agreed upon between the Vendor and the Department. Any Help Center processes that impact the cost or scope will be managed through the Change Request Management Process as described in section 7.14.2. Upon Contract execution and prior to implementation, the Help Center team will provide an onboarding process which will detail all specific process and procedures the Vendor will need to follow.
- b. Monitoring - The Help Center phone line, integrated email addresses, and case list will be monitored by the Help Center Monday through Friday from 8am until 5pm. Additionally, if the risk of increased case volume is forecasted in scenarios such as program launches, the Help Center will be monitored during off hours and weekends to ensure proper coverage. The Vendor's designated Help Center point of contact must be able to monitor the case work and respond to potential escalations during these times. The Vendor's Help Center point of contact must attend all weekly stand-up meetings to discuss case progress.
- c. Escalation - Business production issues that cannot be resolved through normal process and procedures must be escalated by the Vendor to the Help Center. The issue will be tracked and resolved via the Help Center. Urgent priority cases, which cause wide-spread impact to a critical business function with no workaround or that can result in possible user harm if not addressed immediately, may be escalated either via the Department or the Vendor. Urgent priority cases will follow the Urgent priority response guidelines below:
 - i. Upon receipt of an Urgent priority case, the Department will organize a rapid response team to include all appropriate internal and external vendors;
 - ii. The Department will initiate a meeting cadence to discuss the urgent issue and develop a plan of action;
 - iii. The Vendor assigned to manage the Urgent priority case must make daily updates, including on weekends and holidays if deemed necessary, in the work-notes of the case

- contained within the Help Center case management application, and be prepared to give further updates on rapid response and Help Center status calls;
- iv. The Help Center team will monitor and may make requests for updates inside the Help Center case management application while the case is open.
- d. Licensing and Training - The Vendor must inform the Department of any additional user licenses for the Help Center case management application, that are required or any users whose licenses need to be decommissioned. If any training is needed, the Vendor must contact the Help Center team for scheduling.

7.17 TESTING

The testing strategy requires close collaboration between the Department and the Vendor. The strategy is designed to provide the Department with oversight of all testing levels and Vendor performance to ensure contract requirements and business needs are met. This includes Vendor testing processes, Vendor testing, Vendor test data management, Vendor defect management, risk and issue management, requirement traceability, and Department acceptance prior to system go-live.

The Vendor will be responsible for the test phases identified as the owner in the table below and for ensuring automation is incorporated where appropriate for new functionality and in the baseline regression suite. The Department will be the primary owner responsible for the UAT and E2E test phases with Vendor support as provided in the table below.

Throughout the module's implementation, the vendor will submit various testing artifacts such as test cases, scripts, reports, and plans to the Department for review and approval. The Vendor will utilize a test execution and reporting tool such as Jira or ALM for test management and reporting, and the selected tool must be configured for PHI, PII, and HIPAA data. Regular status updates are expected throughout the testing process.

Table 7.17-1 Standard Testing Phases provides a listing of testing phases utilized by the State with associated environments, owner, and description of the testing phase.

Testing Phase	Environment	Owner	Description
Unit	Development	Vendor	Tests individual components of the software to validate expected behavior.
SIT	SIT	Vendor	Performed on the integrated system to confirm integration functionality and quality. SIT testing is conducted in the SIT environment.
Regression (includes automated testing)	SIT	Vendor	Executed to confirm that new configurations and developments do not adversely affect existing system design and functionality.
Performance (includes automated testing)	Performance	Vendor	Determines system performance and validates KPIs. Results are measured against baselined performance metrics such as responsiveness, speed, scalability, and stability under variety of load conditions to eliminate performance bottlenecks from the system.
Security	Security/Disaster Recovery	Vendor	Performed to uncover vulnerabilities, threats, and risks in the application to prevent system

Testing Phase	Environment	Owner	Description
			weaknesses and potential loss of sensitive and/or confidential information.
Disaster Recovery	Security/Disaster Recovery	Vendor	Verifies that the Department can restore data and applications according to the defined RTO and RPO.
UAT	UAT	DHHS (with Vendor support)	Formal validation of the module's acceptance criteria in the UAT environment. Provides the end users and business stakeholders the opportunity to gain experience with the system and execute test cases, using the results to determine whether the system is acceptable.
Parallel (as applicable)	Vendor will create one	Vendor	Executed on the "to be" system functionality and compared to production environment's "as is" functionality. Automation is used as applicable.
Conversion/Migration (as applicable)	N/A	Vendor	Validates the successful and accurate transfer of existing production data to the target system, ensuring data integrity and continuation of business operations.
E2E	E2E	DHHS (with Vendor support)	Conducted in the E2E environment to test the entire system (the module, applicable legacy systems, interfaces, and any third-party systems) and validate all integration points identified in the E2E test paths.
Third Party Assessment	Vendor will create one	Third-party vendor, Vendor will support	Performed by a third-party vendor chosen by the State for each module at the end of UAT prior to Operational Readiness Review (ORR) to uncover any potential vulnerabilities, threats and risks in the application which might result in a loss of sensitive and/or confidential information and user control that would need to be remediated prior to Go-Live. The module vendor will support this and remediate any identified defects.

Table 7.17-1 Standard Testing Phases

ATTACHMENT A: DEFINITIONS

- 1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
- 2) **Agency:** The term “Agency” within this RFP is referring to the North Carolina Department of Health and Human Services (NCDHHS). Synonymous with Department.
- 3) **ALM:** Application Lifecycle Management: A framework and set of tools for managing the entire lifecycle of an application, including development, testing, deployment, and maintenance.
- 4) **API:** Application Programming Interface - An interface that provides programmatic access to service functionality and data within an application or a database.
- 5) **BAA:** Business Associate Agreement, as that term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”).
- 6) **BAFO:** Best and Final Offer - Submitted by an Vendor to alter its initial offer, made in response to a request by the issuing agency.
- 7) **BCP:** Business Continuity and Contingency Plans. These plans describe how a vendor’s solution will carry out normal business functions after an unplanned event.
- 8) **Beneficiary:** An individual eligible to receive services from the North Carolina Department of Health and Human Services, Division of Health Benefits (NC Medicaid).
- 9) **Best Value:** Has the same meaning as defined in N.C.G.S. 143-135.9.
- 10) **BPM:** Business Process Modeling is the activity of representing processes of an enterprise so they can be analyzed, improved, and automated.
- 11) **Business Associate:** A person or organization, other than a member of a covered entity’s workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing (see 45 CFR 160.103).
- 12) **Business Day:** Business days mean Monday through Friday from 8:00 AM – 5:00 PM ET. State holidays are excluded. A list of North Carolina State Holidays is located at <https://oshr.nc.gov/state-employee-resources/benefits/leave/holidays>.
- 13) **BCP:** Business Continuity Plan. Plan to ensure that business processes continue during a time of emergency or disaster.
- 14) **Calendar Day:** A calendar day includes the time from midnight to midnight each day. It includes all days in a month, including weekends and holidays. Unless otherwise specified in this RFP, days means Calendar Days.
- 15) **CAP:** Corrective Action Plan - A written document describing the deliberate set of actions to be taken by an entity, deficiency, or non-compliance
- 16) **Change Management Plan:** Plan defined to manage the changes while executing a project.
- 17) **Change Management Process:** Sequence of steps or activities that a change management team or project leader follow to apply change management to a change in order to drive individual transitions and ensure the project meets its intended outcomes.
- 18) **Change Request:** Formal proposal for an alteration to some product or system.

- 19) **CISM:** Certified Information Security Manager: Offered by ISACA, this certification focuses on information security management, including risk management, governance, and incident response. It's designed for professionals who manage and oversee enterprise-level security programs.
- 20) **CISSP:** Certified Information Systems Security Professional: Offered by International Information System Security Certification Consortium, certification in cybersecurity. It covers security architecture, engineering, and management across eight domains, including access control, cryptography, and software development security.
- 21) **Cloud-Based System:** A solution for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- 22) **CLMS:** Contract Lifecycle Management System: a software solution designed to manage the lifecycle of contracts efficiently and securely. It's used by organizations to streamline the creation, execution, tracking, and analysis of contracts.
- 23) **CMS:** The Centers for Medicare & Medicaid Services. This is the agency within the United States Department of Health and Human Services that administers the Medicare program and works in partnership with state governments to administer Medicaid, Children's Health Insurance Program (CHIP), and health insurance portability standards.
- 24) **Contract Effective Date:** The date the Department accepts the Vendor's proposal by signing the RFP Execution Page.
- 25) **Contractor:** The Vendor awarded the Contract to perform the services and requirements defined therein.
- 26) **COTS:** Commercial Off the Shelf. A ready-made solution that is adapted to the specific needs of the State's business.
- 27) **Communications Management Plan:** Policy-driven approach to providing stakeholders with information. The plan formally defines who should be given specific information, when that information should be delivered and what communication channels will be used to deliver the information.
- 28) **CM:** Configuration Management. A systems engineering process for establishing and maintaining consistency of a products performance, functional and physical attributes with its requirements, design, and operational information throughout its life.
- 29) **Cybersecurity Incident (GS 143B-1320):** An occurrence that:
- a. Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
 - b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.
- 30) **DAST:** Dynamic Application Security Testing: Tests a running application for vulnerabilities by simulating external attacks.
- 31) **Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include "Work Product" and means any expression of Licensor's findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.

- 32) **Department:** State of North Carolina Department of Health and Human Services, which is responsible for managing the delivery of health and human related services for all North Carolinians, especially its most vulnerable citizens, which includes children, elderly, people with disabilities, and low-income families. Includes the Division of Health Benefits. Synonymous with Agency.
- 33) **Dev:** Development, Referring to the Development stage of the Software Development Lifecycle.
- 34) **DDI:** Design, Development, and Implementation is a phase in the project cycle.
- 35) **DHB:** Division of Health Benefits. The division within the NCDHHS responsible for implementing Medicaid transformation and administering the transformed Medicaid program.
- 36) **DHHS or NCDHHS:** The North Carolina Department of Health and Human Services. This department is responsible for managing the delivery of health and human related services for all North Carolinians, especially its most vulnerable citizens, which includes children, elderly, people with disabilities and low-income families. The Department works closely with health care professionals, community leaders and advocacy groups; local, state, and federal entities; and many other stakeholders. Synonymous with Agency and Department.
- 37) **Disaster Recovery Plan:** A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
- 38) **DRP:** Disaster Recovery Plan
- 39) **DSA:** The Data Sharing Agreement is a legally binding document that governs the exchange of data between two or more parties such as divisions within the State or between the State and external partners. It outlines the terms, conditions, and under which data is shared, accessed, and used.
- 40) **DUA:** The Data Use Agreement is a legally binding document that governs the sharing, use, and protection of data, such as PHI and other State sensitive data, between the State and an external organization or agency.
- 41) **EBCI Tribal Option:** Eastern Band of Cherokee Indian (EBCI) Tribal Option. The tribal-designed and operated primary care case management entity option developed collaboratively by the Department and the EBCI. This includes the following counties: Cherokee, Graham, Haywood, Jackson and Swain Counties. Eligible Members in the following counties may opt in: Buncombe, Clay, Henderson, Macon, Madison, and Transylvania.
- 42) **End User Documentation:** Documentation that contains information on individual user interface elements (such as grids, navigation panes, data editors, charts, etc.), and provides instructions for end-users about how to solve the most-common tasks with these interface elements.
- 43) **Enterprise Architecture Documentation:** Conceptual blueprint that defines the structure and operation of an organization.
- 44) **Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
- 45) **HIPAA:** Health Insurance Portability and Accountability Act of 1996, as amended and its promulgating regulations.
- 46) **IAST:** Interactive Application Security Testing: Combines elements of SAST and DAST by analyzing applications during runtime with instrumentation.
- 47) **I/DD:** Intellectual and Developmental Disabilities: A category of conditions characterized by significant limitations in intellectual functioning and adaptive behavior, often referenced in Medicaid Tailored Plans.
- 48) **IFB:** Invitation for Bid

- 49) **Implementation Plan:** Detailed document that identifies all milestones and deliverables along with the methodology and sequencing that will be needed for a successful implementation. The Implementation Plan will also include known due dates, constraints or assumptions that will be necessary for detailed implementation planning and scheduling.
- 50) **Implementation Schedule:** Comprehensive list of milestones, deliverables, and tasks along with the associated due dates, durations and resources required for implementation.
- 51) **Incident Management Plan:** Clearly defined and documented plan of action for use at the time of an incident, typically covering the key personnel, resources, services, and actions needed to implement the incident management process.
- 52) **IMS:** Integrated Master Schedule
- 53) **Integration Testing:** This is performed when two or more units have been tested and are integrated into a single structure. It includes testing on the interfaces between the components and the larger structure. This level of testing is used to identify defects prior to SIT.
- 54) **Interface Testing:** Interface testing is performed by the selected Vendor to ensure providers, EDI service centers, business partners, and other Department Vendors can submit transactions over appropriate channels and can send and receive proper acknowledgements and negative responses, including the testing of timeframes between the receipt of a transaction and the notification/response to the submitter for all modes of transmission. This includes any interfaces relating to external systems.
- 55) **ITD:** Information Technology Division of the NC Department of Health and Human Services
- 56) **ITSM:** Information Technology Service Management. The processes used to manage IT services within an organization.
- 57) **Jira:** A widely used project and issue tracking tool that supports agile development, defect management, and test case tracking.
- 58) **Key Personnel:** Any person performing under the Contract whose absence would cause an immediate and substantial risk to Vendor's ability to perform its obligation in the Contract as specified in the Vendor's offer.
- 59) **LoE:** Letter of Extension
- 60) **Lol:** Letter of Interest
- 61) **Medicaid Program:** The joint federal-state health insurance program for low-income individuals and families who cannot afford health care costs. Medicaid serves low-income parents, children, seniors, and people with disabilities.
- 62) **MES:** Medicaid Enterprise System is the current approach to Medicaid management systems that promotes the use of COTS and SaaS products along with modularity and a higher degree of interoperability among systems.
- 63) **MFA:** Multi-Factor Authentication: A security mechanism requiring two or more verification factors (e.g., password + token or biometric) to authenticate a user, reducing the risk of unauthorized access.
- 64) **MFT:** Managed File Transfer. A technology platform that allows organizations to reliably exchange electronic data between systems and people in a secure way to meet compliance needs.
- 65) **MIS:** Medicaid Integration Services. A platform that will provide module vendors with a common infrastructure, which may consist of State developed and third-party solutions and tools, to communicate and integrate using a consistent standards-based approach.
- 66) **MITA:** The Medicaid Information Technology Architecture (MITA) initiative sponsored by the Center for Medicare and Medicaid Services (CMS) is intended to foster integrated business and IT transformation across the Medicaid enterprise to improve the administration of the Medicaid program.

- 67) **MMIS:** The Medicaid Management Information System (MMIS) is an integrated group of procedures and computer processing operations (subsystems) developed to help automate the management of a Medicaid program.
- 68) **MOA** – The Memorandum of Agreement is a formal, legally binding document that outlines the terms and conditions of an arrangement between two or more parties such as State agencies, departments, or external partners.
- 69) **MOU** – The Memorandum of Understanding is a formal, non-binding agreement that outlines the mutual understanding between two or more parties regarding their roles, responsibilities, and intentions in a collaborative effort.
- 70) **Monthly Status Report**-Please see Weekly Status Report definition. Monthly Status Report is a high-level summary produced at the end of every month as described in the Communications Plan.
- 71) **MSA:** Master Service Agreement
- 72) **NCAC:** North Carolina Administrative Code
- 73) **NCDIT or DIT:** The NC Department of Information Technology, formerly Office of Information Technology Services.
- 74) **NC eVP:** North Carolina electronic Vendor Portal - The State of North Carolina's on-line system for advertising solicitations, posting addendums, and publishing award notifications. Vendors can view and search for procurement opportunities <https://evp.nc.gov>.
- 75) **NCFS:** North Carolina Financial System: A system designed to modernize and centralize financial operations across state agencies.
- 76) **NCID:** North Carolina Identity Management: The standard identity management service that allows State, local, business and citizen users to achieve an elevated degree of security and real-time access control to the State's customer-based applications and information.
- 77) **N.C.G.S.:** North Carolina General Statutes
- 78) **NDA:** Non-Disclosure Agreement
- 79) **NIST:** National Institute of Standards and Technology
- 80) **NoC:** Notice of Concern
- 81) **NoD:** Notice of Deficiency
- 82) **NoE:** Notice of Extension
- 83) **NPI:** National Provider Identifier. Standard unique health identifier for health care providers adopted by the Secretary of Health and Human Services in accordance with HIPAA.
- 84) **OAuth2/OIDC:** OAuth 2.0 / OpenID Connect: an authorization framework enabling secure delegated access to resources; OpenID Connect (OIDC) is an identity layer built on OAuth 2.0 for user authentication.
- 85) **ORR:** Operational Readiness Review: It is a formal process used to assess whether a system, service, or program is fully prepared to go live or transition into production.
- 86) **ORT:** Operational Readiness Testing ensures the application and infrastructure have been installed and configured for successful operation in the production environment prior to Go-Live.
- 87) **PHI:** Protected Health Information, as that term is defined in HIPAA.
- 88) **PMO:** Project Management Office responsible planning, organizing and delineating responsibility for the completion of an organizations' specific information technology (IT) goals.

- 89) Program Management:** The process of managing several related projects.
- 90) Project Management Plan:** The primary source of information on the project and project activities. It is a formal document that specifies how the project will be planned, performed, tracked, controlled, and closed. It should also contain a detailed implementation schedule.
- 91) Project Implementation Schedule:** A comprehensive list of planned dates for performing schedule activities and/or tasks with the associated planned due dates, resources, and durations for meeting schedule milestones required for implementation.
- 92) Proposal:** The response to the RFP solicitation submitted to NCDHHS by the Vendor. This is also referred to as the Response or Offer.
- 93) Provider:** The umbrella term used to refer to individual practitioners and facilities, entities, organizations, and atypical organizations or institutions.
- 94) Provider Data Vendor:** Agency or organization that collects and distributes primary source verified provider information.
- 95) Quality Management Plan:** Describes how quality will be managed throughout the lifecycle of the project.
- 96) RASP:** Runtime Application Self-Protection: Security technology embedded in an application that detects and prevents attacks in real time during execution.
- 97) RCA:** Root Cause Analysis: a systematic process used to identify the underlying causes of problems or incidents, with the goal of preventing them from recurring.
- 98) Real-time:** Real-time refers to the synchronous exchange of data between IT systems resulting in immediate access to or update of data on which resides in another IT system.
- 99) Requirements Management:** The process of documenting, analyzing, tracing, prioritizing, and agreeing on requirements and then controlling change and communicating to relevant stakeholders. It is a continuous process throughout a project.
- 100) Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
- 101) Recipient:** Person enrolled in a participating Medicaid program.
- 102) Release Management Plan:** Managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases.
- 103) RF(x):** Shorthand used in acquisition discussions to refer to any type of formal request document (RFP, RFQ, RFI, etc.) used to solicit information, pricing, or proposals from vendors.
- 104) RFI:** Request for Information
- 105) RFP:** Request for Proposal
- 106) RFQ:** Request for Quote
- 107) RFQu:** Request for Qualification
- 108) RPO:** Recovery Point Objective – The maximum acceptable amount of data loss the Department can tolerate after a disruptive event, measured in time.
- 109) RTO:** Recovery Time Objective - The maximum acceptable amount of time it takes to restore a system or application to a functional state after an outage or disruption.
- 110) Regression Testing:** The objective of regression testing is to retest important functionality of the solution/system after changes have been made. This test is often performed after each build.

Regression testing allows a consistent, repeatable validation of each new release of a modified system component or an MES component or COTS solution. This testing ensures reported defects have been resolved for each new release and that no new quality issues have been introduced in the maintenance process.

- 111) RFP:** Request for Proposal is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over \$10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services.
- 112) RBAC:** Role-Based Access Control. Restricts network access based on a user's role within an organization.
- 113) SaaS:** Software as a Service. A software licensing model, which allows access to software a subscription basis using external servers.
- 114) SAST:** Static Application Security Testing: Analyzes source code or binaries for vulnerabilities without executing the program.
- 115) SAE 18 SOC 2 TYPE 2:** A detailed report on the controls of a service organization's systems used to process customer data and the confidentiality and privacy of the information processed by these systems. This report provides assurance of the security, availability, and process integrity of these systems.
- 116) SAML v2:** Security Assertion Markup Language Version 2: An XML-based open standard for exchanging authentication and authorization data between identity providers and service providers, commonly used for SSO.
- 117) SDLC:** System Development Life Cycle. A project management model that outlines the phases required to build an IT system.
- 118) Security Monitoring Plan:** Plan that documents the collection, analysis, and escalation of indications and warnings to detect and respond to security intrusions.
- 119) ServiceNow:** a cloud-based digital workflow platform that helps organizations automate and manage IT services, operations, and business processes on a single, unified platform
- 120) Severity Definitions:** The State reserves the right to adjust the severity level set by the provider.
 - a. Severity Level 1 (Sev1): A critical incident with very high impact;
 - b. Severity Level 2 (Sev2): A major incident with significant impact;
 - c. Severity Level 3 (Sev3): A minor incident with low impact
- 121) Significant Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:
 - a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:
 - i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or
 - ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

- b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.
- 122) SIT:** System Integration Testing. A high-level software testing process to verify that all related systems maintain data integrity and can operate in coordination with other systems in the same environment.
- 123) SLA:** Service Level Agreement. Part of a contract that defines what services a service provider will provide and the required level or standard for those services.
- 124) SPOC:** Single Point of Contact. A person serving as a coordinator or the focal point of information.
- 125) SMA:** State Medicaid Agency. State agency responsible for the distribution of Medicaid benefits.
- 126) SSO:** Single Sign-On: An authentication process that allows a user to access multiple applications or systems with one set of login credentials, improving usability and security.
- 127) State Contract Administrator:** A person who performs administrative functions related to dealing with contracts, like 1) request to bid, 2) evaluating bid, 3) allotment of contract, 4) Implementing contract, 5) measuring completed work, and 6) computing payments.
- 128) Subcontractor:** An entity having an arrangement with the Vendor, where the Vendor uses the products and/or services of that entity to fulfill some of its obligations under the Contract.
- 129) System:** Information technology components for collecting, creating, storing, processing, and distributing information, typically including hardware, software, and data itself. Multiple systems may comprise a Solution.
- 130) TOGAF:** The Open Group Architecture Framework: is a well-established methodology and framework for enterprise architecture, meaning it provides a structured approach for designing, planning, implementing, and governing an organization's IT architecture.
- 131) Technical Specifications:** Means, as used herein, a specification that documents Documentation of the requirements of a system or system component. Typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance standards, or similar terms.
- 132) Test Management Plan:** Plan that documents the activity of managing the computer software testing process.
- 133) Training Plan:** Identifies the training that Vendor is expected to complete over a stated period of time.
- 134) Transition Plan:** Plan that outlines the processes to be followed during the turnover stage of any project.
- 135) Turnover:** The transfer of care, custody and control of the application or service. This includes all software, product licenses, documentation, data, or other intellectual capital associated with the environment.
- 136) TBD:** To be Determined
- 137) Unit Testing:** The lowest testing level, which is used by developers to verify that the implemented code functions as expected.
- 138) Unintelligible Transmission:** Any file or data packet that does not conform with the format of the data exchange or interface, is not readable by the target systems due to a malformed file (i.e., corrupt data, xml that cannot be parsed, etc.), or is incomplete.

- 139) UAT:** User Acceptance Testing in which the system is opened for end users to test in a pseudo production environment. The end users verify the system functions according to all established specifications and that the infrastructure works within the defined constraints.
- 140) Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
- 141) VRAR:** Vendor Readiness Assessment Report, which is completed by the responding vendor, identifies clear and objective security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the Vendor to concisely identify whether an application or Vendor is achieving the most important State Moderate or low baseline requirements.
- 142) WAF:** Web Application Firewall: A security solution that monitors, filters, and blocks HTTP traffic to and from a web application to protect against common exploits such as SQL injection and cross-site scripting (XSS).
- 143) Weekly Status Report-** Involves collecting and disseminating project information, communicating progress, utilization of resources, and forecasting future progress, schedule variances, project risks and issues and status to various stakeholders, as decided in the communication management plan.
- 144) Work Breakdown Structure (WBS)** A deliverable-oriented hierarchical decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables. It organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of the project work.
- 145) Work Product:** Incidental artifact created during the performance of the Contract. All work products created during the performance of the Contract become the property of the State.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

Section 1: General Terms and Conditions Applicable to All Purchases

1) **DEFINITIONS: AS USED HEREIN:**

Agreement means the Master Service Agreement in conjunction with any task order.

Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State in Section 2, Paragraph 2 of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

Services shall mean the duties and obligations undertaken by the Vendor under, and to fulfill, the specifications, requirements, terms and conditions of the Agreement, including, without limitation, providing web browser access by authorized users to certain Vendor databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.

State shall mean the State of North Carolina, the Department of Information Technology (DIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

- 2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.

- 3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.

- 4) **SUBCONTRACTING:** Reserved.

- 5) **TRAVEL EXPENSES:**

All travel expenses should be included in the Vendor's proposed hourly costs. Separately stated travel expenses will not be reimbursed.

In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in

N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.

- 6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State may advise Vendor of any restrictions or changes in specifications required by North

Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.

- 7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Reserved.
- 8) **AVAILABILITY OF FUNDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 3: Availability of Funds
- 9) **ACCEPTANCE PROCESS:**
- The State shall have the obligation to notify Vendor, in writing ten calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.
 - Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations.
 - The State shall have the obligation to notify Vendor, in writing and within thirty (30) days following installation of any software deliverable if it is not acceptable.
 - Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.

The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

- 10) **PAYMENT TERMS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 35: Payment and Invoice Terms
- 11) **EQUAL EMPLOYMENT OPPORTUNITY:** Reserved.
- 12) **ADVERTISING/PRESS RELEASE:** Reserved
- 13) **LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
- 14) **ACCESS TO PERSONS AND RECORDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 1: Access to Persons and Records

15) **ASSIGNMENT**: Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty

(30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

16) **INSURANCE COVERAGE**: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 18: Insurance.

17) **DISPUTE RESOLUTION**: The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) **CONFIDENTIALITY**: In accordance with N.C.G.S. §143B-1350I and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq.* Such information may include trade secrets defined by N.C.G.S. §66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.

- b) Vendor warrants that all its employees and any approved third-party Vendor or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq.* The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.
- c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
- d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
- e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) DEFAULT: In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.

- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.
- c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9 of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) WAIVER OF DEFAULT: Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) TERMINATION: Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.

- a) The parties may mutually terminate the Agreement by written agreement at any time.
- b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
 - i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, as provided for in 9 NCAC 6B .1030 subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.

- ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part, by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.
- ~~iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.~~

22) LIMITATION OF VENDOR'S LIABILITY:

- a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.

- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the Agreement, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 34: Time is of the Essence.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

26) INDEPENDENT CONTRACTORS: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Contractors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.

27) TRANSPORTATION: Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.

28) NOTICES: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 20: Notices

29) TITLES AND HEADINGS: Titles and Headings in the Agreement are used for convenience only and do not define, limit, or proscribe the language of terms identified by such Titles and Headings.

30) AMENDMENT: The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.

31) TAXES: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 33: Taxes

32) GOVERNING LAWS, JURISDICTION, AND VENUE:

- a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina and stipulates that Wake County shall be the proper venue for all matters.

- b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.

33) 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, 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.

34) COMPLIANCE WITH LAWS: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 7: Compliance with Laws

35) SEVERABILITY: In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

36) CHANGES: The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The Department shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.

37) FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT: The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

38) ELECTRONIC PROCUREMENT: (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Services. The Department's third-party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.

- a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E-Procurement Service.** This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement.

Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.

- b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership, or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the Security Breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any Security Breach.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

- a) Vendor has created, acquired, or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire, or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general-purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.
- b) Vendor shall not acquire any right, title, and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data, or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's

internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.

- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become non-infringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.
- e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.
- f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS: In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

- a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.

- b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.
- c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.
- d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.
- e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:
 - i) Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or
 - ii) Terminate the work authorization, or
 - iii) Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.
 - iv) The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER: The Department may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

- a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.
- b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:

- i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
- ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
- c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
- d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

42) TRANSITION ASSISTANCE

- a) If the Contract is not renewed at the end of the Contract Term, or is terminated prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or Termination of the Contract, all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees.
- b) Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Contract, (notwithstanding this expiration or termination) except for those Vendor terms or conditions that do not reasonably apply to such transition assistance.
- c) The Department shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Contract for performance.
- d) If the Department terminated the Contract for cause, then the State will be entitled to offset the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the Department may have otherwise accrued as a result of said cancellation.

Section 2: Terms and Conditions Applicable to Information Technology Goods and Services

- 1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:**
 Deliverables comprising goods, equipment or products (hardware) may contain software for internal operation, or as embedded software or firmware that is generally not sold or licensed as a severable software product. Software may be provided on separate media, such as a CD-ROM or other media, or may be included within the hardware at or prior to delivery. Such software is proprietary, copyrighted, and may also contain valuable trade secrets and may be protected by patents. Vendor grants the State a license to use the Code (or any replacement provided) on, or in conjunction with, only the Deliverables purchased, or with any system identified in the solicitation documents. The State shall have a worldwide, nonexclusive, non-sublicensable license to use such software and/or documentation for its internal use. The State may make and install copies of the software to support the authorized level of use. Provided, however, that if the hardware is inoperable, the software may be copied for temporary use on other hardware. The State shall promptly affix to any such copy the same proprietary and copyright notices affixed to the original. The State may make one copy of the software for archival, back-up or disaster recovery purposes.

The license set forth in this Paragraph shall terminate immediately upon the State's discontinuance of the use of all equipment on which the software is installed. The software may be transferred to another party only with the transfer of the hardware. If the hardware is transferred, the State shall i) destroy all software copies made by the State, ii) deliver the original or any replacement copies of the software to the transferee, and iii) notify the transferee that title and ownership of the software and the applicable patent, trademark, copyright, and other intellectual property rights shall remain with Vendor, or Vendor's licensors. The State shall not disassemble, decompile, reverse engineer, modify, or prepare derivative works of the embedded software, unless permitted under the solicitation documents.

2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:

- a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Scope of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. **This license shall be for the term of the contract, unless terminated as provided herein.** The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any Department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.
- b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.
- c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
- d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.

3) **WARRANTY TERMS:** Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.

- a. Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.
- b. Vendor warrants to the best of its knowledge that:

- i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
 - iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.
- c. UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.

4) RESTRICTIONS: State's use of the Software is restricted as follows:

- a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.
- b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
- c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
- d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

5) SUPPORT OR MAINTENANCE SERVICES: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:

- a) **Error Correction:** If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a

replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.

- b) **Other Agreement:** This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
- c) **Temporary Extension of License:** If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
 - i) Return of the inoperative CPU to full operation, or
 - ii) Termination of the license.
- d) **Encryption Code:** Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
- e) **Updates:** Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.
- f) **Telephone Assistance:** Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 8:00 AM - 5:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) hours or eight (8) hours or next business day, etc. *(edit this time to what you want your response time to be)*, for calls made at any time.

- 6) **STATE PROPERTY AND INTANGIBLES RIGHTS:** The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data, and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 3: Terms and Conditions Applicable to Personnel and Personal Services

- 1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will

possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third-party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third-party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).

- a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
- b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
- c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.

2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Scope of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement"). (Reserve if not needed).

3) **PERSONNEL:** Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be notified to the Agency's Contract Administrator in writing accompanied by the names, *roles*, *resume* and references of Vendor's recommended substitute personnel. *Within ten (10) calendar days of the request for a substitution, the State will notify the Vendor if the recommended substitute is acceptable. If the State does not accept the recommended substitute, the Vendor will have ten (10) calendar days to make another recommendation.* The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.

- a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and

telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.

- b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular workdays and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
- c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
 - i) Such use does not conflict with the terms, specifications, or any amendments to the Agreement, or
 - ii) Such use does not conflict with any procurement law, regulation or policy, or
 - iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
- d) At no time may the Key Personnel Role be vacant. It is the Vendor's responsibility to keep the role filled until the Department approves a substitution.

4) **PERSONAL SERVICES:** Reserved

Section 4: Software as a Service (SaaS) Terms and Conditions

1) **DEFINITIONS:**

Data means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

Support includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.

2) **ACCESS AND USE OF SAAS SERVICES:**

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for

commercial third parties (so-called “service bureau” uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as “confidential” or “proprietary” shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*

- b) The State’s access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State’s normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor’s SaaS tenants for similar Services. Vendor’s right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.
- d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor’s solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
- e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an “ok” or “agree” button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
- f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
- g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.

- h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
- i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.

3) WARRANTY OF NON-INFRINGEMENT; REMEDIES:

- a) Vendor warrants to the best of its knowledge that:
 - i) The services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
- b) Reserved
- c) Reserved
- d) Reserved

4) ACCESS AVAILABILITY; REMEDIES

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services. The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.
- b) Reserved

5) EXCLUSIONS:

- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or services failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services

6) PERFORMANCE REVIEW AND ACCOUNTABILITY: N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) LIMITATION OF LIABILITY: LIMITATION OF VENDOR'S CONTRACT DAMAGES LIABILITY: See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 22: Limitation of Vendor's Liability

- 8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 23: Vendor's Liability for Injury to Persons or Damage to Property
- 9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.
- 10) **TRANSITION PERIOD:**
- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions listed herein.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
 - f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 5: Travel Expenses
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 23: Prohibition Against Contingent Fees and Gratuities
- 14) **AVAILABILITY OF FUNDS:** See Attachment C: Agency Terms and Conditions, Section 1, Paragraph 3: Availability of Funds
- 15) **PAYMENT TERMS (APPLICABLE TO SAAS):**
- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein

but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.

- b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
 - c) For any third-party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
 - d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
 - e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.
- 16) **ACCEPTANCE CRITERIA:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 9: Acceptance Process
- 17) **CONFIDENTIALITY:** See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 18: Confidentiality
- 18) **SECURITY OF STATE DATA:**
- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts,

or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The service provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any Security Breaches within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security control appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii) That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.

- (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the service provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;
 - (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75- 65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security

Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.
- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, another related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - i) The scale and quantity of the State Data loss;

- ii) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
- iii) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
- iv) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall investigate the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.
- o) Secure Data Disposal: When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

ATTACHMENT C: AGENCY TERMS AND CONDITIONS

Section 1: DHHS Department of Health Benefits (DHB)

1) ACCESS TO PERSONS AND RECORDS

- a. Pursuant to N.C.G.S. § 147-64.7 and N.C.G.S. § 143-49(9), the Department, the State Auditor, appropriate State or federal officials, and their respective authorized employees or agents shall have access to persons and premises, or such other locations where duties under the Contract are being performed, and are authorized to inspect, monitor, or otherwise evaluate all books, records, data, information, systems, and accounts of the Contractor, their Subcontractor(s), other persons directed by the Contractor, or Contractor's parent or affiliated companies as far as they relate to transactions under the Contract, performance of the Contract, or to costs charged to the Contract. The Contractor shall retain any such books, records, data, information, and accounts in accordance with Section 1, Paragraph 24, **RECORD RETENTION** of this Attachment C of the Contract. Changes or additional audit, retention or reporting requirements may be imposed by federal or state law and/or regulation, and the Contractor must adhere to such changes or additions.
- b. The State Auditor shall have access to persons and records as a result of all contracts or grants entered by State agencies or political subdivisions in accordance with N.C.G.S. § 147-64.7.
- c. The financial auditors of the Department shall also have full access to all financial records and other information determined by the Department to be necessary for the Department's substantiation of the monthly payment(s). These audit rights are in addition to any audit rights any federal agency may have regarding the use of federally allocated MFP funds.
- d. The following entities may audit the records of this Contract during and after the term of the Contract to verify accounts and data affecting fees or performance:
 - i. The State Auditor;
 - ii. The internal auditors of the affected department, agency or institution; and
 - iii. The Joint Legislative Commission on Governmental Operations and legislative employees whose primary responsibility is to provide professional or administrative services to the Commission.
- e. Nothing in this section is intended to limit or restrict the State Auditor's rights.
- f. This provision shall survive termination or expiration of this Contract.

2) ADVERTISING

Contractor agrees not to use the existence of this Contract or the name of the Department or State of North Carolina as part of any commercial advertising or marketing of its products or services, excepted as permitted under this Contract. A Contractor may inquire whether the Department is willing to act as a reference by providing information directly to other prospective customers. The Department is under no obligation to serve as a reference.

3) AVAILABILITY OF FUNDS

All payments to Contractor are expressly contingent upon and subject to the appropriation, allocation

68/9+, and availability of funds to the Department for the purposes set forth in the Contract. If the Contract or any purchase order issued hereunder is funded in whole or in part by federal funds, the Department's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Contract or purchase order. If the term of the Contract extends into fiscal years after that in which it is approved, such continuation of the Contract is expressly contingent upon the appropriation, allocation, and availability of funds by the N.C. General Assembly for the purposes set forth in this RFP and any resulting Contract. If funds to effect payment are not available, the Department will provide written notification to the Contractor and may terminate the Contract in accordance with TERMINATION of this Section 21 of Attachment. D. of the Contract. If the Contract is terminated, the Contractor agrees to take back any affected deliverables and software not yet delivered under the Contract, terminate any Services supplied to the Department under the Contract, and relieve the Department of any further obligation thereof. The Department shall remit payment for deliverables and services accepted prior to the date of the previously mentioned notice in conformance with the payment terms.

4) BACKGROUND CHECKS AND DISCLOSURE OF LITIGATION AND CRIMINAL CONVICTION AND ADVERSE FINANCIAL CONDITION

The Contractor's failure to fully and timely comply with the terms of this Sections 7.7, 7.8, and 7.9 herein including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Contract and result in Termination for Cause.

- a. Upon execution of this Contract, the Contractor shall notify the State if it, or any of its Subcontractors, or their officers, directors, or their Key Personnel, who may provide services under this Contract, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation, or deception. The Contractor shall promptly notify the Department of any criminal litigation, investigations or proceeding involving the Contractor or any Subcontractor, or any of the foregoing entities' then current officers or directors during the term of this Contract.
- b. The Contractor shall notify the State of any civil litigation, regulatory finding or penalty, arbitration, proceeding, or judgments against it or its Subcontractors during the three (3) years preceding the Effective Period Commencement Date of the Contract, or which may occur during the term of this Contract that involves (1) services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Contractor; and (2) a claim or written allegation of fraud by the Contractor or any Subcontractor hereunder, arising out of their business activities; and (3) a claim or written allegation that the Contractor or any Subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Contractor or its Subcontractors shall be disclosed to the Department to the extent they affect the financial solvency and integrity of the Contractor or Subcontractor.
- c. Contractor agrees not to use any personnel in the performance of this Contract who have been convicted of any of the crimes listed in subpart a. herein above. In addition, Contractor will not use or authorize any Subcontractor to use in the performance of this Contract any persons who have been convicted of any federal or state crime involving antitrust laws, anti-kickback laws, self-referral laws, improper influencing of public officials, or improper management or destruction of public records or financial records.
- d. The Contractor shall notify the State of any legal action that could adversely affect the Contractor's ability to meet the requirements of the Contract.

- e. All notices under subsection a., b., c., and d. herein shall be provided in writing to the State within thirty (30) Calendar Days after the Contractor learns about any such criminal, regulatory, or civil matters or financial circumstances or material change to prior disclosures, unless such matters are governed by the other stated terms and conditions of the Contract. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Contractor may rely on good faith certifications of its Subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.
- f. The Department reserves the right to request a criminal background check on Contractor's employees or independent contractors or the employees of Contractor's approved Subcontractors.
- g. Where requested by the Department, Contractor must obtain, at its own expense, and provide the Department, or its designee, a North Carolina State Bureau of Investigation (SBI) and/or Federal Bureau of Investigation (FBI) background check on all employees prior to assignment.
- h. Contractor shall keep any records related to these verifications in accordance with Section 1, Paragraph 24, **RECORD RETENTION** of this Attachment C. of the Contract.

5) BENEFICIARIES

The Contract shall inure to the benefit and be binding upon the Parties and their respective successors. It is expressly understood and agreed that the enforcement of the Terms and Conditions of the Contract, and all rights of action relating to such enforcement, shall be strictly reserved to the Department and Contractor. Nothing contained in this Contract shall give or allow any claim or right of action whatsoever by any third person. It is the express intention of the Department and Contractor that any such other person or entity receiving services or benefits under the Contract shall be deemed an incidental beneficiary only and not a contractual third-party beneficiary.

6) CHANGE IN CORPORATE STRUCTURE

The Contract shall inure to the benefit and be binding upon the Parties and their respective successors. It is expressly understood and agreed that the enforcement of the Terms and Conditions of the Contract, and all rights of action relating to such enforcement, shall be strictly reserved to the Department and Contractor. Nothing contained in this Contract shall give or allow any claim or right of action whatsoever by any third person. It is the express intention of the Department and Contractor that any such other person or entity receiving services or benefits under the Contract shall be deemed an incidental beneficiary only and not a contractual third-party beneficiary.

7) COMPLIANCE WITH LAWS

- a. Contractor shall comply with all applicable federal and state laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and performance in accordance with this Contract.
- b. Contractor is responsible for ensuring its Subcontractors comply with all laws, rules, regulations, and licensing requirements applicable to Contractor's performance under this Contract, including but not limited to the applicable provisions of (a) Title XIX of the Social Security Act and Titles 42 and 45 of the Code of Federal Regulations; and (b) those laws, rules, or regulations of federal and State agencies having jurisdiction over the subject matter of this Contract, whether in effect when this Contract is signed, or becoming effective during the term

of this Contract.

c. Clean Air Act

- i. Contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.
- ii. Contractor agrees to report each violation to the Department and understands and agrees that the Department will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
- iii. Contractor agrees to include these requirements in each subcontract exceeding one hundred fifty thousand dollars (\$150,000) financed in whole or in part with Federal assistance.

d. Federal Water Pollution Control Act

- i. Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
- ii. Contractor agrees to report each violation to the Department and understands and agrees that the Department will, in turn, report each violation as required to assure notification to the federal agency providing funds hereunder, and the appropriate Environmental Protection Agency Regional Office.
- iii. Contractor agrees that these requirements will be included in each subcontract exceeding one hundred fifty thousand dollars (\$150,000) financed in whole or in part with Federal assistance.

e. Pandemic, Endemic and Other North Carolina State Emergencies

- i. Contractor agrees to comply with all applicable standards, Executive Orders and Department issued guidance for pandemics, endemics, and other North Carolina State emergencies.
- ii. Notice shall be provided by the Department of the standards, orders and Department issued guidance prior to the Effective Date of the requirements, where practical.
- iii. In the event requirements are announced and made effective immediately, such as Executive Orders, the Contractor shall adhere to such requirements.
- iv. Contractor agrees to communicate to Subcontractors for compliance with all applicable standards, orders, and Department-issued guidance.

f. Certifications and Representations

- i. Contractor shall certify annually pursuant to C.F.R. § 200.209 Certifications and Representations that it is in compliance with federal certification and representation requirements regarding Nondiscrimination, Drug-Free Workplace Requirements, Environmental Tobacco Smoke, Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier Covered Transactions and Lobbying.
- ii. Contractor shall certify annually that is in compliance with state certification requirements regarding Verification of Employee Work Authorization, Ineligibility, Prior Convictions and Prior Employment.

8) **CONTRACT ADMINISTRATORS**

Contract Administrators means the persons to whom notices provided for in this Contract shall be given, and to whom matters relating to the administration of this Contract shall be addressed. Contract Administrators for both Parties are included in Attachment M: Contract Administrators.

Either Party may change its administrator or their address and telephone number by written notice to the other Party in accordance with **NOTICES** of this Attachment C of the Contract.

9) CONTRACT DISCLOSURES

Unless otherwise provided herein, Contractor shall complete any initial disclosures required under the Contract within thirty (30) Calendar Days of execution unless another timeframe is approved by the Department. Disclosures should be sent to the Department's Contract Administrator in accordance with **NOTICES** of this Attachment C of the Contract.

10) COOPERATION WITH OTHER STATE VENDORS

Contractor shall cooperate with Department Vendors that are providing goods or services to or on behalf of the Department in relation to Medicaid including those Vendors providing services with respect to system integration, encounter processing, enrollment and eligibility, data analytics, and those engaged by the Department to monitor, validate, or verify Contractor's performance.

11) COUNTERPARTS

This Contract may be executed in two (2) or more counterparts, each, and all of which shall be deemed an original and all of which together shall constitute but one and the same instrument. Any signature page transmitted by electronic mail in portable document format will have the same legal effect as an original executed signature page.

12) RESERVED

13) DISCLOSURE OF CONFLICTS OF INTEREST

The Contractor shall disclose any known conflicts of interest, or perceived conflicts of interest, at the time they arise, as follows:

- a. Disclose any relationship to any business or associate to whom the Contractor is doing business that creates or may give the appearance of a conflict of interest related to this Contract.
- b. By signing the RFP, Contractor certifies that it shall not knowingly take any action or acquire any interest, either directly or indirectly, that will conflict in any manner or degree with the performance of its services during the term of the Contract.
- c. Disclose prior to employment or engagement by the Contractor, any firm principal, staff member or Subcontractor, known by the Contractor to have a conflict of interest or potential conflict of interest related to this Contract.
- d. All notices required by this subsection must be provided to the Department within thirty (30) Calendar Days of Contractor becoming aware of the conflict.

14) ENTIRE AGREEMENT AND ORDER OF PRECEDENCE

This Contract consists of the following documents incorporated herein by reference:

- a. Any amendments, business requirements, or implementation plans, executed by the Parties, in reverse chronological order;
- b. Execution of Contract, if any;
- c. Best and Final Offers and negotiation documents, in reverse chronological order, if any;
- d. Written clarifications, in reverse chronological order, if any;
- e. Addenda to the RFP, in reverse chronological order, if any;

- f. This RFP in its entirety; and
- g. Offeror's proposal.

In the event of a conflict between the Contract documents, the term in the Contract with the highest precedence shall prevail. The Contract documents constitute the entire agreement between the parties and supersede all prior oral or written statements or agreements

15) RESERVED

16) RESERVED

17) INDEMNIFICATION

- a. Contractor shall hold and save the State, its officers, agents, and employees, harmless from liability of any kind, including all claims and losses accruing or resulting to any other person, firm, or corporation furnishing or supplying work, services, materials, or supplies in connection with the performance of this Contract, and from any and all claims and losses accruing or resulting to any person, firm, or corporation that may be injured or damaged by the Contractor in the performance of this Contract and that are attributable to the negligence or intentionally tortious acts of Contractor.
- b. Contractor represents and warrants that it shall make no claim of any kind or nature against the State's agents who are involved in the delivery or processing of Contractor goods and/or services to the State. The representations and warranties in the preceding sentences shall survive the termination or expiration of this Contract. The State, Department, and/or Office of the Attorney General shall have the option to participate at their own expense in the defence of such claim(s) or action(s) filed, and the State shall be responsible for its own litigation expenses if it exercises this option.
- c. Contractor shall hold and save the Department, State, its officers, agents, and employees, harmless from liability of any kind, including costs and expenses, resulting from infringement of the rights of any third party in any copyrighted material, patented or unpatented invention, articles, device, or appliance delivered relating to this Contract. This provision shall survive the termination or expiration of this Contract.
- d. Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity that otherwise would be available to the Department and State under applicable law.

18) INSURANCE

During the term of the Contract, the Contractor, at its sole cost and expense, shall provide commercial insurance coverage of such type and with such terms and limits as may be reasonably associated with the Contract. At a minimum, the Contractor shall provide and maintain the following coverage and limits:

- a. **Worker's Compensation**: The Contractor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of five hundred thousand dollars (\$500,000), covering all of Contractor's employees who are engaged in any work under the Contract. If any work is sublet, the Contractor shall require the Subcontractor to provide the same coverage for any of his employees engaged in any work under the Contract.

- b. **Commercial General Liability**: General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of two million dollars (\$2,000,000) Combined Single Limit.
- c. **Automobile**: Automobile Liability Insurance, to include liability coverage, covering all owned, hired, and non-owned vehicles, used relating to the Contract. The minimum combined single limit shall be five hundred thousand dollars (\$500,000) for bodily injury and property damage; five hundred thousand dollars (\$500,000) for uninsured/under insured motorist; and five thousand dollars (\$5,000) for medical payment.
- d. **Requirements**: Providing and maintaining adequate insurance coverage is a material obligation of the Contractor and is of the essence of this Contract. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Contractor shall always comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or this Contract. The limits of coverage under each insurance policy maintained by the Contractor shall not be interpreted as limiting the Contractor's liability and obligations under the Contract.

19) **MEDIA CONTACT APPROVAL AND DISCLOSURE**

Contractor shall not use the name or seal of the North Carolina Division of Health Benefits, the North Carolina Department of Health and Human Services or the State of North Carolina in any media release or public announcement or disclosure relating to the terms of this Contract without prior approval of the Department. Contractor shall not provide any information to the media regarding a recipient of services under this Contract without first receiving approval from the Department. In the event the Contractor is contacted by the media for information related to the terms of this Contract, the Contractor shall contact the Department as soon as practical. Contractor must submit any proposed media release regarding the terms of this Contract to the Department for review and approval at least seven (7) State Business Days in advance of intended disclosure, to the extent practicable. The Department may, to the extent reasonable and lawful, timely object to its publication or require changes to the information intended for public release. The requirements of this Section shall not apply to any information the Contractor is required by law or by any court of competent jurisdiction to disclose.

20) **NOTICES**

Any notices permitted or required under the Contract must be delivered to the appropriate Contract Administrator for each Party. Unless otherwise specified in the Contract, any notices shall be in writing and **delivered by email**. In addition, notices may be delivered by first class U.S. Mail, commercial courier (e.g., FedEx, UPS, DHL), or personally delivered provided the notice is also emailed to the Contract Administrator at approximately the same time. All Notices required under this Contract including, but not limited to legal matters, contract termination, allegations of breach, and audits shall be delivered in accordance with this section of the Contract.

21) **OUTSOURCING**

Any Contractor or Subcontractor providing call or contact center services to the State of North Carolina or any of its agencies shall disclose to inbound callers the location from which the call or conduct center services are being provided. If, after award of a contract, the Contractor wishes to relocate or outsource any portion of performance to a location outside of the United States, or to contract with a Subcontractor for any such performance, which Subcontractor and nature of the

work has not previously been disclosed to the State in writing, prior written approval must be obtained from the State agency responsible for the contract. Contractor shall give notice to the using agency of any relocation of the Contractor, employees of the Contractor, or other persons providing performance under a State contract to a location outside of the United States.

22) OWNERSHIP OF DELIVERABLES

All project materials, including deliverables, software, data, and documentation created during the performance or provision of services hereunder that are not licensed to the Department or other State entity, or are not proprietary to the Contractor are the property of the Department and must be kept confidential or returned to the Department, or destroyed. Proprietary Contractor materials shall be identified to the Department by the Contractor prior to use or provision of services hereunder and shall remain the property of the Contractor. Derivative works of any Contractor proprietary materials prepared or created during the performance of provision of services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the Department and the State. This term shall survive termination or expiration of the Contract.

23) PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES

Contractor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for obtaining any Contract or award issued by the State and its Departments and other agencies or entities. The Contractor further warrants that no commission or other payment has been or will be received from or paid to any third-party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the Department in writing prior to acceptance of the Contract or award in question. The Contractor and its authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of the Contract; obligation or Contract for future award of compensation as an inducement or consideration for making the Contract. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for termination of all outstanding contracts. Violations of this provision may result in debarment of the Contractor as permitted by 09 NCAC 06B.1206, 01 NCAC 05B.1520, or other provision of law.

24) RECORD RETENTION

All records and data held by the Contractor as it relates to this Contract shall be retained and maintained as required by North Carolina law, federal law, State and Department Record Retention requirements and policies.

- a. All records created or modified by the Contractor and not duplicated in Department system via interfaces must be retained for ten (10) years, unless a longer or shorter period is required by federal or State law or policy. Federal record retention standards are located in 45 C.F.R. § 74.53. The State policy is mandated by the State Archives of North Carolina.
- b. Records shall not be destroyed, purged, or disposed of without the express written consent of the Department.
- c. If any litigation, claim, negotiation, audit, disallowance action or other action involving this Contract starts before the expiration of the legally required retention period, the records must be retained until completion of the action and resolution of all issues which arise from it.
- d. In the event there are changes in record retention requirements or policies due to North Carolina law, federal law, State or Department record Retention Policies, the Contractor shall make the necessary changes to be in compliance with all Records Retention requirements.

- e. Record Retention requirements included within the body of this Contract, subsequent contracts and amendments are intended to supplement this term. In the event of conflict, the provisions of this term are the controlling requirements.
- f. At the point the Contract terminates/expires, all data must be transitioned to the State in a format prescribed by the Department unless that data has exceeded its archive requirements. The Department may request verification from the Contractor that archive requirements are being met.
- g. This term survives termination or expiration of the Contract.

25) RESPONSE TO STATE INQUIRIES AND REQUESTS FOR INFORMATION

The Contractor shall prioritize requests from the Department to respond to inquiries from any Departments under the State of North Carolina, the North Carolina General Assembly or other government agencies or bodies. Contractor shall respond to urgent requests from the Department within twenty-four (24) hours and according to the guidance and timelines provided by the Department.

26) RIGHT TO PUBLISH - RESERVED

27) SEVERABILITY

If a court of competent authority holds that a provision or requirement of the Contract violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Contract shall remain in full force and effect.

28) SOVEREIGN & GOVERNMENTAL IMMUNITY

Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of sovereign immunity that otherwise would be available to the Department and State under applicable law. Notwithstanding any other term or provision in this Contract, nothing herein is intended nor shall be interpreted as waiving any claim or defense based on the principle of governmental immunity that otherwise would be available to the Contractor under applicable law against a third party.

29) RESERVED

30) SUBCONTRACTORS

- a. Unless otherwise notified by the Department, acceptance of Contractor's proposal includes any Subcontractor(s) specified therein.
- b. Work performed under this Contract by the Contractor or its employees shall not be subcontracted without prior written approval of the Department. Contractor must submit a written request for approval in accordance with **NOTICES** of this Attachment C of the Contract at least thirty (30) Calendar Days prior to the anticipated start of services by the Subcontractor. Any request for Subcontractor approval shall include a completed *Attachment N: Subcontractor Identification Form*.
- c. Upon request and within five (5) State Business Days of such request, Contractor shall provide the Department with complete copies of any contracts made by and between the Contractor and any Subcontractors. The Contractor remains solely responsible for the performance of its Subcontractors. Subcontractors, if any, shall adhere to the same standards required of the Contractor and this Contract. Any contracts made by the Contractor with a Subcontractor shall

include an affirmative statement that the Department is an intended third-party Beneficiary of the Contract; that the Subcontractor has no contract with the Department; and that the Department shall be indemnified by the Contractor for any claim presented by the Subcontractor. Notwithstanding any other term herein, Contractor shall timely exercise its contractual remedies against any non-performing subcontractor and, when deemed appropriate by the Department, substitute another Subcontractor.

- d. The Contractor shall neither participate with nor enter into any agreement with any individual or entity that has been excluded from participation in federal health care programs or has been debarred from doing business with the State of North Carolina.
- e. Any contract(s) between the Contractor and Subcontractor(s) require:
 - i. The Subcontractor to agree that the State, CMS, the DHHS Inspector General, the US Comptroller General, or their designees have the right to audit, evaluate, and inspect its premises, any books, records, contracts, computer or other electronic systems of the Subcontractor relating to its Medicaid enrollees, or of the Subcontractor's contractor, that pertain to any aspect of services and activities performed, or determination of amounts payable under the Contractor's contract with the State;
 - ii. The Subcontractor to agree that the right to audit by the State of North Carolina, the DHHS Inspector General, the US Comptroller General or their designees, will exist through ten (10) years from the final date of the contract period or from the date of completion of any audit, whichever is later; and
 - iii. That if the State, CMS or the DHHS Inspector General determine that there is a reasonable possibility of fraud or similar risk, the State, CMS or the DHHS Inspector General may inspect, evaluate, and audit the Subcontractor at any time.

31) SUBSTANCE USE DATA (42 C.F.R. PART 2)

Contractor is fully bound by the provisions of 42 C.F.R. Part 2 upon receipt of data from DHB that includes Patient Identifying Information (PII) regarding substance use disorder, as those terms are defined by 42 C.F.R. 2.11. Contractor shall implement appropriate safeguards to prevent the unauthorized uses and disclosures of data protected under 42 C.F.R. Part 2. Contractor shall report any unauthorized uses, disclosures, or breaches of data subject to this term and condition, to the Contract Administrators for DHB within three (3) Calendar Days of the unauthorized use, disclosure, or breach. This notice is in addition to any other notice requirement regarding unauthorized disclosure of PII or PHI required by the Contract. Information disclosed to Contractor is limited to that which is necessary for the Contractor to perform its duties under the Contract. Contractor shall not re-disclose information to a third party unless that third party is a contract agent of the Contractor or subcontractor, helping to provide services described in the contract and only if the subcontractor only further discloses the information back to the contractor or lawful holder from which the information originated.

32) SURVIVAL

The expiration, termination, or cancellation of this Contract will not extinguish the rights of either party that accrue prior to expiration, termination, or cancellation or any obligations that extend beyond termination, expiration or cancellation, either by their inherent nature or by their express terms.

33) TAXES

Any applicable taxes shall be invoiced as a separate item and in accordance with this paragraph and applicable laws.

- a. N.C.G.S. § 143-59.1 bars the Department from entering into contracts with Contractors if the Contractor or its affiliates meet one of the conditions of N.C.G.S. § 105-164.8(b) and refuses to collect use tax on sales of tangible personal property to purchasers in North Carolina. Conditions under N.C.G.S. § 105-164.8(b) include: (1) Maintenance of a retail establishment or office, (2) Presence of representatives in the State that solicit sales or transact business on behalf of the Contractor and (3) Systematic exploitation of the market by media-assisted, media-facilitated, or media-solicited means. By execution of the proposal document the Contractor certifies that it and all its affiliates, (if it has affiliates), collect(s) the appropriate taxes.
- b. All agencies participating in this Contract are exempt from federal taxes, such as excise and transportation. Exemption forms submitted by the Contractor will be executed and returned by the using agency.

34) TIME IS OF THE ESSENCE

Time is of the essence in the performance of this Contract and all provisions that specify a time for performance.

35) PAYMENT AND INVOICE TERMS

- a. Contractor shall submit a State of North Carolina Substitute W-9 Form, Request for Taxpayer Identification Number within two (2) State Business Days of contract award. The W-9 can be found at: <https://www.osc.nc.gov/state-north-carolina-sub-w-9>.
 - i. Completed W-9 should be sent to Medicaid.FinanceAP@dhhs.nc.gov.
 - ii. Contractor shall submit verification of submission of required forms via email to the Department's Contract Administrator for contractual matters. Failure to provide a completed form may delay payment to the Contractor.
- b. Contractor shall register for the North Carolina electronic Vendor Portal (eVP) within two (2) State Business Days of execution of the Contract at the following link: <https://evp.nc.gov/>.
- c. Contractor shall submit verification of registration with the North Carolina electronic Vendor Portal (eVP) to the Department's Contract Administrator for contractual matters. Failure to register may delay payment to Contractor
- d. Contractor must submit one (1) invoice per month, no later than the fifteenth (15th) Calendar Day of the month, unless the Department approves another date. Invoices shall state the period of performance (month, year) and include the total amount invoiced for the period.
- e. Invoices must be submitted as follows:
 - i. Electronically to: Medicaid.FinanceAP@dhhs.nc.gov and to the Invoices Electronic Submission Contact in *Attachment M: Contract Administrators*
 - ii. Department accounting staff may be reached at 919-855-4114 for questions regarding invoices.
 - iii. The Department will promptly notify the Contractor of any changes to the information above for submission of invoices.
- f. Payment will only be made for services and/or deliverables accepted by the Department in accordance with the Contract requirements *Attachment E: Cost Proposal* and actual implementation dates.
- g. Except as otherwise provided, the Contractor is responsible for all payments to Subcontractors under the Contract.

- h. Payment terms are not later than thirty (30) Calendar Days after receipt of a correct invoice as verified by the Department.
- i. In the event any invoice is incorrect, and the Department requires changes, the payment terms shall be net thirty (30) Calendar Days from the date the corrected invoice is resubmitted by the Contractor.
- j. The Department reserves the right to dispute an invoice after payment and require the Contractor to include a credit on the subsequent month's invoice to resolve disputes.
- k. Any reductions based on liquidated damages or other performance issues, may be withheld from the Contractor's invoices. Contractor shall provide a credit memo for such reductions within ten (10) Calendar Days, upon Department's request.

Section 2: DHHS Privacy and Security Office (PSO)

1) NCDHHS PRIVACY AND SECURITY REQUIREMENTS

Under this agreement the Vendor shall implement data security measures compliant with industry best practices. Additionally, the Vendor agrees to adhere to the requirements established by the NCDHHS Privacy and Security Office (PSO) in the NCDHHS Privacy and Security policies as well as the NC Statewide Security Policies:

- [NC Statewide Security Policies](https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies) (<https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies>)
- [NCDHHS Privacy and Security Policies](https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/) (<https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/>)

2) COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS

The Vendor shall comply with all applicable laws, ordinances, codes, rules, regulations, licensing requirements, and electronic storage standards concerning privacy, data protection, confidentiality, security, and mandatory reporting including those of federal, state, and local agencies having jurisdiction where business services are provided for accessing, receiving, or processing all confidential information.

If the DHHS Division or Office determines that some or all the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended (HIPAA), or its implementing regulations, including the Privacy Rule (45 C.F.R. Parts 160 and 164, subparts A and E), Security Standards (45 C.F.R. Parts 160, 162 and 164, subparts A and C), and HITECH provision, the Vendor agrees to comply with all HIPAA requirements and will execute such agreements and practices as the Division or Office may require to ensure compliance.

3) BREACH, INCIDENT, AND NOTIFICATION REQUIREMENTS

a. Duty to Report

Regardless of any other notification requirements the Vendor may have under this contract they shall report any suspected or confirmed privacy or security incidents or breaches to the PSO. This includes but is not limited to unauthorized access, use, disclosure, modification, or destruction of DHHS data.

Reports shall be made using the following website <https://security.ncdhhs.gov> no later than 24 hours of initial discovery. If the data is subject to Social Security Administration (SSA), Internal

Revenue Service (IRS) or state tax, or Centers for Medicare and Medicaid Services (CMS) requirements, the report shall be made within one (1) hour, but no later than 24 hours of discovery.

At a minimum, incident reports shall contain to the extent known:

- The nature of the incident
- The date the incident occurred
- The date the vendor became aware of the incident
- The identity of affected or potentially affected individual(s)
- Any specific information known about the incident

b. Investigation

As part of any breach or incident investigation, the Vendor agrees to make good-faith, reasonable efforts to cooperate with DHHS Divisions and Offices to mitigate the damage or harm of such security incidents.

c. Breach Notification

If any applicable federal regulations, state regulations, local law, or rules require the DHHS division/office or the Vendor to give affected persons written notice of a privacy or security breach arising out of the Vendor's performance under this contract, the Vendor shall bear the cost of the notice.

d. Federal Office of Civil Rights (OCR)

If the Vendor is contacted by OCR regarding work being performed under this contract, they shall notify the PSO within 24 hours of initial notification.

4) CONTINUOUS MONITORING:

In addition to the Continuous Monitoring requirements established in *Section 3.3.2: Solutions Not Hosted on State Infrastructure* of this contract, the Vendor agrees to comply with the following:

a) 3rd Party Security Assessment

Vendors providing Infrastructure as a Service, Platform as a Service, and/or Software as a Service for NCDHHS are required to obtain approval from the PSO to ensure their compliance with statewide and departmental privacy and security policies.

To obtain such approval, the Vendor shall annually provide NCDHHS with both a written attestation to its compliance and an industry recognized, third party assessment report, such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, HITRUST CSF and ISO 27001. NCDHHS is required to review these security assessment reports, assess the risk of each vendor, ensure completion of all findings using a Corrective Action Plan (CAP), and provide an annual certification of the Vendor's compliance to the State CIO.

b) NCDHHS Assessment

The NCDHHS Privacy & Security office may perform periodic independent security assessments of Vendor hosted applications on the public/private/hybrid cloud or On-Prem data centers. The Vendor must provide access to their applications' hosting environment and their key resources to NCDHHS designated resources and NCDHHS engaged vendors to perform a privacy & security risk assessment that includes vulnerability analysis, penetration testing, and risk analysis based on the latest NIST 800-53, Federal, State and NCDHHS requirements.

c) Privacy Threshold Analysis

If requested, the Vendor shall work with the NCDHHS to provide a data inventory of all cloud hosted services and assist with the completion of a Privacy Threshold Analysis (PTA) documenting the data classification and the data fields hosted within the cloud, offsite, or Vendor-hosted environment. The Vendor shall review a Privacy Threshold Analysis (PTA) with the NCDHHS Privacy and Security Office annually and assist with updating the PTA when changes to the data being hosted occur.

If, during completion of the PTA, the NCDHHS Privacy and Security Office determines that the contract will involve data classified as Restricted, Highly Restricted, or other sensitive data, a Data Use Agreement (DUA) must be signed prior to restricted or sensitive data being shared with the selected vendor. The current NCDHHS standard DUA template can be accessed here: [Template NCDHHS Data Use Agreement 072025.docx](https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/) (https://policies.ncdhhs.gov/departamental/policies-manuals/section-viii-privacy-and-security/)

5) **OVERSIGHT / RECORD RETENTION:**

North Carolina General Statutes Chapters 121 and 132 govern the retention and disposition of all records located in, maintained by, or in the legal custody of NCDHHS.

Along with Federal record retention requirements, NCDHHS is subject to two retention schedules: the [NCDHHS Records Retention and Disposition Schedule for Grants](https://www.ncdhhs.gov/about/administrative-offices/office-controller/records-retention) (https://www.ncdhhs.gov/about/administrative-offices/office-controller/records-retention), and the [NC Department of Natural and Cultural Resources \(NCR\) Records Retention and Disposition Program Schedule](https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule) (https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule).

Examples of some general retention schedules include:

- Medicaid and Medical Assistance grants and programs are ten (10) years
- HIPAA record retention is six (6) years
- Internal Revenue Service (IRS) record retention is seven (7) years
- Social Security Administration (SSA), the record retention period is seven years
- Grant record retention period is a minimum of five (5) years

These examples represent the minimum data retention requirements. If data maintained under this contract is involved in any litigation, claim, negotiation, audit, disallowance action, or other action before the retention period expires, the retention schedule shall be extended until resolution of all issues. In cases where multiple retention schedules apply, the longer retention schedule shall prevail.

Records developed or maintained under this contract shall not be destroyed, purged, or disposed of without the express written consent of the appropriate NCDHHS Division or Office record or data owner and only in compliance with the published disposition schedule(s).

Any destruction of data must meet all requirements identified in the [Statewide Media Protection Policy](https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment) (https://it.nc.gov/documents/statewide-policies/scio-media-protection/download?attachment). This includes ensuring electronic data is permanently deleted and non-recoverable. Data destruction shall be performed in accordance with the most current revision of NIST Special Publication 800-88. Additionally, a certificate of destruction shall be provided to the NCDHHS data owner upon completion of the data destruction.

6) **USE OF ARTIFICIAL INTELLIGENCE**

The transparent, secure, responsible, and ethical deployment of AI is essential to ensuring accountability and the protection of civil liberties in government operations and decision-making. The Vendor is fully and solely responsible and liable for and must disclose the use of Artificial Intelligence (AI) technologies within the proposed product, service, and performance. These AI technologies include, but are not limited to Machine Learning, Natural Language Processing (NLP), Generative AI (GenAI), Predictive Analytics (Predictive AI), Assistive AI, Conversational AI, and Computer Vision.

Any use of AI in the performance of the contract shall be implemented in compliance with the [North Carolina State Government Responsible Use of Artificial Intelligence Framework](https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment%3Fattachment=).

(<https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment%3Fattachment=>).

If AI is being used, the Vendor's proposal shall include a section which specifically identifies how security and privacy are addressed within the AI portions of the application. Minimally this section shall include the following:

- The purpose and scope of AI's use
- How the AI will be implemented in a manner that is compliant with the seven principles and practices identified in [Framework for Responsible Use of Artificial Intelligence](https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment) (<https://it.nc.gov/documents/nc-state-government-responsible-use-artificial-intelligence-framework/download?attachment>)
- How the Vendor will ensure data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) under the [NC Statewide Data Classification and Handling Policy](https://it.nc.gov/documents/statewide-policies/statewide-data-classification-handling-policy/open) (<https://it.nc.gov/documents/statewide-policies/statewide-data-classification-handling-policy/open>) is not used to train AI models unless explicitly authorized by the NCDHHS Business Owner and the PSO
- Safeguards used to prevent unauthorized access, use, or disclosure of data used by the AI
- Inclusion of a [NIST AI Risk Assessment](https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf) (<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>) as a deliverable in the Vendor's proposal.

NCDHHS reserves the right to authenticate and verify Vendor's adherence to the provisions of this section and Vendor shall make good-faith, reasonable efforts to cooperate with NCDHHS to do so

7) **FLOW-DOWN:**

In addition to the subcontracting requirements in Paragraph 4) of the NCDIT Terms and Conditions, Attachment B, Section: (1) if a sub-vendor is used in the performance of this contract, written approval of the PSO is also required; and (2) Vendor must include, without modification, all the security and privacy terms and conditions in this Attachment C, NCDHHS Privacy and Security Terms and Conditions in each sub-contract.

Section 3: NCDHHS Development of Artificial Intelligence Systems

1) **DEFINITIONS: AS USED HEREIN:**

AI System shall have the meaning set forth in the Advancing American AI Act, section 7223(4) of Pub.L. 117-263.

Custom Development: means any design, modifications, customizations, configurations, or enhancements to AI Systems or associated implementations or workflows, and any related work product or deliverables, in each case developed specifically for the State under this contract, including (a) prompt templates specifically developed for the State under this contract and (b) any modifications, customizations, configurations or enhancements to AI Systems as a result of model training or fine-tuning. For clarity, Custom Development excludes any background intellectual property existing prior to entry into this contract or developed independently by such Vendor or Subcontractor without use of or reference to the State's confidential information or design specifications during the term of this contract.

Data: shall have the meaning set forth in the Attachment B: North Carolina Department of Information Technology Terms and Conditions, Section 4, paragraph 1) Definitions and shall, without limiting the generality of the foregoing, specifically include Data Inputs and Data Outputs.

Data Inputs: means all data, information, PII or content submitted to the AI System, used to fine-tune, test, or validate the AI System, or otherwise provided to the Vendor or Subcontractor in the performance of this contract, including but not limited to user prompts, queries, instructions, source data, documents, and any other information or content submitted or provided by or on behalf of the State.

Data Outputs: means all data, information, PII or content generated by the AI System in the performance of this contract, including but not limited to responses, results, analyses, anonymized data, derivative data, metadata, logs, synthetic data, and any other output or action produced by the AI System.

State Data: collectively means Data Inputs and Data Outputs.

LLM: means a large language model, which is a generative AI model trained on vast, diverse datasets that enable the model to generate natural-language responses to user prompts and the definition includes any decoder or encoder design used in probabilistic language modeling.

Subcontractor: means the licensor of the AI System provided pursuant to this contract, if different from Vendor.

2) **ORDER OF PRECEDENCE:**

The terms and conditions of this section shall apply to this contract notwithstanding any language in this contract or any Subcontractor's commercial terms and conditions purporting to invalidate or override customer purchasing documentation or contract terms or establish a different order of precedence than set forth herein. In the event of a conflict between this section and any term or condition of this contract or a Subcontractor's commercial terms and conditions, the terms and conditions of this section shall control for AI Systems to the extent of the conflict.

3) **INTELLECTUAL PROPERTY RIGHTS:**

- a) Rights in State Data: The State retains full ownership of and will own all State Data, Data Inputs, Data Outputs, and Custom Developments. To the extent the Vendor or Subcontractor obtains any intellectual property rights in State Data, or any improvements, enhancements, feedback, or derivative works thereof, Vendor and Subcontractors hereby assign and transfer all such rights to the State effective immediately upon creation. The Vendor retains ownership of the underlying AI System and base models.

- b) **Vendor License and Permitted Uses:** Neither Vendor nor Subcontractor shall have any rights to use State Data, information provided to the Vendor nor Subcontractor, or Custom Developments; provided, however, that Vendor shall have a limited, revocable, non-exclusive, non-transferable, license to use State Data and Custom Developments solely for the following permitted purposes: (i) performing the specific requirements of this contract; (ii) providing technical support and maintenance as required under this contract; and (iii) such other uses as may be expressly authorized in writing by the State. This license shall be exercised only during the contract period of performance and only through the Vendor or Subcontractors as authorized under this contract.
- c) **Custom Developments and Model Rights:** The Vendor shall: (i) dedicate the Custom Developments, including any custom models resulting from such Custom Developments, to the State's exclusive use; (ii) treat such Custom Developments, custom models and all associated Data as the State's confidential information; and (iii) not use, reproduce, or derive benefit from such Custom Developments or custom models for any other purpose, or for the benefit of any other party, without express written authorization from the State.
- d) **Feedback and Improvements:** The State retains ownership of any feedback provided by the State to the Vendor or Subcontractor with respect to the AI System and any improvements, enhancements, corrections, annotations, or other modifications made to State Data (collectively, "Data Improvements") or Custom Developments, regardless of whether such Data Improvements are generated by State personnel, the Vendor, Subcontractor, or through automated processes. To the extent the Vendor or Subcontractor obtains any intellectual property rights in such feedback or Data Improvements, except for the limited right to use provided herein, Vendor and Subcontractor hereby assign and transfer all such rights to the State effective immediately upon creation.
- e) **State Data Usage**
 - i) **AI Use Disclosure:** Vendor shall disclose the use of any AI System, including any use by a Vendor and Subcontractor in the performance of this contract. This includes both AI Systems that are expressly part of the contracted deliverables as well as any AI Systems utilized in the fulfillment of contract obligations. Unless instructed otherwise by the Contract Administrator, the initial disclosure shall be made in the Vendor's Response to the RFP and shall be amended or supplemented after award no less than thirty (30) days prior to a material change to the facts initially or previously disclosed. The Vendor must use only American AI Systems. The use of foreign AI Systems in the performance of this contract, including any AI components manufactured, developed, or controlled by non-U.S. entities, is prohibited;
 - ii) **Data Handling:** The State Data shall not be used to train, fine-tune, or otherwise improve any LLM or other machine learning or AI models, including those operated by third parties, or to develop or improve the AI System(s) for any other customers or any commercial or non-commercial purposes. State Data shall not be retained, accessed, or used beyond the scope and duration expressly permitted under this contract;
 - iii) **License Grant to State:** Notwithstanding anything to the contrary in the Vendor's licensing terms for the AI System, the Vendor grants to the State an irrevocable, royalty-free, non-exclusive license to use the AI System for the duration of this contract. This license includes the right to: (a) operate and access the AI System through agreed-upon methods; (b) input Data Inputs and receive Data Outputs; (c) allow authorized State personnel and contractors to use the AI System; and (d) integrate the AI System with State systems.

4) CONFIDENTIALITY OF STATE DATA:

The Vendor and Subcontractor shall:

- a) Protect all State Data by treating it as sensitive and confidential in perpetuity;
- b) Not disclose any State Data to any party without prior written permission of the Contract Administrator;

- c) Use State Data solely as required for the performance of the contract and for no other purpose and in no other manner whatsoever;
- d) Implement "eyes off" Data handling procedures that restrict human review of State Data except as strictly necessary to provide the AI System to the State (including ensuring that any human access to State Data must be logged, justified, and limited to the minimum necessary for system functionality);
- e) Implement and maintain appropriate technical and organizational measures to ensure that all State Data is logically and physically segregated from the Data of any other customer or client, and is not commingled with Data of other customers or clients; and
- f) Upon completion, termination or expiration of the contract, unless otherwise directed in writing by the State, securely delete all State Data from the AI System and all its other systems and all copies, backups and derivatives thereof, and certify deletion to the Contract Administrator in writing.

5) AUDIT AND COMPLIANCE:

Vendor Obligations for Compliance, Auditing, and Documentation. The Vendor shall:

- a) Provide, upon State request, and under appropriate confidentiality protections, comprehensive documentation including but not limited to: (a) compliance verification with terms and conditions of this contract; (b) AI System decision-making processes, logic, and operational parameters; (c) system documentation consistent with NIST AI Risk Management Framework guidelines, including system cards or equivalent documentation; (d) privacy controls effectiveness and PII processing prohibition compliance; (e) testing methodologies used to detect and mitigate noncompliance with unbiased AI principles; (f) known biases, limitations, safety concerns, and performance metrics; and (g) any other information necessary for the State to complete an AI Impact Assessment;
- b) Implement human oversight and intervention capabilities, including: (a) mechanisms for human review and override of AI decisions when required; (b) clear escalation procedures for human intervention; and (c) for high-impact AI Systems, automatic recording and retention of decision-making events and rationale. AI is considered high impact when its output serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on rights or safety;
- c) Establish feedback mechanisms allowing the State to: (a) provide performance feedback and improvement requests through formal channels; (b) request system modifications or enhancements; and (c) report operational concerns without requiring incident classification. State Data and State confidential information shall be expressly excluded from any feedback the Vendor may use for system improvement purposes or any other purposes (except solely the performance of the contract);
- d) Submit new model versions and features to State review and testing for compliance with performance standards prior to deployment. Performance standards shall include: (a) accuracy and reliability metrics; (b) security and privacy compliance; and (c) operational effectiveness criteria.

6) DATA PORTABILITY AND INTEROPERABILITY:

The Vendor shall ensure the use of open and standard Data formats and application programming interfaces (APIs) for all Data Outputs, Custom Developments and AI Systems. The Vendor, or any applicable Subcontractor, shall not use proprietary technologies or formats that otherwise require additional licensing or create vendor dependencies.

7) CHANGE MANAGEMENT:

- a) Advance Notice: Vendor shall provide a thirty (30) day written notice before implementing, updating or upgrading any AI enhancements, features, or components being incorporated into the AI services,

including but not limited to modifications to system prompts, behavioral instructions, or other modifications that would impact performance.

- b) State Review: Following State receipt of change notice, the State has thirty (30) business days to test, review, and approve/reject proposed changes for performance and compliance with these terms and conditions.
- c) Version Control: Vendor shall: (a) maintain the previous AI version for ninety (90) calendar days post-deployment of a new version; (b) allow State to opt out of new features while retaining existing functionality by providing notice to the Vendor prior to deployment of the new version; (c) provide rollback capability to the previous version within thirty (30) calendar days if requested within the 90-day period under clause (a) of this section.

8) SYSTEM EVALUATION, TESTING, AND SAFETY MONITORING:

- a) Vendor shall make best efforts to ensure the AI system complies with the following Unbiased AI Principles:
 - i) Truth Seeking: The AI system shall be truthful in responding to user prompts seeking factual information or analysis. The AI system shall prioritize historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory;
 - ii) Ideological Neutrality: The AI system shall be a neutral, nonpartisan tool that does not manipulate responses in favor of ideological dogmas such as Diversity, Equity, Inclusion. Vendor shall not intentionally encode partisan or ideological judgments into the LLM's outputs.
- b) Vendor shall implement ongoing monitoring for bias, and safety issues, and shall:
 - i) Implement continuous improvement processes to enhance detection and mitigation of performance, bias, and safety issues and/or systems generating illegal or prohibited content, including regular evaluation of system outputs (excluding Data Outputs as defined in section 1.0 above) against verified factual sources;
 - ii) Notify the State within 24 hours of identifying any safety issue and provide written updates to the Contract Administrator every twenty-four (24) hours until all mitigation or remediation activities have been completed;
 - iii) Provide, upon request, detailed documentation of mitigation or remediation efforts, including testing results demonstrating resolution;
 - iv) Provide, upon request, quarterly reports summarizing AI System performance, user feedback, and any bias or safety incidents.
- c) The State reserves the right to conduct assessments of the AI model(s) used in connection with the AI System, including bias and safety evaluations, at any time during the contract period of performance.
- d) Vendor shall provide timely cooperation and access to enable effective performance of such assessments, including but not limited to disclosure of the LLM's system prompt, specifications, evaluations, or other relevant documentation.
- e) If the State assessment identifies performance issues with unbiased AI principles, safety concerns, or other harmful outputs:
 - i) State shall provide written notification to the Vendor specifying the nature of the identified issues
 - ii) Vendor shall, at no additional cost to the State, investigate and remediate substantiated issues within thirty (30) calendar days of notification
- f) If remediation efforts fail to adequately address performance, bias, and safety issues:
 - i) State retains the right to suspend use of the AI System until remediation is satisfactorily completed;
 - ii) The State may, at its discretion, initiate procedures for termination for cause in accordance with the terms of this contract;

- iii) The State may seek third-party remediation at Vendor's expense;
- iv) The Vendor shall be liable for any decommissioning costs and reasonable costs associated with transitioning to an alternative solution; and
- v) Vendor shall indemnify and hold harmless the State against any claims, damages, or liabilities arising from demonstrable harm caused by issues that were not properly disclosed or were misrepresented by the Vendor.

ATTACHMENT D: DESCRIPTION OF OFFEROR

Provide the information about the offeror.

Offeror's full name	
Offeror's address	
Offeror's telephone number	
Ownership	☐ Public ☐ Partnership ☐ Subsidiary ☐ Other (specify)
Date established	
If incorporated, State of incorporation.	
North Carolina Secretary of State Registration Number, if currently registered	
Number of full-time employees on January 1 st for the last three years or for the duration that the Vendor has been in business, whichever is less.	
Offeror's Contact for Clarification of offer: Contact's name Title Email address and Telephone Number	
Offeror's Contact for Negotiation of offer: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Contractual Issues: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Offeror's Contact for Technical Issues: Contact's name Title Email address and Telephone Number	

ATTACHMENT E: COST FORM

INSTRUCTIONS to VENDORS

Pricing Tables Submission Instructions:

The Cost Proposal Workbook is required to be completed as part of the RFP submission. Vendors shall provide all-inclusive, turnkey costs for the solution and services described in this RFP, including all direct and indirect costs. The Total Proposed Price is derived from data entered in:

- Sheet 2: Deliverables Costs
- Sheet 3: Software O&M Costs
- Sheet 4: Labor Costs

Vendors must also provide supporting details in Sheet 5: Additional Information, sufficient for the State to have a clear understanding of the Vendor's pricing methodology, cost structure, and labor rates to provide the Solution and services outlined in the RFP.

The electronic version of the Cost Proposal Workbook in Excel format is provided in the Solicitation documents in the Ariba sourcing event.

Summary of Six (6) Worksheets in the Cost Proposal Workbook

1. Instructions – Provides an overview of workbook usage and general guidance.
2. Cost Summary – Auto-calculates the Total Proposed Price using data from Deliverables, O&M, and Labor worksheets.
 - Includes Options to Award: ServiceNow and NCFS integration options are listed for evaluation purposes. Exercise of these options is at the State's sole discretion.
3. Deliverables Costs – Enter firm, fixed prices for all deliverables during the DDI stage and O&M years, including any updates or maintenance.
4. Software O&M Costs – Provide annual costs for software licensing, maintenance, and cloud hosting. Vendors may add other fees with descriptions.
5. Labor Costs – Enter fully burdened off-site hourly rates and estimated hours for key personnel (Attachment K) for both Implementation and O&M stages. Rates must include all expenses (travel, per diem, training, etc.).
6. Additional Information – Document assumptions and basis of estimates to explain pricing methodology.

a) Payments

- i. No payments will be made for items not quoted in the Vendor's Cost Proposal Workbook.
- ii. Each invoice must include a cumulative summary of invoiced amounts through the contract lifecycle.
- iii. Deliverables will be invoiced upon delivery and formal approval by the Department.
- iv. Software hosting, licensing, and maintenance fees will be invoiced monthly at one-twelfth (1/12) of the annual cost.

Basis of Estimates (BOEs):

Vendors must include BOE information to describe any general method, assumptions, or other useful information needed to understand the estimates. The State is interested in understanding how the Vendor estimated the prices in its Proposal and, as such, the Vendor may format the BOEs and assumptions information in any reasonable manner that communicates the required information. BOEs must only be

provided in worksheet 5. Basis of Estimates, contained in the Cost Proposal Workbook, and not in any other worksheets in the Cost Proposal Workbook

The Vendor must describe their BOEs in support of all cost-related worksheets contained in the Cost Proposal Workbook. The State is interested in the *quality* of the BOEs rather than the *volume* of information provided. Vendor's may use estimates driven by bottom-up analysis, analogy, statistical modeling, or any combination of these or other appropriate methods and apply expert judgment where applicable. Note that when using the analogy method, comparisons should be made to *actual* results (e.g., actual labor hours on a project), not proposed quantities (i.e., those included in a previous proposal).

Each major element of a BOE should identify:

General:

- Assumptions having a significant impact on the estimate
- Method(s) of estimation and Results of the estimate
- Pertinent actual data and the source(s) of data used (e.g., previous projects, parametric models, etc.)
- Adjustments made to account for risk (particularly the risk assumed on efforts with fixed prices)

Software-related BOEs must address at least:

- Software/configuration sizing in terms of new, modified, reused, and deleted software/configuration when applicable.
- Other pertinent measurements of the scope of work (e.g., effort associated with the creation of training materials)
- Productivity estimates and how they drive labor estimates
- Derivation of labor quantities and costs
- Derivation of material/non-labor costs (including licensing costs)

Operations-related BOEs must address at least:

- Derivation of labor quantities and productivities
- Derivation of material/non-labor costs

Note that BOEs are not required to describe the derivation of labor rates (compensation, benefits, etc.). In addition, statements such as, "in our experience, it takes approximately XXX hours to complete this effort," do not, by themselves, constitute sufficient BOEs. BOEs should be responded to in the same sequence as the cost tables.

Each invoice submitted for payment must include a summary log of all invoiced amounts through the contract lifecycle. The worksheets contained in the Cost Proposal Workbook must be completed and submitted by the Vendor in accordance with these INSTRUCTIONS to VENDORS and in the Cost Proposal Workbook.

Optional Cost Components – North Carolina Financial System (NCFS) Integration Option and ServiceNow Integration Option

Vendors must complete the Optional Cost Component tables labeled "ServiceNow Integration Option" and "NCFS Integration Option." These costs will be considered as part of the Total Cost of Ownership for evaluation purposes but may or may not be awarded at the time of contract execution. Vendors must include all assumptions and Basis of Estimates in Worksheet 5. Additional Information

Note: The screen images in the following pages are captured from the Cost Proposal Workbook and are provided for reference only. The Cost Proposal Workbook must be completed in Excel format.

Notes

The Offeror must use this Cost Proposal Workbook to provide its Total Proposed all inclusive, turnkey costs associated with the solutions and services outlined in the RFP, including all direct and indirect costs. The total proposed cost is made up of data from worksheets "2. Deliverables Costs", "3. O&M Costs", and "4. Labor Costs". The Offeror should also supply any assumptions and basis of estimated in worksheet "5. Basis of Estimates" sufficient for the State to have a clear understanding of the Offeror's pricing methodology.

In addition to the items below, the State expects Offerors to review the Cost Proposal Instructions in the **Attachment E: Cost Form in the RFP**.

The Offeror must not modify formulas in this workbook and any lines not used must be set to \$0.

Contract Lifecycle Management System

Instructions	
Offeror Name:	<Offeror Name>
Worksheet Title	Instructions
1. Cost Summary	The Cost Summary tab will automatically calculate the Offeror's Total Proposed Price using prices entered by the Offeror in worksheet "2. Deliverables Costs", worksheet "3. O&M Costs" and worksheet "4. Labor Costs". The Offeror should also supply assumptions and basis of estimate in worksheet '5. Additional Information'. The Implementation costs consist of deliverable based costs and labor costs during the implementation period of the project.
2. Deliverables Costs	The Offeror must propose a firm, fixed price for all Deliverable Costs in Implementation and Operation and Maintenance years. The proposed cost per Deliverable must be all-inclusive of initial submission and any updates or maintenance required. Payments will be made using a deliverables-based approach.
3. O&M Costs	The Offeror must provide the ongoing maintenance, services, support, and cloud hosting necessary to provide the solution and services outlined in the RFP. The Offeror may provide any additional costs that are specific to the operations that are not outlined in this Cost Proposal Workbook.
4. Labor Costs	The Offeror must provide the Labor costs for all key personnel used to support the Implementation stage and Operations & Maintenance stage. The labor costs required during the Implementation stage must not include the labor needed to develop the deliverables identified in the Deliverables costs worksheet.
5. Additional Information	The Offeror should provide any basis of estimates and assumptions how costs were developed that enables the State to have a full understanding of the Offeror's pricing methodology.

0. Instructions

Notes								
The Total Proposed Price on this worksheet will be automatically calculated using the totals of prices entered in Worksheets 2. Deliverables Costs, 3. O&M Costs, and 4. Labor Costs.								
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.								
Evaluation considers TCO inclusive of Options to Award (ServiceNow and NCFs). Exercise of options is at the State's sole discretion.								

Contract Lifecycle Management System - Base Solution								
1. Cost Summary								
Offeror Name:		<Offeror Name>						
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2	Total Proposed Costs
Implementation - Deliverables	\$0							\$0
Implementation - Labor	\$0							\$0
Operations and Maintenance - Software Related	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Deliverables		\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Labor	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0

Contract Lifecycle Management System - North Carolina Financial System (NCFs) Integration Option								
1. Cost Summary								
Offeror Name:		<Offeror Name>						
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2	Total Proposed Costs
Implementation - Deliverables	\$0							\$0
Implementation - Labor	\$0							\$0
Operations and Maintenance - Software Related	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Deliverables		\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Labor	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0

Contract Lifecycle Management System - ServiceNow Integration Option								
1. Cost Summary								
Offeror Name:		<Offeror Name>						
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2	Total Proposed Costs
Implementation - Deliverables	\$0							\$0
Implementation - Labor	\$0							\$0
Operations and Maintenance - Software Related	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Deliverables		\$0	\$0	\$0	\$0	\$0	\$0	\$0
Operations and Maintenance - Labor	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0

1. Cost Summary

Notes									
The costs on this worksheet will be automatically updated in the 1. Cost Summary worksheet. Draft versions and maintenance of Deliverables are to be included in each Deliverable cost.									
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.									
Contract Lifecycle Management System - Base Solution									
2. Implementation Costs									
Offeror Name: <Offeror Name>									
Number	Phase	Deliverable	DDI Contract Year 1	O&M Contract Year 2	O&M Contract Year 3	O&M Contract Year 4	O&M Contract Year 5	O&M Option Year 1	O&M Option Year 2
DEL-SEC-001	Planning	Vendor Readiness Assessment Report (VRAR)	Included in Response	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-SEC-002	Planning	Privacy Threshold Analysis (PTA)	Included in Response	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-001	Planning	Vendor Kickoff Presentation	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-002	Planning	Implementation Plan	\$0						
DEL-PROJ-007	Planning	Project Work Plan (PWP)	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TRAIN-001	Development	Training Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-005	Implementation	Requirements Traceability Matrix (RTM)	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-006	Implementation	Weekly Status Meetings & Status Deck	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-QUA-002	Implementation	Operational Readiness Review (ORR)	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-001	Implementation	Master Test Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-002	Implementation	Test Summary Results Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-SEC-005	Implementation	User Access Control Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-SEC-006	Implementation	Privileged User Access Control Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-SEC-007	Implementation	Vulnerability Management Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-SEC-008	implementation	Initial DR/BCP Test Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-ARC-001	Project Lifecycle	System Design Document (SDD)	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-QUA-001	Project Lifecycle	Quality Assurance Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC-004	Project Lifecycle	Privacy and Security Incident Management Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-STAF-001	Project Lifecycle	Staffing Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC-003	Project Lifecycle	Third Party Security Assessment Report	Included in Response	\$0	\$0	\$0	\$0	\$0	\$0
DEL-OPS-001	O&M	Turnover Plan	Not Required	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC-014	O&M	Annual Disaster Recovery Test & AAR	Not Required	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC-009	O&M	Service Organization Control (SOC) 2 Type II Report (or equivalent 3rd party attestation report)	Not Required	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC 016	O&M	Annual Independent Third Party Penetration Test Report	Not Required	\$0	\$0	\$0	\$0	\$0	\$0
DEL-SEC 017	O&M	Annual SOC 2 Type 2 Report	Not Required	\$0	\$0	\$0	\$0	\$0	\$0
Deliverable Costs:			\$0	\$0	\$0	\$0	\$0	\$0	\$0

2. Deliverable Costs

Contract Lifecycle Management System - NCFS Integration Option									
2. Implementation Costs									
Offeror Name:		<Offeror Name>							
Number	Phase	Deliverable	DDI Contract Year 1	O&M Contract Year 2	O&M Contract Year 3	O&M Contract Year 4	O&M Contract Year 5	O&M Option Year 1	O&M Option Year 2
DEL-PROJ-005	Development	Requirements Traceability Matrix	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TRAIN-001	Development	Training Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-002	Implementation	Implementation Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-QUA-002	Implementation	Operational Readiness Review	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-001	Implementation	Master Test Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-002	Implementation	Test Summary Results Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-ARC-001	Project Lifecycle	System Design Document (SDD)	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-QUA-001	Project Lifecycle	Quality Assurance Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-STAF-001	Project Lifecycle	Staffing Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Deliverable Costs:			\$0	\$0	\$0	\$0	\$0	\$0	\$0

Contract Lifecycle Management System - ServiceNow Integration Option									
2. Implementation Costs									
Offeror Name:		<Offeror Name>							
Number	Phase	Deliverable	DDI Contract Year 1	O&M Contract Year 2	O&M Contract Year 3	O&M Contract Year 4	O&M Contract Year 5	O&M Option Year 1	O&M Option Year 2
DEL-PROJ-005	Development	Requirements Traceability Matrix	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TRAIN-001	Development	Training Plan and Schedule	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-PROJ-001	Implementation	Implementation Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-QUA-002	Implementation	Operational Readiness Review	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-001	Implementation	Master Test Plan	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-TEST-002	Implementation	Test Summary Results Report	\$0	Not Required	Not Required	Not Required	Not Required	Not Required	Not Required
DEL-ARC-001	Project Lifecycle	System Design Document (SDD)	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-QUA-001	Project Lifecycle	Quality Assurance Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
DEL-STAF-001	Project Lifecycle	Staffing Plan	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Deliverable Costs:			\$0	\$0	\$0	\$0	\$0	\$0	\$0

2. Deliverable Costs (Option to Award)

Notes							
The costs on this worksheet will be automatically updated in the 1. Cost Summary sheet. The Offeror may enter additional fees and services under the Description column and provide a description for these services It is the responsibility of the Offeror to ensure spreadsheet calculations are correct. Software/Cloud O&M are billed monthly at 1/12 of annual costs; O&M deliverables are billed upon delivery/acceptance (See RFP 4.1 Offer Costs).							
Contract Lifecycle Management System - Base Solution							
3. Operations and Maintenance Costs - Software Related							
Offeror Name: <Offeror Name>							
Operations and Maintenance Costs							
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2
Software Licensing Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Software Maintenance Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Cloud Hosting	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Other Fees - Describe	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total O&M Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Contract Lifecycle Management System - NCFS Integration Option							
3. Operations and Maintenance Costs - Software Related							
Offeror Name: <Offeror Name>							
Operations and Maintenance Costs							
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2
Software Licensing Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Software Maintenance Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Cloud Hosting	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Other Fees - Describe	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total O&M Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Contract Lifecycle Management System - ServiceNow Integration Option							
3. Operations and Maintenance Costs - Software Related							
Offeror Name: <Offeror Name>							
Operations and Maintenance Costs							
Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2
Software Licensing Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Software Maintenance Fees	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Cloud Hosting	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Other Fees - Describe	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Total O&M Costs:	\$0	\$0	\$0	\$0	\$0	\$0	\$0

3. Software O&M Costs

Notes																							
The costs on this worksheet provide the contractor / subcontractor hourly labor rates for the various job titles in Attachment K: Vendor Key Personnel. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Offeror's staff training, project facility, and any other expenses must be included in the Offeror's fixed hourly rates.																							
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.																							

Contract Lifecycle Management System - Base Solution

4. Labor Costs

Offeror Name: <Offeror Name>																														
Job Title	Contract Year 1						Contract Year 2				Contract Year 3				Contract Year 4				Contract Year 5				Option Year 1				Option Year 2			
	Implementation			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance		
	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total
Implementation / Deployment Program Lead / Manager	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$58.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Security Architecture and Compliance Specialist	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Training & Change Management Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Customer Service Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0
Totals:		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0

Contract Lifecycle Management System - NCFS Integration Option

4. Labor Costs

Offeror Name:<Offeror Name>																																						
Job Title	Contract Year 1						Contract Year 2						Contract Year 3						Contract Year 4						Contract Year 5						Option Year 1				Option Year 2			
	Implementation			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance			Operations & Maintenance							
	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total								
Implementation / Deployment Program Lead / Manager	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	34	\$0	\$0.00	0	\$0	\$10.00	1	\$10											
Security Architecture and Compliance Specialist	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
Training & Change Management Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
Customer Service Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0											
Totals:		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		34	\$0		0	\$0		1	\$10											

Contract Lifecycle Management System - ServiceNow Integration Option

4. Labor Costs

Offeror Name: <Offeror Name>																												
Job Title	Contract Year 1						Contract Year 2				Contract Year 3				Contract Year 4				Contract Year 5				Option Year 1			Option Year 2		
	Implementation			Operations & Maintenance			Operations & Maintenance				Operations & Maintenance				Operations & Maintenance				Operations & Maintenance				Operations & Maintenance			Operations & Maintenance		
	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total	Rate	Hours	Total				
Implementation / Deployment Program Lead / Manager	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Security Architecture and Compliance Specialist	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Training & Change Management Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Customer Service Lead	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Quality Assurance Representative	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0	\$0.00	0	\$0				
Totals:		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0		0	\$0				

4. Labor Costs

Notes			
The Offeror should provide any basis of estimates and assumptions on how costs were developed that enables the State to have a full understanding of the Offeror's pricing methodology. Please enter the Cost Area with the assumptions and basis of estimates information in the table below.			
Contract Lifecycle Management System			
5. Additional Information			
Offeror Name: <Offeror Name>			
Item #	Worksheet Name	Cost Area or Element	Assumptions / Basis of Estimates
1			
2			
3			
4			
5			
6			

5. Basis of Estimates

ATTACHMENT F: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature: _____

Date:

Printed Name: _____

Title:

ATTACHMENT G: LOCATION OF WORKERS UTILIZED BY VENDOR – DISCLOSURE STATEMENT

In accordance with the Statewide Information Security Manual (SISM), the State restricts the location of information systems that receive, process, store, or transmit State and Federal data to the United States which includes the following areas: US States, US Territories, US Embassies, and US Military installations (stateside or overseas). This restriction applies to the Vendor and to any subcontractors engaged to provide Services under this Agreement or with access to State Data. The Vendor must ensure that its subcontractor agreements contain the same restrictions and will be responsible for monitoring and enforcing subcontractor compliance at all times.

Pursuant to N.C.G.S. §143B-1361(b), the Vendor must complete and return this Disclosure Statement Attachment F with its solicitation response. The Vendor may attach additional pages to its response if needed. The State of North Carolina will evaluate Disclosure Statement Attachments for additional risks, costs, and other factors associated with its service prior to making an award for any such Vendor's offer. The Vendor must provide the following information in its bid response:

- a. The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the contract and whether any of this work will be performed outside the United States.

Click here to enter text.

- b. The corporate structure and location of corporate employees and activities of the Vendor, its affiliates or any other subcontractors.

Click here to enter text.

- c. Vendor agrees to provide notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States in the event such relocation occurs during the contract term.

Click here to enter text.

- d. Vendor agrees that any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided.

Click here to enter text.

- e. Will any work under this contract be performed outside the United States?

☐

YES

☐

NO

The use of resources or workers located outside the United States is a critical security exception that must be escalated to the State Chief Information Officer for review pursuant to N.C.G.S. §143B-1376(c) and §143B-1320(c). These critical security exceptions are approved only in rare and extenuating circumstances. Vendor should account for this when preparing its response.

ATTACHMENT H: VENDOR REFERENCES/PAST PERFORMANCE

The electronic version of the template for the Past Performance Questionnaire, found in this Attachment H, is provided in the solicitation document within the Ariba sourcing event.

The Past Performance Questionnaires from Vendor references will be used in the evaluation of past performance. The Vendor is responsible for obtaining past performance information from their references and must provide the completed Past Performance Questionnaire from at least three (3) client references for which it has provided services of similar size and scope to that requested herein.

At least one (1) of the three (3) references must be from a State Medicaid program or healthcare organization where the services provided are substantially similar in scope to that proposed in the RFP.

The Department reserves the right to contact any or all of these client references to determine whether the services provided are substantially similar in scope to that proposed in the RFP, and validate the information provided in the Past Performance Questionnaire.

Client references from the NC Department of Health and Human Services, its divisions, programs, or employees are prohibited and will not be considered to satisfy this requirement.

The completed and signed Past Performance Questionnaires, provided from the references to the Vendor, **MUST** be included in the response to this RFP as directed in section 6.3.2 Offer Organization.



NC DEPARTMENT OF
**HEALTH AND
HUMAN SERVICES**

**Business Reference Response to Past
Performance Questionnaire For:
State of North Carolina Request for Proposal (RFP)
Number: 30-2025-037-DHB
Contract Lifecycle Management System (CLMS)**

PART A: Name of Vendor Submitting Proposal

NAME OF VENDOR:

PART B: Company / Respondent Providing Reference

NAME OF COMPANY / AGENCY:

RESPONDENT ADDRESS: CITY, STATE & ZIP:

RESPONDENT TELEPHONE NUMBER:

RESPONDENT E-MAIL ADDRESS:

RESPONDENT NAME AND TITLE:

PART C: Contract Information

PROGRAM TITLE:

BRIEF PROGRAM DESCRIPTION AND WORK PERFORMED:

CONTRACT TYPE (TIME AND MATERIAL, FIXED PRICE, COST):

CURRENT PROGRAM PHASE (DESIGN, OPERATIONS):

PERIOD OF PERFORMANCE (INCLUDING ALL OPTIONS):

CONTRACT DOLLAR VALUE (INCLUDING ALL OPTIONS):

CONTRACTORS ROLE (PRIME OR SUB):

WAS THIS A COMPETITIVELY AWARDED CONTRACT (YES / NO):

PART D: Performance Information

Code	Rating Descriptions
E	EXCEPTIONAL – Performance meets contractual requirements and exceeds many requirements to the Agency's benefit. The contractual performance was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
V	VERY GOOD – Performance meets contractual requirements and exceeds some requirements to the Agency's benefit. The contractual performance was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
S	SATISFACTORY – Performance meets contractual requirements. The contractual performance contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
M	MARGINAL – Performance does not meet some contractual requirements. The contractual performance reflects a serious problem for which the contractor has not yet identified corrective actions or the contractor's proposed actions appear only marginally effective or were not fully implemented.
U	UNSATISFACTORY – Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance being assessed contains serious problem(s) for which the contractor's corrective actions appear or were ineffective.

N/A	NOT APPLICABLE – Unable to provide a rating. Contract did not include performance for this aspect, performance was not observed, or information was not available. Do not know.
-----	--

In the tables that follow, indicate your rating for the contractor's performance by placing an "X" in the appropriate code to the right of each question. Refer to the Rating Descriptions above. Provide supporting information and comments for each response in the space provided. Attach additional pages if more space is needed.

TECHNICAL / BUSINESS EXPERTISE

TE1: Contractor understood the CLMS Solution and provided the technical expertise required to meet contract performance.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE2: Contractor provided staff with appropriate technical skills and training commensurate with those required for successful project completion.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE3: Contractor deployed an CLMS Solution to a State Medicaid program.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE4: Contractor provided an effective solution for the CLMS.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

TE5: Contractor solution that was deployed did not substantially deviate from solution that was proposed.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

QUALITY OF SERVICES

QS1. Contractor provided and followed effective quality control plan to meet program objectives.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

QS2. Contractor corrected deficiencies in a timely manner and pursuant to their quality control procedures.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SCHEDULE AND COST

SC1. Contractor delivered services within the required time period specified by contract requirements.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SC2. Contractor performed the effort within the estimated cost/price and actual costs/rates realized closely reflected the negotiated costs/rates.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SC3. Contractor submitted accurate invoices on a timely basis.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

SC4. Contractor demonstrated cost efficiencies in performing the required effort.						
SUPPORTING INFORMATION:	E	V	S	M	U	N/A

PART E: General Comments and Signature
PLEASE PROVIDE ANY ADDITIONAL COMMENTS CONCERNING THIS CONTRACTOR'S PERFORMANCE, AS DESIRED.

Based on what you know today about the Contractor's ability to execute what they promised in their proposal, would you award another contract to the Contractor, if given the choice? Yes or No. Please explain in the area below.	
Have there been any indications that the Contractor has had any financial problems? Yes or No. Please explain in the area below.	
RESPONDENT SIGNATURE: Please provide your signature confirming the information you have provided is an objective assessment of the Contractor's past performance.	DATE:

Thank you for your prompt response and assistance!

ATTACHMENT I: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form or change the order of the rows or column in the file.

1. Vendor Name:
2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):
3. Have you been in business for more than three years? ☐ Yes ☐ No
4. Have you filed for bankruptcy in the past three years? ☐ Yes ☐ No
5. In the past three years, has your auditor issued any notification letters ☐ Yes ☐ No
addressing significant issues? If yes, please explain and provide a copy of the notification letters.
6. Are the financial figures below based on audited financial statements? ☐ Yes ☐ No
7. Start Date of financial statements:
End Date of financial statements:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments			
b. Accounts Receivable (beginning of year)			
c. Accounts Receivable (end of year)			
d. Average Account Receivable for the Year (calculated)			
e. Inventory (beginning of year)			
f. Inventory (end of year)			
g. Average Inventory for the Year (calculated)			
h. Current Assets			
i. Current Liabilities			
j. Total Liabilities			
k. Total Stockholders' Equity (beginning of year)			
l. Total Stockholders' Equity (end of year)			
m. Average Stockholders' Equity during the year (calculated)			
INCOME STATEMENT DATA			
a. Net Sales			
b. Cost of Goods Sold (COGS)			
c. Gross Profit (Net Sales minus COGS) (calculated)			
d. Interest Expense for the Year			
e. Net Income after Tax			
f. Earnings for the Year before Interest & Income Tax Expense			
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities			

b. Capital Expenditures (property, plant, equipment)			
--	--	--	--

8. Provide annual reports with Financial Statements and management discussion, in electronic format, for the past three complete fiscal years:
9. Provide the following information for the past three complete fiscal years:

ATTACHMENT J: ENTERPRISE ARCHITECTURE

The Department maintains a comprehensive set of Enterprise Architecture information and artifacts that must be created and maintained by each vendor. The Department's Enterprise Architecture standards are based on the Federal Enterprise Architecture framework (FEA), TOGAF and is aligned with the business capabilities and processes described within the Medicaid Information Technology Architecture (MITA) framework as applicable.

The Enterprise Architecture standards require the use of industry standard conventions such as UML2, BPMN and TOGAF to consistently describe all applications and all other architecture. Vendors are required to provide standard documentation of the following architecture areas, during the DDI phase of the project and to maintain this documentation during the O&M phase of the project:

BUSINESS ARCHITECTURE: Describes the business needs, dependencies and outcomes.

APPLICATION ARCHITECTURE: Describes the applications, products or software services used.

DATA ARCHITECTURE: Describes the data, how it is used, stored and transmitted.

INFRASTRUCTURE ARCHITECTURE: Describes the hardware, platforms or infrastructure services used.

PERFORMANCE ARCHITECTURE: Describes the performance measures and metrics that must be met.

SECURITY ARCHITECTURE: Describes the security measures across each of the five above areas.

While this attachment will provide a high-level understanding of the Departments EA standards, the Department maintains the right to add or change required Enterprise Architecture information and artifacts as needed.

Information is entered into enterprise architecture repository using online forms and templates while additional information is provided through attached documents or diagrams. The Department has standardized Microsoft Office products, which will be used as the accepted format for most of the attached artifacts. Other formats are being considered to support the documentation of data models and will be presented to the vendor upon finalization of the standard.

The following table outlines the key concepts that the vendor will be required to document through the EA information and artifacts collected by the Department.

Attachment J: Enterprise Architecture Table 1. Key Concepts	
Business Architecture	Business Capabilities, Business Processes, Functional and Non-Functional Requirements with traceability across the architecture
Application Architecture	Functional Design, Conceptual Design, Detailed Design, Application Data Exchanges, Application Maintenance Procedures, Disaster Recovery Plan, Software and Service Inventory, Application Definitions
Data Architecture	Data Management (Data Development, Operations, Governance, Quality, Dictionary), Data Exchanges, Data Integrations, Data Interfaces, Data Architecture Designs, <u>Conceptual Data Models</u> , Logical Data Models, Physical Data Models
Infrastructure Architecture	User Infrastructure Design, Interface and Data Exchange Infrastructure Design, Cloud/Data Center Infrastructure Design

Performance Architecture	Performance Measures and Metrics, Compliancy Monitoring, Business Performance Monitoring, Application Performance Monitoring, Application Reliability Monitoring, Standards Management
Security Architecture	Business Security and Disaster Recovery, Application Security, Data Security, Infrastructure Security, Security Monitoring.

All Enterprise Architecture information and diagrams must be maintained throughout the life of the solution and must be controlled through Project and Operational Change Management procedures.

ATTACHMENT K: VENDOR KEY PERSONNEL

- a) Key Personnel will be the accountable individuals to the State and will interface directly with existing State staff to form a management team. Key Personnel cost should be included in the fixed support cost and not be viewed as resources billable at an hourly rate. NCDHHS shall have full access to key personnel and 100% of their time be dedicated to this Contract. Any resources proposed as shared must be identified along with the percentage of time expected on this project. Any resources proposed at less than 100% (excluding the Account Manager) must be approved by the State Contract Manager. All other staff should be included in the fixed cost and not be listed as Key.
- b) Vendor must identify key personnel to be assigned for the duration of the Contract. Key Personnel must be identified and mapped to the staffing roles provided in *Attachment K: Table 1: Key Personnel*. Vendor must indicate the name of the proposed individual to perform each role. If a substitution is needed and the appropriate personnel is not immediately available, the Contractor should notify the Department of the interim personnel as they work to obtain the Department approval of the formal substitution request.
- c) If the Vendor must provide additional Key Personnel for consideration, the following information must be provided:
 - i. Name;
 - ii. Role;
 - iii. Experience relevant to the services to be provided under this Contract;
 - iv. Certifications or credentials for the role suggested; and
 - v. Requested effective date.

The Contractor shall provide an updated org chart within five (5) business days of the Department's approval of substitution.
- d) The Vendor must provide a detailed staffing contingency plan for handling sudden and unexpected increases in volume of transactions or the number of users with a description on how the plan will be implemented and coordinated with the Department.

Table 1: Key Personnel

Key Personnel Role	Duties and Responsibilities of the Role	Minimum Certifications, Credentials, and Experience Preferred by NCDHHS
Implementation / Deployment Program Lead / Manager	- Serves as the primary point of contact (POC) and provides high level business support as needed for directing operations throughout the life of the Contract to include: project oversight; participation in all meetings as well as ensures the appropriate stakeholders are represented in meetings. - Ensures all reports, deliverables, and invoices are accurate and timely; manages and updates the project work plan (PWP) and/or project schedule; leads weekly status and stand-up meetings.	4+ years of experience within the last 10 years in managing a program of equal or greater scope 4+ years of experience in system implementation / deployment. - Project management experience, primarily with CLMS implementation or similar enterprise SaaS solutions. - Strong communication and collaboration skills.

Key Personnel Role	Duties and Responsibilities of the Role	Minimum Certifications, Credentials, and Experience Preferred by NCDHHS
	- Provides agendas and captures minutes; provides weekly status reports to manage the project. - Ensures production readiness and support; and available through go-live / project warranty.	Information technology experience preferred.
Security Architecture and Compliance Specialist	- Act as the primary point of contact for the DHHS Privacy and Security Office (PSO). - Ensure the solution complies with federal, state, and agency privacy and security policies and procedures. - Implement and enforce industry-standard security best practices to maintain an optimal security posture for the solution. - Design, develop, and review security documentation and deliverables to ensure alignment with the requirements. - Coordinate with DHHS PSO approved third-party independent assessors to successfully complete the independent privacy and security assessments for Operational Readiness Review (ORR) and Biennial for CEF requirements.	10+ years Security Architecture, 5+ Years in Cloud Security Architecture and Industry standard frame works such as NIST 800-53, HITRUST, SOC2 TYPE2. - Practical experience in implementing Cloud Security Well Architected Principles; Designing and Implementing the Data Security in compliance with the HIPAA regulatory requirement. - Cloud Security Specialist and Vendor Agnostic certifications such as CISSP, CISM is required.
Training & Change Management Lead	- Develop and deliver training curriculum. - Conduct surveys and prepare Training Evaluation Reports. - Support adoption and change management. - Experience in organizational change management and stakeholder engagement.	Four (4) years of experience with Organizational Change Management, adult learning principles, and LMS platforms.
Customer Service Lead	- Manage Tiered support model. - Oversee issue resolution and escalation. - Maintain knowledge base and user assistance. - Provides customer support services via telephone and other mediums such as web portal, and email to the Division to assist in problem solving for individual cases and organizational matters.	- Four (4) years of experience in customer service. - ITIL Foundation certification
Quality Assurance Representative	- Coordinates and oversees all quality functions and reviews. - Ensures all quality deliverables adhere to and align with federal and state program expectations. Serves as point of escalation for quality.	10+ years of QA experience, 7 of which should be management/ leadership of a QA team. - Experience with SDLC and Agile methodologies, testing tools, experience with all phases of testing (e.g., SIT/UAT/E2E), assuring program

Key Personnel Role	Duties and Responsibilities of the Role	Minimum Certifications, Credentials, and Experience Preferred by NCDHHS
	▪ Coordination and oversight of testing phases (e.g., Unit, SIT, UAT, E2E, Regression, Performance, Security), processes, and deliverables. ▪ Ensure requirements traceability (RTM) and coverage for all deliverables. Validate test environments mirror production and meet security/privacy standards. ▪ Coordination and oversight of test planning sessions. ▪ Coordinate and oversight of defect management during execution. Coordinate Production Readiness Testing.	quality standards, proven communication skills/liaison, risk mitigation, and support in technical reviews. ▪ Skilled in automated testing tools and security testing frameworks. ▪ Strong communication for status reporting and risk escalation.

ATTACHMENT L: SERVICE LEVEL AGREEMENTS

Business SLAs (During Implementation, O&M & Transition)

The State has identified the Service Level Agreements (SLAs), as set forth in the table below, that will be monitored throughout the life of the contract. The Vendor must work with the State to drive the automation of all SLA validation, verification, and reporting.

The State and Vendor agree that failure to meet certain performance standards will result in liquidated damages as set forth in the table below. The State reserves the right to adjust the liquidated damages in alignment with the 10% Retainage, described in *Section 7.14.5 Retainage*, of any of the SLAs with thirty (30) days’ notice to the Vendor of changes in the liquidated damages. The change will go into effect upon execution of an Amendment.

The total amount of SLA liquidated damages assessed to the Vendor will at no time exceed 10% of the monthly invoices due.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK
TABLE 1 SERVICE LVEL AGREEMENTS STARTS ON NEXT PAGE

Table 1. Service Level Agreements

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-001	The Vendor must ensure that the solution is available 24 hours a day, 7 days a week, 365 days a year, with a monthly availability of 99.5% uptime, excluding approved planned maintenance downtime. The solution is considered unavailable when any of the capabilities or integrations do not function as described in this RFP and subsequent documentation.	System availability must meet or exceed 99.5% over each Monthly audit period. Availability (%) = (Total Time - Downtime) / Total Time * 100	Monthly	Availability	1. Failure to achieve 99.5% availability shall result in a service credit equal to 10% of the monthly recurring fees, applied against future fees. 2. Failure to achieve 99% availability shall result in a service credit equal to 25% of the monthly recurring fees, applied against future fees. 3. Failure to achieve 95% availability shall result in a service credit equal to 50% of the monthly recurring fees, applied against future fees or may be used to establish eligibility for early termination of the Agreement. If the Services achieve 99.5% availability for the month but are unavailable for a consecutive period of 120 minutes during that month, the Vendor shall provide a credit equal to one pro-rated day of the monthly subscription Services fee, applied to future Services charges.

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-002	The Vendor must notify the Department's Contract Administrator of any solution deficiencies, which are anticipated to cause service disruptions, lasting more than one (1) hour, within thirty (30) minutes of becoming aware of the issue and provide its plan for resolution within four (4) hours of the notification of the deficiency to the Department.	Failure to notify Department and/or provide a resolution plan within the times listed.	On Occurrence	Notification	A 5% service credit of the monthly recurring fees will be applied against future fees for each failure to comply per occurrence.
SLA-003	The Vendor shall use reasonable efforts to correct interruptions and delays with the solution within forty-eight (48) hours of discovery. The Vendor must inform the Department if more than forty-eight (48) hours are needed to resolve the problem and provide a time by which the problem is expected to be corrected.	Failure to notify Department and/or provide a resolution plan within the times listed.	On Occurrence	Availability	In addition to liquidated damages applied for failing to meet the Service Availability requirement (SLA-001), if downtime exceeds 48 hours, the Vendor shall grant pro-rata refunds of fees for the affected period.

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-004	The Vendor must report all, including suspected, privacy/security incidents involving unauthorized access, use, disclosure, modification, or data destruction to the Department Contract Administrator and the DHHS Privacy and Security Office within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare & Medicaid Services (CMS) data, the Vendor must report the incident within one (1) hour after the incident is first discovered. Sufficient technical evaluation will be completed by the Contractor to verify the number of members potentially affected. The Contractor shall share, coordinate, and assist in workarounds (as required) with any impacted modules.	Failure to report within one (1) hour	On Occurrence	Security	10% of monthly retainage for each failure to meet the notification periods identified in the SLA.

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-005	If the Vendor is out of compliance with the Federal, State, and/or DHHS privacy & security policies, a mitigation plan to regain compliance is due to the Department within ten (10) State Business Days, with mitigation and testing to be completed in the timeframe defined in the mitigation plan.	Failure to comply	Monthly	Security	5% of monthly retainage for each occurrence of a mitigation plan that is delayed beyond 10 business days
SLA-006	The Vendor shall perform patching and corrections to mitigate critical security vulnerabilities within seven (7) State business days, high vulnerabilities within thirty (30) State business days, medium vulnerabilities within sixty (60) State business days, and low vulnerabilities within ninety (90) State business days. The Vendor must determine the level of criticality in consultation with the Department and in accordance to the Vulnerability Risk Ratings And Remediation State requirements.	Failure to comply	Monthly	Security	\$5,000 retainage shall be assessed per occurrence per day for Critical vulnerabilities, and \$5,000 per occurrence per week if the patch or correction is not implemented within the Performance Standard timeframe.

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-007	The Vendor will provide a monthly summary report that describes any notifications they have received regarding system problems, incidents, or defects. This report must be provided to the Department Contract Administrator on the first State business day of the month.	Failure to provide summary report	Monthly	Compliance	\$500 retainage shall be assessed for each occurrence
SLA-008	In the event of a disaster, the Vendor shall setup the alternate processing site with a Recovery Time Objective (RTO) of twenty-four (24) hours and a Recovery Point Objective (RPO) within twenty-four (24) hours from the time a disaster is declared.	Failure to restore essential services and information in 24 hours	Per Occurrence	Security	5% of the monthly retainage shall be assessed for each occurrence
SLA-009	In the event of a disaster, the Vendor will restore essential services and information, irrespective of the time the incident occurred, in less than or equal to five (5) minutes 100% of the time.	Failure to restore essential services and information in less than or equal to five (5) minutes 100% of the time.	Per Occurrence	Security	5% of the monthly retainage shall be assessed for each occurrence

SLA ID #	SLA Description	Metric	Frequency	Category	Liquidated Damages
SLA-010	The Vendor must perform Disaster Recovery Testing at a minimum annually once to verify and validate the State-approved Business Continuity Plan and Disaster Recovery Plan and report the DR test results using the standard After Action Report Template provided by the DHHS Privacy and Security Office withing thirty (30) days.	Failure to provide the After-Action Report	Annually	Security	\$500.00 retainage per day shall be assessed for each day beyond the thirty (30) days, until the detailed Business Continuity Plan, Disaster Recovery Plan and Disaster Recovery test results are delivered to the Department
SLA-011	The Vendor shall provide the Corrective Action Plans (CAP) or Plan of Action Milestones (PO&AM) for mitigating the identified gaps in the internal risk assessments, third-party privacy & security assessments, or security audits to the DHHS Privacy & Security Office (PSO) within ten (10) State Business Days.	Failure to provide the CAP or PO&AM	Per Occurrence	Security	5% of monthly retainage for each occurrence of a CAP or PO&AM plan delayed beyond 10 business days.

THE REST OF THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT M: CONTRACT ADMINISTRATORS

Contract Administrators are the persons to whom notices provided for in this Contract shall be given, and to whom matters relating to the administration of this Contract shall be addressed. The Department and the Vendor may change its respective administrator, address, and telephone number by providing written notice.

For the Department:

Contract Administrator for all contractual matters:

Name and Title	Michael Brown, Acquisition Support Specialist
Address	1915 Health Services Way, Raleigh NC 2760
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	208-590-5866
Email Address	Michael.c.brown@dhhs.nc.gov

Contract Administrator for all day-to-day matters:

Name and Title	Brandon Newpher, Associate Director, Technology and MES Contracting
Address	1915 Health Services Way, Raleigh NC 2760
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	919-527-7238
Email Address	brandon.newpher@dhhs.nc.gov

State Privacy and Security Point of Contact:

Name and Title	Tarun Nagireddy, IT Security Architect
Address	1915 Health Services Way, Raleigh NC 2760
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	919-855-3021
Email Address	tarun.nagireddy@dhhs.nc.gov

State Technical Point of Contact:

Name and Title	Bernadette Pyatt, Applications Systems Analyst I
Address	1915 Health Services Way, Raleigh NC 2760
Mail Service Center Address	2015 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	Office: 919-855-3023
Email Address	bernadette.pyatt@dhhs.nc.gov

Invoices Electronic Submission Contact:

Name and Title	Pedro Osorno, Technology Monitoring and Compliance Specialist
Address	1915 Health Services Way, Raleigh NC 2760
Mail Service Center Address	2501 Mail Service Center, Raleigh, NC 27699-2501
Telephone Number	919-855-4100
Email Address	pedro.osorno@dhhs.nc.gov

For the Vendor:

Contract Administrator for all contractual communication:

Name & Title	
Address 1 Physical Address	
Address 2 Mail Service Center Address	
Telephone Number	
Email Address	

Vendor's Technology contact for technical matters:

Name & Title	
Address 1 Physical Address	
Address 2 Mail Service Center Address	
Telephone Number	
Email Address	

ATTACHMENT N: DELIVERABLES AND MILESTONES SCHEDULE

Table 1.0 lists the Deliverables to be provided by the Vendor for this project, along with the anticipated due date and frequency for each Deliverable.

Deliverables submitted by the Vendor should follow industry standards, best practices, and the description provided. Upon submission of the Deliverable(s), the State will review that Deliverable, and acceptance will be in accordance with the *Attachment B: Department of Information Technology Terms and Conditions Acceptance Process*. The Vendor must ensure that, for each deliverable, no more than two review iterations are used to gain acceptance by the Department of the deliverable.

The Vendor must provide deliverables that meet the following minimum quality standards:

- a. Provide accurate and comprehensive content.
- b. Ensure appropriate technical level for the audience
- c. Utilize correct grammar, spelling, and versioning
- d. Ensure diagrams are clear, concise, and add value
- e. Follow industry standards and best practices
- f. Appropriately define and reference information

Informal reviews and walkthroughs of draft and final deliverables are encouraged. When submitting deliverables for review, the Vendor must not submit an excessive number of deliverables to the Department for simultaneous review.

1.0 DELIVERABLES

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-STAF-001	Planning	Staffing Plan	30 Days after Contract Effective Date.	Annually or upon request.	The Staffing Plan demonstrates the Vendor's ability to meet all Contractual staffing requirements. Staffing plan to include key personnel and an organizational structure to comply with all requirements described in this Contract.
DEL-PROJ-001	Planning	Vendor Kickoff Presentation	15 Days after Contract Effective Date	Once	The Vendor will work jointly with DHHS to develop, design and present the kickoff presentation that will provide a clear overview of the project implementation plan which marks the start of vendor onboarding.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-PROJ-007	Planning	Project Work Plan (PWP)	30 Days after Contract Effective Date	Updated as needed throughout project	Vendor must develop and maintain a Project Work Plan that supports transparent reporting, tracks milestones and dependencies, and integrates with the Department's Integrated Master Schedule (IMS).
DEL-TEST-001	Development	Master Test Plan	30 Days Prior to Implementation Phase	Each System Build	The Master Test Plan documents the overall testing approach and plan for each testing phase (Functional/Integration/Load/Stress/UAT/Production). The Master Test Plan will include at a minimum: a. Definition and scope/out of scope of testing for all test phases b. Assumptions/Risks/Dependencies c. Data Strategy and Plan per phase d. Defect Process e. Automation and Manual testing and tools for each test phase f. Entrance / Exit Criteria for each test phase g. Management and testing team procedures / roles and responsibilities / testing procedures / reporting procedures / escalation procedures h. Integration Strategies - describes the integration build process and verification approach i. Test Design - defines the test scenarios in scope / out of scope per test phase
DEL-TRAIN-001	Development	Training Plan	60 Days Prior to Implementation Phase	Annually or When Changed	The Training Plan describes the Vendor's cohesive and responsive training to ensure that all users can be efficient and effective while using the solution, including Vendor's staff, State staff, and external users. The plan reflects the relative lead-time for the development of training materials prior to conducting training classes (including the training of testing participants and all training before implementation); how users' skills will remain current throughout the operations phase; and how the Vendor will build and maintain the training environment. Additionally, it specifies the planned duration of implementation training rollout, including development of Desk Procedures (User Manual) for use in the Operations Phase. The plan specifies delivery media to be used for each training activity and the accessibility of training materials and/or training news before, during, and after training. It describes the process used to identify and track training needs and to evaluate trainee feedback to improve course materials and methods.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					The Training Plan will be updated annually to define the approach and actions to engage stakeholders during training to address specific training activities for the upcoming year and shall be completed at least ninety days prior to the beginning of the Contract year. Training programs and materials require prior approval from the Department's Contract Administrator for day-to-day activities initially and on an ongoing basis before changes to programs and materials are implemented.
DEL-QUA-001	Implementation	Quality Assurance Plan	30 Days after Implementation	Annually or When Changed	The Quality Assurance Plan (QA Plan) is a document consisting of the following: a. Include oversight of performance and processes. b. Measure the completion of deliverables, service delivery problems, and participant satisfaction. c. Provide representation for scheduled meetings to discuss and maintain an adequate project team that can deliver the stated outcomes and audit support.
DEL-QUA-002	Implementation	Operational Readiness Review (ORR)	Prior to Go-Live as per project schedule	Once per implementation; biennial for CEF compliance	Vendor must prepare and submit the Operational Readiness Review package, including security and compliance documentation, and coordinate with DHHS PSO and approved third-party assessors to complete independent privacy and security assessments.
DEL-TEST-002	Implementation	Test Summary Results Report	5 Days after the Associated Testing	Each System Build	For each test phase, the Vendor will develop a comprehensive Test Summary Result Report that describes all completed activities associated with conducting each test. The Test Summary Result Reports are used as 'tollgates'/exit criteria to current test phase and entrance criteria to the next test phase. The Test Summary Results Report is also used in order to document the final test results of all QA activities for each test phase to ensure complete traceability to ensure there are no testing gaps. Each Test Summary Results report contains the following: a. Overview of testing activities / Test Phase / Test Dates / Test Environment (configuration) b. Total Number of Test Cases Executed c. Test Case Final Execution Status (Passed / Failed / NA/ Deferred / Date / Evidence of Completion) d. Total Number of Defects Logged e. Defect Final Execution Status (Passed / Failed / NA / Deferred /

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					Date / Evidence of Completion) f. Requirements Traceability Matrix mapping test cases to requirements providing no gaps in testing coverage
DEL-PROJ-005	Implementation	Requirements Traceability Matrix (RTM)	30 Days after Contract Effective Date	Annually or Upon Request	Vendor must manage, maintain (RTM maintenance), and demonstrate requirements traceability throughout the life of the contract, including providing product demonstrations and post-configuration reviews to support project implementation, operations, and audits.
DEL-PROJ-006	Implementation	Weekly Status Meetings & Status Deck	First meeting within 7 days of kickoff	Weekly throughout project	Vendor must conduct a weekly status meeting to discuss project tasks and activities (e.g., deliverables, milestones, issues, risks, and service level agreements), utilizing the Department-provided status deck template.
DEL-ARC-001	Development	System Design Document (SDD)	30 Days Prior to Implementation	Annually or Upon Change	Enterprise Architecture Documentation will contain data and information regarding the total solution to include each subsystem. The Enterprise Architecture includes data and information related to the: Application Architecture, Data Architecture, Infrastructure Architecture, Security Architecture, Performance Architecture and Business Architecture as defined within the Federal Enterprise Architecture Framework.
DEL-PROJ-002	Project Lifecycle	Implementation Plan	30 Days after Project Kick-off	When Changed	The Implementation Plan shall define the tasks necessary to implement the solution in accordance with the requirements of this Contract. The plan shall include the following: i. The identification and execution of any software customization and/or configuration. ii. A high level project schedule mapping the proposed timeline of events and submission of deliverables. iii. The format and delivery method of requirements and deliverables. iv. A list of all assumptions, constraints, risks/issues, and risk/issue mitigation strategies with target resolution dates. v. Key activities scheduled for the period of thirty (30) Calendar Days post-implementation. vi. All other milestones and deliverables along with the methodology and sequencing that will be needed for a successful implementation.
DEL-PROJ-003	Project Lifecycle	Implementation Schedule	30 Days after Project Kick-off	When Changed	The Implementation Schedule shall define the activities (e.g., deliverables with review / approval schedule, implementation activities), sequenced (i.e., including dependencies) with durations,

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					integrated into a schedule that outlines tasks, timelines, and responsibilities required to successfully execute a project and achieve its objectives. The schedule must be developed using industry standards (e.g., reflects predecessors, successors, State holidays as non-working days, etc.).
DEL-SEC-001	Pre-Award	Vendor Readiness Assessment Report (VRAR)	Included in Proposal to this RFP.	Once	VRAR Template may be downloaded by clicking the following link: https://it.nc.gov/documents/vendor-readiness-assessment-report
DEL-SEC-002	Pre-Award	Privacy Threshold Analysis (PTA)	Included in Proposal to this RFP.	Once	The Vendor is responsible for completing this assessment which helps NCDHHS identify and mitigate privacy risks associated with its programs and systems by evaluating the type and extent of PII being handled and deciding if a more detailed privacy analysis is needed to ensure compliance with state and federal privacy laws and policies. https://ncconnect.sharepoint.com/sites/ESRMO-PTA/SitePages/Home.aspx
DEL-SEC-003	Pre-Award	Third Party Security Assessment Report	Included in Proposal to this RFP.	Annually	FedRAMP, SOC 2 Type 2, ISO 27001, or HITRUST or equivalent. SaaS vendors cannot use IaaS/PaaS certification unless the application is explicitly covered as part of the IaaS/PaaS assessments. Report should be dated within the last year from the date of the proposal submission.
DEL-SEC-004	Project Lifecycle	Privacy and Security Incident Management Plan	60 Days after contract effective date	Annually	The Vendor will provide a Privacy and Security Incident Management Plan annually with established processes that minimally: • Detect and identify events • Triage and analyze events to determine whether an incident is underway • Respond and recover from an incident • Improve the organization's capabilities for responding to a future incident.
DEL-SEC-005	Implementation	User Access Control Report	30 Days Prior to Implementation Phase	Annually during O&M or Upon Change	The Vendor will provide a User Access Control Report annually on a date identified by the State that will minimally include: • The list of users who have access and what level of access to the system. • Ensure that only legitimate users have access to the system.
DEL-SEC-006	Implementation	Privileged User Access Control Report	30 Days Prior to Implementation Phase	Quarterly	The Vendor will provide Privileged User Access Control Reports quarterly that minimally provides: • Privileged access that must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					basis. • A document outlining separation of duties kept as a reference for who should have what access and to ensure no conflict of access or roles.
DEL-SEC-007	Implementation	Vulnerability Management Report	30 Days Prior to Implementation Phase	Monthly	• Report of all servers and systems patched proactively/timely to mitigate the vulnerabilities. • Report of the application components security scanning reports for identifying OWASP TOP 10 vulnerabilities.
DEL-SEC-008	Pre-Award	Disaster Recovery / Business Continuity Test Report	Included in Proposal to this RFP.	Annually	The Vendor shall conduct an annual test of the Disaster Recovery and Business Continuity Plan and submit the Disaster Recover/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Department.
DEL-SEC-009	Pre-Award	Service Organization Control (SOC) 2 Type II Report (or any equivalent 3rd party attestation report)	Included in Proposal to this RFP.	Annually	The Vendor will provide a completed Security Audit Report with results provided to the Department by the 30th of September each year. The Security Audit Report must include either an electronic data processing (EDP) systems audit using SSAE - 18 at a minimum level service organization control (SOC) 2 Type II, ISO 27001, HiTRUST, FedRAMP or any equivalent 3rd party attestation report.
DEL-OPS-001	Operations	Turnover Plan (Initial & Updated)	Initial: 12 months before final contract year; Updated: 6 months before final contract year	During O&M	Vendor must develop and maintain a comprehensive Turnover Plan, including initial submission at least twelve (12) months before the start of the final contract year and an updated version six (6) months prior. .
DEL-SEC-014	Operations	Annual Disaster Recovery Test & AAR	Year 2	Annually	Vendor must perform DR testing each year and submit an After Action Report.
DEL-SEC-016	Operations	Annual Independent Third-Party Penetration Test Report	Year 2	Annually	Vendor must conduct annual independent penetration testing and submit results.
DEL-SEC-017	Operations	Annual SOC 2 Type 2 Report	Year 2	Annually	Vendor must provide an annual SOC 2 Type 2 report by an accredited auditor.
DEL-SEC-018	Operations	Corrective Action Plans & Remediation	Year 2	Annually	Vendor must provide CAPs for any deficiencies found in audits or assessments.

Milestones and Capabilities

The vendor must provide a detailed approach for implementing the Contract Lifecycle Management System solution, as well as a high-level timeline and list of key milestones required during the DDI phase of the project. Following the award of the contract, the State will collaborate with the Vendor to finalize the timeline and key milestones.

ATTACHMENT O: BUSINESS CONTINUITY PLAN

Vendor shall provide, in Vendor's response to this RFP, a narrative describing Vendor's approach to business continuity, including the types of information in Vendor's business continuity plan. The narrative should not exceed three (3) pages. A full business continuity plan must be submitted to the Department in accordance with the Implementation Plan.

When due, the Vendor's proposed business continuity plan must address the following:

1. Introduction – Who the plan is intended for and its purpose.
2. Plan Objectives:
 - a. The essential aspects of the business process supported by the system;
 - b. The way to continue business should the system fail;
 - c. The business recovery procedures for return to operations status; and
 - d. A way to convert back to business as usual after the system is available.
3. System Overview – How the application/system operates and its function.
4. Communication Plan Notification – When the application is unavailable, who is notified and how?
5. Roles, Responsibilities, and Authority – List areas of support and roles of staff involved in this process.
 - a. Example 1:
 - i. Application Support:
 - ii. An Application Analyst is responsible for the following:
 - b. Example 2:
 - i. Hardware Support:
 - ii. A Systems Engineer is responsible for the following:
 - c. Example 3:
 - i. Database Support:
 - ii. A DBA is responsible for the following:
 - d. Example 4:
 - i. Business Recovery Services Vendor for Distributed Platforms
 - ii. Describe services of Business Recovery Services Vendor, if applicable.
6. Plan Initiation
7. Criteria for Restoration of the Business Process due to a Business Disruption – List criteria for invoking the business recovery procedures described in this contingency plan.
8. Business Recovery Procedures – Application Support
 - a. Staffing – Identify staff that needs to be involved in the recovery process;
 - b. Equipment and Components – List equipment and components in their entirety including quantities and attributes. This section shall include all necessary equipment particular to this application;
 - c. Procedures – Includes plans for acquiring, replacing, and alternate siting and any equipment needed;
 - d. Software and Data Backup Procedures – List all software with location and description of how it is backed up;

- e. Software and Data Recovery Procedures – Describe how the software listed above will be restored;
 - f. Succession Plan – List Application Support Order of Succession including Name, Title, and Phone Number with Area Code; and
 - g. Vendor List – List Suppliers including Name, Product/Service/Commodities, and Phone number with Area Code.
9. Business Recovery Procedures – Hardware Support
- a. Staffing – Identify staff that needs to be involved in the recovery process;
 - b. Equipment Types – List Equipment and type;
 - c. Client Equipment – Document any specialty equipment for the client, if any. Workstation equipment requirements, if applicable, to this section should be included here. If workstation equipment is not applicable to this section, it must be included in a different section of the Vendor's Plan;
 - d. Application Equipment – Document any application equipment;
 - e. Equipment Recovery Procedures – Describe how equipment is recovered;
 - f. Software and Data Backup Procedures – List steps taken to begin the backup process then document and describe the procedures;
 - g. Software and Data Recovery Procedures – List steps taken to begin the business recover process then document and describe the procedures;
 - h. Succession Plan – List Hardware Support Order of Succession including Name, Title, and Phone Number with Area Code; and
 - i. Vendor List – List Hardware Service Suppliers including Name, Title, and Phone Number with Area Code.

ATTACHMENT P: DISASTER RECOVERY PLAN

Vendor shall provide, in Vendor's response to this RFP, a narrative describing Vendor's approach to disaster recovery, including the types of information in Vendor's Disaster Recovery Plan. The narrative should not exceed three (3) pages. A full Disaster Recovery Plan must be submitted to the Department in accordance with the Implementation Plan.

When due, the Vendor's Disaster Recovery Plan must, at a minimum, include the following information:

Vendor's proposed Disaster Recovery Plan must fully describe the roles, responsibilities, tasks, timings and dependencies that will be crucial to a successful failover. In addition to a narrative description of the people, processes and tools needed, Vendor's proposed Disaster Recovery Plan must include business process modeling notation (BPMN) diagrams to visually depict the processes. The Disaster Recovery Plan must further define the priorities and sequencing for bringing services and integrations online.

1. Application System Summary
 - a. Technical Support Information
 - b. Operating System;
 - c. Programming Language(s); and
 - d. Internet Accessible – Yes or No
2. Hosting Information
 - a. Vendor Name;
 - b. Vendor Support Phone Number and Website;
 - c. Vendor Account and/or Technical Contact Name and Phone Number;
 - d. Server(s) Name;
 - e. Server Type;
 - f. Server OS;
 - g. Server Location;
 - h. IP Address;
3. Technical Support Information
 - a. Server OS;
 - b. Server Location; and
 - c. IP Address.
4. Failover Site Information
 - a. Server(s) Name;
 - b. Server Type;
 - c. Server OS;
 - d. Server Location;
 - e. IP Address;
 - f. Warm/Hot Site;
 - g. Server(s) Name;
 - h. Server Type;
 - i. Server OS;

- j. Server Location;
 - k. IP Address;
 - l. Vendor Access Method; and
 - m. VPN Info
5. Other Information
 - a. External File Requirements;
 - b. Seats/Units;
 - c. License Requirements;
 - d. Protocol Requirement;
 - e. Port Requirements;
 - f. Third Party Requirements;
 - g. Code Libraries;
 - h. Known Bottlenecks;
 - i. Batch Processing; and
 - j. Supports Life Safety – Yes, No, or Unknown
 6. System Notes
 - a. Interface Engine;
 - b. Inbound Interfaces;
 - c. Outbound Interfaces; and
 - d. Other Comments
 7. Maintenance and Recovery Procedures
 - a. Maintenance; and
 - b. Backup Method/Schedule.
 8. Support Personnel
 - a. Name (Last/First);
 - b. Identify the following:
 - c. System Administrator or Application Administrator;
 - d. Site;
 - e. System;
 - f. Office Phone;
 - g. Pager Number;
 - h. Home Phone;
 - i. Cell Phone; and
 - j. Name (Last/First)
 9. Procedures – The Vendor must describe their procedures. The description shall, at a minimum, address the following in chronological order:
 - a. Recovery Procedures
 - i. Assumptions;
 - ii. System Architecture- Insert a drawing/process flowchart depicting the application architecture
 - iii. Software;
 - iv. Hardware – Insert hardware drawing with purpose of each item.
 - v. Backup Schedules
 - b. Additional Procedures – The Vendor must provide Time and Description for the following:
 - i. Server Recovery Procedures – Server restoration priorities;
 - ii. Application Recover and Validation Procedures;

- iii. Final Data Integrity Validation Procedures;
- iv. Security Procedures;
- v. Customer Recovery Procedures; and
- vi. System Restoration Checklist –Check all applicable tasks covered by the DR Plan

Restore Task	Checkbox
Restore Servers	
• Hardware	
• Application Modules	
• Databases	
Restore Desktops (If Needed)	
Restore Integrations/Exchanges/Interfaces	
Restore Peripheral Devices	
Validation Steps	
• Add a test Minor Enhancement effort	

ATTACHMENT Q: STATE CERTIFICATIONS

Vendor Certifications Required by North Carolina Law

Instructions: **The person who signs this document should read the text of the statutes and Executive Order listed below and consult with counsel and other knowledgeable persons before signing. The text of each North Carolina General Statutes and of the Executive Order can be found online at:**

Article 2 of Chapter 64:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/ByArticle/Chapter_64/Article_2.pdf

- a. G.S. 133-32:
<http://www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=133-32>
- b. Executive Order No. 24 (Perdue, Gov., Oct. 1, 2009):
<https://ethics.nc.gov/media/242/download?attachment>
- c. G.S. 105-164.8(b):
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_105/GS_105-164.8.pdf
- d. G.S. 143-48.5:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-48.5.html
- e. G.S. 143-59.1:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.1.pdf
- f. G.S. 143-59.2:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.2.pdf
- g. G.S. 143-133.3:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-133.3.html
- h. G.S. 143B-139.6C:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143B/GS_143B-139.6C.pdf

Certifications

- (1) **Pursuant to G.S. 133-32 and Executive Order No. 24 (Perdue, Gov., Oct. 1, 2009)**, the undersigned hereby certifies that the Vendor named below is in compliance with, and has not violated, the provisions of either said statute or Executive Order.
- (2) **Pursuant to G.S. 143-48.5 and G.S. 143-133.3**, the undersigned hereby certifies that the Vendor named below, and the Vendor's subcontractors, complies with the requirements of Article 2 of Chapter 64 of the NC General Statutes, including the requirement for each employer with more than 25 employees in North Carolina to verify the work authorization of its employees through the federal E-Verify system." E-Verify System Link: www.uscis.gov.
- (3) **Pursuant to G.S. 143-59.1(b)**, the undersigned hereby certifies that the Vendor named below is not an "*ineligible Vendor*" as set forth in G.S. 143-59.1(a) because:
 - (a) Neither the Vendor nor any of its affiliates has refused to collect the use tax levied under Article 5 of Chapter 105 of the General Statutes on its sales delivered to North Carolina when the sales met one or more of the conditions of G.S. 105-164.8(b); **and**
 - (b) **[CHECK ONE OF THE FOLLOWING BOXES]**

- ☐ Neither the Vendor nor any of its affiliates has incorporated or reincorporated in a "tax haven country" as set forth in G.S. 143-59.1(c)(2) after December 31, 2001; or
- ☐ The Vendor or one of its affiliates has incorporated or reincorporated in a "tax haven country" as set forth in G.S. 143-59.1(c)(2) after December 31, 2001 but the United States is not the principal market for the public trading of the stock of the corporation incorporated in the tax haven country.

- (4) **Pursuant to G.S. 143-59.2(b)**, the undersigned hereby certifies that none of the Vendor's officers, directors, or owners (if the Vendor is an unincorporated business entity) has been convicted of any violation of Chapter 78A of the General Statutes or the Securities Act of 1933 or the Securities Exchange Act of 1934 within 10 years immediately prior to the date of the bid solicitation.
- (5) **Pursuant to G.S. 143B-139.6C**, the undersigned hereby certifies that the Vendor will not use a former employee, as defined by G.S. 143B-139.6C(d)(2), of the North Carolina Department of Health and Human Services in the administration of a contract with the Department in violation of G.S. 143B-139.6C and that a violation of that statute shall void the Agreement.
- (6) The undersigned hereby certifies further that:
- (a) He or she is a duly authorized representative of the Vendor named below;
- (b) He or she is authorized to make, and does hereby make, the foregoing certifications on behalf of the Vendor; and
- (c) He or she understands that any person who knowingly submits a false certification in response to the requirements of G.S. 143-59.1 and -59.2 shall be guilty of a Class I felony.

Vendor's Name: _____

Vendor's
Authorized Agent: Signature _____ Date _____

Printed Name _____ Title _____

Witness: Signature _____ Date _____

Printed Name _____ Title _____

The witness should be present when the Vendor's Authorized Agent signs this certification and should sign and date this document immediately thereafter.

ATTACHMENT R: Federal Certifications and Disclosures

The undersigned states that:

- 1. He or she is the duly authorized representative of the Contractor named below;
- 2. He or she is authorized to make, and does hereby make, the following certifications on behalf of the Contractor, as set out herein:
 - a. The Certification Regarding Nondiscrimination;
 - b. The Certification Regarding Drug-Free Workplace Requirements;
 - c. The Certification Regarding Environmental Tobacco Smoke;
 - d. The Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier Covered Transactions; and
 - e. The Certification Regarding Lobbying;
- 3. He or she has completed the Certification Regarding Drug-Free Workplace Requirements by providing the addresses at which the contract work will be performed;
- 4. [Check the applicable statement]

☐ He or she **has completed** the attached **Disclosure Of Lobbying Activities** because the Contractor **has made, or has an agreement to make**, a payment to a lobbying entity for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action;

OR

☐ He or she **has not completed** the attached **Disclosure Of Lobbying Activities** because the Contractor **has not made, and has no agreement to make**, any payment to any lobbying entity for influencing or attempting to influence any officer or employee of any agency, any Member of Congress, any officer or employee of Congress, or any employee of a Member of Congress in connection with a covered Federal action.

- 5. The Contractor shall require its subcontractors to whom such certifications and disclosures apply, if any, to make the same certifications and disclosure.

Signature	Click or tap here to enter text. Title
Click or tap here to enter text. Contractor Name	Date

[This Certification Must be Signed by the Same Individual Who Signed the Proposal Execution Page]

I. Certification Regarding Nondiscrimination

The Grantee certifies that it will comply with all applicable federal statutes, executive orders, and regulations, including but not limited to: Title VI of the Civil Rights Act of 1964; Title IX of the Education Amendments of 1972; Section 504 of the Rehabilitation Act of 1973; the Age Discrimination Act of 1975; the Drug Abuse Office and Treatment Act of 1972; the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970; Title VIII of the Civil Rights Act of 1968; the Food Stamp Act and USDA policy; and any other applicable nondiscrimination statutes.

II. Certification Regarding Drug-Free Workplace Requirements

1. The Contractor certifies that it will provide a drug-free workplace by:
 - a. Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violation of such prohibition;
 - b. Establishing a drug-free awareness program to inform employees about:
 - i. The dangers of drug abuse in the workplace;
 - ii. The Contractor's policy of maintaining a drug-free workplace;
 - iii. Any available drug counseling, rehabilitation, and employee assistance programs; and
 - iv. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;
 - c. Making it a requirement that each employee be engaged in the performance of the agreement be given a copy of the statement required by paragraph (a);
 - d. Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the agreement, the employee will:
 - i. Abide by the terms of the statement; and
 - ii. Notify the employer of any criminal drug statute conviction for a violation occurring in the workplace no later than five days after such conviction;
 - e. Notifying the Department within ten days after receiving notice under subparagraph (d)(ii) from an employee or otherwise receiving actual notice of such conviction;
 - f. Taking one of the following actions, within 30 days of receiving notice under subparagraph (d)(ii), with respect to any employee who is so convicted:
 - i. Taking appropriate personnel action against such an employee, up to and including termination; or
 - ii. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency; and
 - g. Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e), and (f).

2. The sites for the performance of work done in connection with the specific agreement are listed below (list all sites; add additional pages if necessary):

Address:

Street: Click or tap here to enter text.
City, State, Zip Click or tap here to enter text.
Code:

Address:

Street: Click or tap here to enter text.
City, State, Zip: Click or tap here to enter text.
Code:

3. Contractor will inform the Department of any additional sites for performance of work under this agreement.
4. False certification or violation of the certification may be grounds for suspension of payment, suspension or termination of grants, or government-wide Federal suspension or debarment. 45 C.F.R. 82.510.

III. Certification Regarding Environmental Tobacco Smoke

Public Law 103-227, Part C-Environmental Tobacco Smoke, also known as the Pro-Children Act of 1994 (Act), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by Federal grant, contract, loan, or loan guarantee. The law does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, and portions of facilities used for inpatient drug or alcohol treatment. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1,000.00 per day and/or the imposition of an administrative compliance order on the responsible entity.

The Contractor certifies that it will comply with the requirements of the Act. The Contractor further agrees that it will require the language of this certification be included in any subawards that contain provisions for children's services and that all subgrantees shall certify accordingly.

IV. Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion Lower Tier

Covered Transactions Instructions

[The phrase "prospective lower tier participant" means the Contractor.]

1. By signing and submitting this document, the prospective lower tier participant is providing the certification set out below.
2. The certification in this clause is a material representation of the fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originate may pursue available remedies, including suspension and/or debarment.
3. The prospective lower tier participant will provide immediate written notice to the person to whom this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
4. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549, 22 CFR 513.100. You may contact the person to whom this proposal is submitted for assistance in obtaining a copy of those regulations.
5. The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter any lower tier covered transaction with a person who is debarred,

suspended, determined ineligible or voluntarily excluded from participation in this covered transaction unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this document that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not debarred, suspended, ineligible, or voluntarily excluded from covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the Nonprocurement List.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized in paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension, and/or debarment.

Certification

1. **The prospective lower tier participant certifies**, by submission of this document, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

V. Certification Regarding Lobbying

The Contractor certifies, to the best of his or her knowledge and belief, that:

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

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

3. The undersigned shall require that the language of this certification be included in the award document for subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) who receive federal funds of \$100,000.00 or more and that all subrecipients shall certify and disclose accordingly.

4. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000.00 and not more than \$100,000.00 for each such failure.

VI. Disclosure Of Lobbying Activities

Instructions

This disclosure form shall be completed by the reporting entity, whether subawardee or prime Federal recipient, at the

initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Use the SF-LLL-A Continuation Sheet for additional information if the space on the form is inadequate. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying activity is and/or has been secured to influence the outcome of a covered Federal action.
2. Identify the status of the covered Federal action.
3. Identify the appropriate classification of this report. If this is a follow-up report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.
4. Enter the full name, address, city, state and zip code of the reporting entity. Include Congressional District, if known. Check the appropriate classification of the reporting entity that designates if it is, or expects to be, a prime or sub-award recipient. Identify the tier of the subawardee, e.g., the first subawardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grants.
5. If the organization filing the report in Item 4 checks "Subawardee", then enter the full name, address, city, state and zip code of the prime Federal recipient. Include Congressional District, if known.
6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizational level below agency name, if known. For example, Department of Transportation, United States Coast Guard.
7. Enter the Federal program name or description for the covered Federal action (Item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans, and loan commitments.
8. Enter the most appropriate Federal Identifying number available for the Federal action identified in Item 1 (e.g., Request for Proposal (RFP) number, Invitation for Bid (IFB) number, grant announcement number, the contract grant, or loan award number, the application/proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP- DE-90-001."
9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the prime entity identified in Item 4 or 5.
10. (a) Enter the full name, address, city, state and zip code of the lobbying entity engaged by the reporting entity identified in Item 4 to influence the covered Federal action.

(b) Enter the full names of the individual(s) performing services, and include full address if different from 10(a). Enter Last Name, First Name and Middle Initial (MI).

11. Enter the amount of compensation paid or reasonably expected to be paid by the reporting entity (Item 4) to the lobbying entity (Item 10). Indicate whether the payment has been made (actual) or will be made (planned). Check all boxes that apply. If this is a material change report, enter the cumulative amount of payment made or planned to be made.

12. Check the appropriate boxes. Check all boxes that apply. If payment is made through an in-kind contribution, specify the nature and value of the in-kind payment.

13. Check the appropriate boxes. Check all boxes that apply. If other, specify nature.

14. Provide a specific and detailed description of the services that the lobbyist has performed, or will be expected to perform, and the date(s) of any services rendered. Include all preparatory and related activity, not just time spent in actual contact with Federal officials. Identify the Federal official(s) or employee(s) contacted or the officer(s), employee(s), or Member(s) of Congress that were contacted.

15. Check whether or not a SF-LLL-A Continuation Sheet(s) is attached.

16. The certifying official shall sign and date the form, print his/her name, title, and telephone number.

Public reporting burden for this collection of information is estimated to average 30 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0046), Washington, D. C. 20503

Disclosure of Lobbying Activities

(Approved by OMB 0344-0046)

Complete this form to disclose lobbying activities pursuant to 31 U.S.C. 1352

1. Type of Federal Action ☐ a. contract ☐ b. grant ☐ c. cooperative agreement ☐ d. loan ☐ e. loan guarantee ☐ f. loan insurance		2. Status of Federal Action ☐ a. Bid/offer/application ☐ b. Initial Award ☐ c. Post-Award		3. Report Type ☐ a. initial filing ☐ b. material change For Material Change Only: Year: Enter Quarter: Enter Year Qtr Date of Last Enter a date. Report:									
4. Name and Address of Reporting Entity: ☐ Prime ☐ Subawardee Tier (if known): Enter Text Congressional District (if known): Enter Text		5. If Reporting Entity in No. 4 is Subawardee, Enter Name and Address of Prime: <table border="1"><tr><td>Name:</td><td>Click or tap here to enter text.</td></tr><tr><td>Street Address:</td><td>Click or tap here to enter text.</td></tr><tr><td>City, State, Zip:</td><td>Click or tap here to enter text.</td></tr><tr><td>Congressional District (if known):</td><td>Click or tap here to enter text.</td></tr></table>				Name:	Click or tap here to enter text.	Street Address:	Click or tap here to enter text.	City, State, Zip:	Click or tap here to enter text.	Congressional District (if known):	Click or tap here to enter text.
Name:	Click or tap here to enter text.												
Street Address:	Click or tap here to enter text.												
City, State, Zip:	Click or tap here to enter text.												
Congressional District (if known):	Click or tap here to enter text.												
6. Federal Department/Agency: Click or tap here to enter text.		7. Federal Program Name/Description: Click or tap here to enter text.											
		CFDA Number (if applicable):		Click here to enter text.									

8. Federal Action Number (if known):		Click or tap here to enter text.		9. Award Amount (if known)		\$ Click here to enter text.	
10. a. Name and Address of Lobbying Entity (if individual, last name, first name, MI) Click or tap here to enter text.				b. Individuals Performing Services (last name, first name, MI): (including address if different from No.10a.) Click or tap here to enter text.			
(attach Continuation Sheet(s) SF-LLL-A, if necessary)							
11. Amount of Payment (check all that apply):		\$ Click or tap here to enter text.		13. Type of Payment (check all that apply):			
		☐	Actual	☐	Planned		
12. Form of Payment (check all that apply):		☐	a. cash	☐	b. In-kind (specify below):		
		Nature:		Click to enter text.			
		Value:		\$ Click to enter text.			
						☐ a. retainer ☐ b. one-time fee ☐ c. commission ☐ d. contingent fee ☐ e. deferred ☐ f. other; specify: Click or tap here to enter text.	
14. Brief Description of Services Performed or to be Performed and Date(s) of Services, including officer(s), employee(s), or Member(s) contacted, for Payment Indicated in Item 11(attach Continuation Sheet(s) SF-LLL-A, if necessary): Click or tap here to enter text.							
15. Continuation Sheet(s) SF-LLL-A attached:				☐ Yes		☐ No	
16. Information requested through this form is authorized by title 31 U. S. C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U. S. C. 1352. This information will be reported to the Congress semi-annually and will be available for public inspection. Any person who fails to file the required disclosure shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.				Signature:			
				Print Name:		Click or tap here to enter text.	
				Title:		Click or tap here to enter text.	
				Telephone No.		Enter text.	Date:
Federal Use Only						Authorized for Local Reproduction Standard Form - LLL	

ATTACHMENT S: BUSINESS ASSOCIATE AGREEMENT

NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES, DIVISION OF HEALTH BENEFITS BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is made between North Carolina Department of Health and Human Services, Division of Health Benefits ("DHB" and "Covered Entity") and _____ ("Business Associate") (collectively the "Parties").

1. BACKGROUND

- a. Covered Entity and Business Associate are parties to an agreement entitled Contract# 30-2025-037-DHB -- Contract Lifecycle Management System, whereby Business Associate agrees to perform certain services for or on behalf of Covered Entity.
- b. Covered Entity is an organizational unit of the North Carolina Department of Health and Human Services (the "Department") that has been designated in whole or in part by the Department as a health care component for purposes of the HIPAA Privacy Rule.
- c. The relationship between Covered Entity and Business Associate is such that the Parties believe Business Associate is or may be a "business associate" within the meaning of the HIPAA Privacy Rule.
- d. The Parties enter into this Business Associate Agreement as an attachment to the Contract with the intention of complying with the HIPAA Privacy Rule provision that a covered entity may disclose Protected Health Information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

2. DEFINITIONS

Unless some other meaning is clearly indicated by the context, the following terms shall have the following meaning in this Agreement:

- a. "Electronic protected health information" or "ePHI" shall have the same meaning as the term "Electronic protected health information" in 45 C.F.R. § 160.103.
- b. "HIPAA" means the Administrative Simplification Provisions, Sections 261 through 264, of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as modified and amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.
- c. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a Person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- d. "Person" shall have the same meaning as the term "person" in 45 C.F.R. § 160.103 and shall include a human being that is born alive, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.
- e. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Part 160 and Part 164.
- f. "Protected Health Information" or "PHI" shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. § 160.103, limited to the information compiled, created, or received by Business Associate from or on behalf of Covered Entity.
- g. "Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

- h. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or the Person to whom the authority involved has been delegated.
- i. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subpart C.
- j. Unless otherwise defined in this Agreement, terms used herein shall have the same meaning as those terms have in the Privacy Rule.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

- a. Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required By Law.
- b. Business Associate agrees to use appropriate safeguards and comply, where applicable, with subpart C of 45 C.F.R. Part 164 with respect to ePHI, to prevent use or disclosure of the ePHI other than as provided for by this Agreement.
- c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- d. Business Associate agrees to comply with all applicable requirements of the Security Rule (45 C.F.R. Part 164, Subparts A and C) with respect to electronic protected health information.
- e. Business Associate shall implement physical, administrative and technical safeguards that reasonably protect the confidentiality, integrity and availability of any ePHI that it creates, receives, maintains or transmits on behalf of the NCDHHS.
- f. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement of which it becomes aware, including breaches of unsecured PHI as required by 45 C.F.R. § 164.410.
- g. Business Associate agrees, in accordance with 45 C.F.R. § 164.502(e)(1) and § 164.308(b)(2), to ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.
- h. Business Associate agrees to make available PHI as necessary to satisfy Covered Entity's obligations in accordance with 45 C.F.R. § 164.524.
- i. Business Associate agrees to make available PHI for amendment and incorporate any amendment(s) to PHI in accordance with 45 C.F.R. § 164.526.
- j. Unless otherwise prohibited by law, Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from or created or received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.
- k. Business Associate agrees to make available the information required to provide an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

4. PERMITTED USES AND DISCLOSURES

- a. Except as otherwise limited in this Agreement or by other applicable law or agreement, if the Contract permits, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract, provided that such use or disclosure:

- 1) Would not violate the Privacy Rule if done by Covered Entity; or
- 2) Would not violate the minimum necessary policies and procedures of the Covered Entity.
- b. Except as otherwise limited in this Agreement or by other applicable law or agreements, if the Contract permits, Business Associate may disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that:
 - 1) The disclosures are Required By Law; and
 - 2) Business Associate obtains reasonable assurances from the Person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the Person, and the Person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- c. Except as otherwise limited in this Agreement or by other applicable law or agreements, if the Contract permits, Business Associate may use PHI to provide data aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B).
- d. Notwithstanding the foregoing provisions, Business Associate shall not use or disclose PHI if the use or disclosure would violate any term of the Contract or other applicable law or agreements.

5. TERM AND TERMINATION

- a. **Term.** This Agreement shall be effective as of the effective date of the Contract and shall terminate when the Contract terminates.
- b. **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, at its option:
 - 1) Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement and services provided by Business Associate, to the extent permissible by law, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
 - 2) Immediately terminate this Agreement and services provided by Business Associate, to the extent permissible by law; or
 - 3) If neither termination nor cure is feasible, report the violation to the Secretary as provided in the Privacy Rule.
- c. **Effect of Termination.**
 - 1) Except as provided in paragraph (2) of this section or in the Contract or by other applicable law or agreements, upon termination of this Agreement and services provided by Business Associate, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.
 - 2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide Covered Entity notification of the conditions that make return or destruction not feasible. Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

6. GENERAL TERMS AND CONDITIONS

- a. This Agreement amends and is part of the Contract.
- b. Except as provided in this Agreement, all terms and conditions of the Contract shall remain in force and shall apply to this Agreement as if set forth fully herein.

- c. In the event of a conflict in terms between this Agreement and the Contract, the interpretation that is in accordance with the Privacy Rule shall prevail. In the event that a conflict then remains, the Contract terms shall prevail so long as they are in accordance with the Privacy Rule.
- d. A breach of this Agreement by Business Associate shall be considered sufficient basis for Covered Entity to terminate the Contract for cause.

IN WITNESS WHEREOF, Business Associate agrees to and executes this Agreement as of the Effective Date of the Contract.

BUSINESS ASSOCIATE

Name:
Title:

Date

NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES, DIVISION OF HEALTH BENEFITS

Melanie Bush
Deputy Secretary
NC Medicaid

Date

ATTACHMENT T: TECHNICAL / MANAGEMENT PROPOSAL

The Technical / Management Proposal is comprised of responses to selected sections of the RFP and Specifications listed in the following tables. Provide the section responses in the order found in the tables with the instructions provided before each table. Label each RFP section within the body of the technical / management proposal.

By signing the Execution Page of this RFP, the Vendor agrees to meet all Requirements in the tables provided in *Section 3.5.1 and the Requirements and Tables OR1 and OR2 in section 3.7.1*. If any of these Requirements cannot be met, the State will disqualify the Vendor from further evaluation.

Vendor to provide a detailed narrative, diagrams, process flows, exhibits, examples, sketches, relevant descriptive literature, or other information to demonstrate how the Vendor's solution(s) will address each section area listed in the table below. Please be as detailed as possible while keeping within the page limitation listed for each section.

RFP Section	Area	Page Limitation
Section 3.1.1	Objectives of a CLMS	15
Section 3.1.2	Solution Architecture – Contract Development, Repository, And Monitoring	15
Section 3.1.3	Key Functional Requirements of a CLMS	15
Section 3.1.5	Implementation and Support	10
Section 3.2.3	General Requirements and Specifications: Site and System Preparation	5
Section 3.2.4	General Requirements and Specifications: Equivalent Items	2
Section 3.2.5	General Requirements and Specifications: Enterprise Licensing	2
Section 3.4.2	Enterprise Specifications: Architecture Diagrams Defined	10
Section 7.1	Vendor Utilization of Workers Outside the U.S.	2
Section 7.4	Vendor's License or Support Agreements	10
Section 7.6	Disclosure of Litigation	2

Vendor to provide a response for all Specifications in the tables provided in Section 3.6.1 and Table 26-27 in Section 3.7.1. Each Specification must have a response provided in a format with a header to include two columns: a) the Specification number as provided in the RFP, and b) the Specification Description as provided in the RFP, and then an area following the header that contains the narrative response to the Specification. The narrative can contain diagrams, process flows, exhibits, examples, sketches, relevant descriptive literature, or other information to demonstrate how the Vendor's solution(s) will address each Specification.

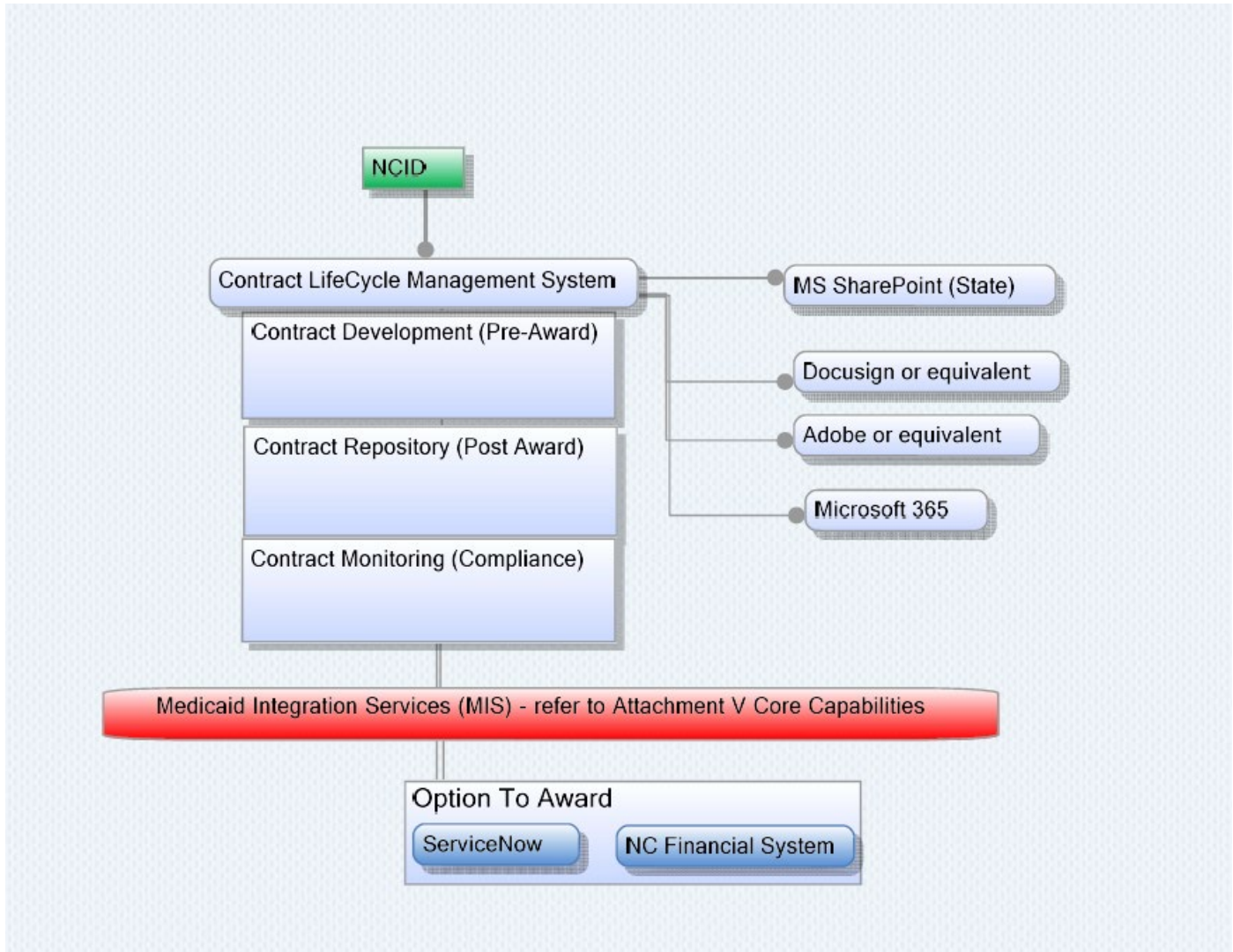
Note: The Specification tables in Section 3.6.1 in this RFP are ranked in descending order of importance.

RFP Section	Area	Page Limitation
Section 3.6.1: Table S1	Functionality CLMS - Development	n/a
Section 3.6.1: Table S2	Functionality CLMS - Repository	n/a
Section 3.6.1: Table S3	Functionality CLMS - Monitoring	n/a
Section 3.6.1: Table S4	Business	n/a
Section 3.6.1: Table S5	Operations	n/a
Section 3.6.1: Table S6	Compliance	n/a
Section 3.6.1: Table S7	Security	n/a
Section 3.6.1: Table S8	Enterprise Architecture	n/a
Section 3.6.1: Table S9	Testing	n/a
Section 3.6.1: Table S10	Quality Assurance	n/a

Section 3.6.1: Table S11	Training	n/a
Section 3.7.1 Table OS1	ServiceNow Integration	n/a
Section 3.7.1 Table OS2	NCFS Integration	n/a

ATTACHMENT U: CONCEPTUAL ARCHITECTURAL DIAGRAMS

The following is the conceptual architectural diagram relating to the future state of the CLMS Solution:



ATTACHMENT V: MEDICAID INTEGRATION SERVICES CORE CAPABILITIES

Introduction

The North Carolina Department of Health and Human Services, Division of Health Benefits (Department) is in the process of implementing Medicaid Integration Services (MIS) that will provide module vendors with a common infrastructure, which may consist of State developed and third-party solutions and tools, to communicate and integrate using a consistent standards-based approach.

The MIS will be configured and set up to run in the cloud and provides core shared services to be leveraged by the different module vendors and systems. The following provides additional details of these core services:

Core MIS Services

1. Application Program Interface (API) Management

The MIS API services provide API Management capability to support lifecycle management, covering the design, deployment and management of APIs that will be the primary means of integration of MIS components and MES vendor modules. API management includes API Gateway and API traffic management capability including rate-limiting to control impact on backend services.

The API Management infrastructure will provide a graphical web portal interface that allows the management of the entire lifecycle of interfaces connecting MES modules via the MIS. The MIS will use the API Management Portal to design, secure, publish, monitor, manage, and deploy interfaces across multiple vendor cloud environments. Using the portal, the MIS team will define integration across module API contracts, fulfill contract implementation, define access control and usage policies, set rates and limits, and deploy the API for testing and later operations.

The MIS platform provides API Management capability to support lifecycle management, covering the design, deployment, and management of APIs that will be the primary means of integration across the MES. API management includes API Gateway and API traffic management capability including rate-limiting to control impact on backend services.

S No.	Type of API	Description	MIS API Gateway	MIS API Management Portal	Module Vendor Interaction
1	Module Vendor Internal Application Specific API	These are APIs that the vendor uses within their module for completing the required functionality	Not Applicable	Recommended to be available to support discoverability	Publish their APIs in the Open API specification format
2	Module Vendor External Facing APIs	These are the APIs that vendor exposes for other entities to interact and integrate with the module	API is managed through the gateway for governance, security, and	Yes. – Other module vendors can use this to discover and learn about the API	Act as a publisher for an API also known as API provider

S No.	Type of API	Description	MIS API Gateway	MIS API Management Portal	Module Vendor Interaction
			traffic management		Act as a consumer for the other module vendor APIs
3	Third Party APIs	These are external APIs that may be published by federal agencies and other trusted sources and are identified as useful to integrate in the Medicaid business operations	API Gateway provides the end point access. Not all external APIs may be governed through the API Gateway	Yes	Discover and learn about these API on the API Management Portal Register Module Application to have access to these APIs
4	MIS Service APIs	These are APIs that provide access to the MIS core capabilities or are APIs that may be developed to support integration requests between different MES modules	Yes	Yes	Discover and learn about these API on the API Management Portal Register Module Application to have access to these APIs

a. API Standards

The MIS **recommends the use of API first style-based integration approach** for module interactions and integration points. The MIS promotes the following standards and architectural practices.

S No.	Area	Preferred Standard/Style
1	API Architectural Style	REST
2	API Specification	Open API Specification (OAS) 3.0
3	Security	OAuth 2.0 and OIDC where applicable
4	Payload	JSON

The MIS also **supports Simple Object Access Protocol (SOAP)-based web services** and other integration approaches like **message queues**. The MIS platform supports the following standards for these.

S No.	Area	Preferred Standard/Style
1	SOAP	SOAP 1.2
2	Web Services	Web Services Description Language (WSDL) 1.2
3	SAML	Security Assertion Mark Up Language 2.0

The MIS preferred and recommended style is to use Representational State Transfer (REST)-based APIs for integration.

2. Managed File Transfer

The MIS provides support for exchanging data through a managed file transfer mechanism. The Managed File Transfer (MFT) service platform supports modules to reliably exchange electronic data with other modules and systems in a secure way. The MFT services provides full visibility to these data exchanges including ability to see who is transferring files, what is being shared, and the volume passing through the system. The MFT service can proactively identify events like delays and failed transfers before they impact downstream modules or missed Service-Level Agreements (SLAs).

The following table identifies the high level MFT capability and the recommendation for use for the module vendor.

S No.	MFT Capability Access Mode	Recommendation for Module Vendor
1	Use of MIS published standards (upload, download etc.) to support file transfer capabilities	Preferred way to interact with MFT capability and use it for checking status, progress, and errors
2	Use of MFT provided Web Interface	Only for ad-hoc situations
3	Use of MFT provided native interfaces such as SFTP and SCP	Preferred only in case of large data files. Also, will be used where the trading partner (federal agency, other module vendors) requires the use of data files

a. Authentication and Security

All service accounts for the Module Vendors using the MFT capability will be managed and provisioned using the MIS platform's Identity Credential and Access Management (ICAM) service infrastructure.

b. Supported Protocols

The Managed File Transfer service will support the following standards:

- Secure FTP (SFTP (SSH File Transfer Protocol, FTPS, and Secure Copy Protocol (SCP)) for protected file transfer; and
- AS2, AS3 and AS4 messages with support for multiple file attachments.

3. ICAM

Identity Credential and Access Management (ICAM) is an Authentication and Authorization Service.

The ICAM solution will work in conjunction with State of NC's enterprise-IAM platform, i.e., NCID (North Carolina Identity Management Service), in a federated model using the Security Assertion Markup Language (SAML) 2.0 protocol.

The following table identifies the role of each system as it pertains to user identity:

S No.	System	Roles
1	NCID	- Identity Provider (IdP) for users in the system - All users will be registered in the NCID system first
2	Module Vendor	Act as a Service Provider (SP) to NCID

The MES Portal has been developed to provide an MES Landing Page which gives users a single point of entry into the Department's MES Medicaid system and displays the MES module tiles to which a user has access based on the coarse-grained authorization. To facilitate this functionality, modules / applications are required to utilize a State developed API to push coarse-grained authorization to the user's NCID profile.

Fine-grained authorization will be maintained and provided by the modules / applications to give the user the appropriate access within the application.

4. Operation Portal with Centralized Information Technology Service Management (ITSM) Capabilities

The State provides a unified web-based operations portal to allow for performing various operations including request, monitor, configure, control and report on each of the MIS platform services. The operations portal will **provide a module specific view** of all relevant transactions flowing through the MIS platform.

The Solution will follow the State provided ITSM solutions in the following business areas:

- Change Management
- Incident Management
- Problem Management
- Release Management

a. Change Management

All State initiated change(s) or changes that impact Medicaid production operations will be tracked in the State provided change management solution. All module vendors will be required to use this solution to facilitate cross module collaboration, centralized approvals and tracking deployment of changes to the production environment.

b. Incident Management

The module vendors will raise incidents that impact the overall MES Enterprise operations to facilitate cross-module tracking and resolution of incidents. These incidents will be reported in this State provided Incident Management system for review and to manage communication and escalation to the appropriate module vendor partner for resolution.

c. Problem Management

Problems will primarily be managed by the State Central Technical Operations team. The module vendors reporting incidents will be prompted to link new incidents to existing problems if known. The module vendors will support the State Central Technical Operations team in managing the life cycle of the problem.

d. Release Management

The module vendors must follow the State provided and defined Release Management process.

5. Defect Tracking

The module vendors will use their existing defect tracking systems to manage their development and product defects, but the State will require the use of the State provided defect tracking system for module-to-module integration testing and User acceptance testing for modules.

6. Test Management

The Solution must utilize the State provided test management infrastructure and service to support centralized test management across all MES modules, MIS, and the Medicaid partners. This service will allow DHHS to monitor and report on testing progress. The module vendors will be required to provide data to the centralized test management system to support consolidated reporting including generation of key metrics and reporting progress.

ATTACHMENT W: WORK PRODUCTS

Work products are incidental artifacts created during the performance of the contract. The table below lists the Work Products to be provided by the Vendor for this project, along with the anticipated due date and frequency for each Work product. Work Products submitted by the Vendor should follow industry standards, best practices, and the description provided. *NOTE: Work Products are NOT separately priced. The efforts and time required to develop work products must be factored into the overall cost and timeframe of project implementation and operations.*

1.0 WORK PRODUCTS

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-OPS-001	Project Lifecycle	Defect Tracking	10 Days After Contract Award	Throughout DDI and O&M	The Vendor will work with the identified State Departments to track all defects. This is in addition to any defect management functions that the Vendor may typically operate.
WP-OPS-002	Project Lifecycle	Risk and Issue Tracking	10 Days After Contract Award	Throughout DDI and O&M	The Vendor will work with the identified State Departments to track all risks and issues.
WP-OPS-003	Project Lifecycle	SLA Self-Assessment Report - Project Phase	60 Days After Contract Award	Monthly	The Vendor must minimally include the following in SLA self-assessment report: Vendor not meeting SLA, SLA number not being met, Evidence used for determination, Date SLA became out of compliance, Resolution Process (if known), Planned Resolution Date (if known), Criticality Level, Escalation Required (Y/N), Corrective Action
WP-PROJ-001	Project Lifecycle	Project Status Meeting Agenda	10 Days after Project Kick-off	Once	The Project Status Meeting Agenda is designed to provide a listing of discussion topics for the Monthly Status Meeting attended by NC DHHS and Vendor. At a minimum, the Agenda will include the following topics that is also required in the project status report among others: a. Overall project status/health by phases/major functions in progress b. Progress summary information c. Project timeline d. Risks and Issues e. Potential scope changes f. Staffing, changes g. Sub-contractor status h. Project metrics i. Open action items

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-PROJ-002	Project Lifecycle	Project Status Meeting Minutes	2 Days after Project Status Meeting	Once	The Project Status Meeting Minutes will provide a detailed summary of items discussed during the initial contract meeting between NC DHHS personnel and Vendor. The purpose of the Project Status Meeting is to discuss program progress, escalate issues, evaluate performance, review additional program requirements, and discuss other management topics as identified by program management. The Minutes may provide a summary of the following topics among others: a. Date, Meeting location, Meeting start time b. Name of individual chairing the Meeting and meeting attendees c. Report on motion to approve previous Meeting's published Minutes d. Summary of general announcements e. Summary of meeting discussion and action item outcomes, by item f. Announcement of Date, time, and location of next scheduled Meeting g. Time of meeting adjournment
WP-PROJ-003	Project Lifecycle	Project Status Report	30 Days after Project Kick-off	Once	The Project Status Report communicates a concise management view of progress made to the mutually agreed project plan provided at a minimum weekly (or on an agreed upon cadence with DHHS). At a minimum, this report provides the following information: a. Overall project status/health by phases/major functions in progress b. Accomplishments in the current reporting period, planned activities for the next two reporting periods c. Project timeline, earned value metrics with explanation of performance status, variances, corrective action plans, estimated cost to complete remaining work, and estimated cost at completion of work d. Active risks, mitigation plans and activities e. Major project issues that require NC DHHS attention and resolution f. Potential scope changes g. Staffing changes h. Sub-contractor status, if applicable i. Project metrics (i.e., cost and schedule performance, measurement of performance, etc.), trend analysis (i.e., SLAs against targets) j. Action items status The information generated and provided must be timely and reliable.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-PROJ-004	Project Lifecycle	Weekly Status Report	10 Days After Internal Project Kickoff	Weekly	Summarizes project team accomplishments, planned work, actual statuses and trends for key performance indicators against targets.
WP-PROJ-005	Project Lifecycle	Meeting Agendas	48 hours prior to Scheduled Meeting	Each Meeting	Provides a listing of discussion topics for the meeting attended by NC DHHS and Vendor.
WP-PROJ-006	Project Lifecycle	Meeting Minutes	48 hours after Scheduled Meeting	Each Meeting	Provides a detailed summary of items discussed during the meeting between NC DHHS personnel and Vendor.
WP-PROJ-007	Project Lifecycle	Test Cases / Scripts / Results	15 Days Prior to Scheduled Testing	As Needed	Test Cases provide detailed test steps to be performed on a system to validate it operates as expected as well as the expected results. Actual Test Results will match the documented expected results in order to pass. All Test Results will be captured and stored with each test case.
WP-TRAIN-001	Implementation	Training Evaluation Report	48-Hours Post-Training	Each Training	Training Evaluation Report will document and assesses the effectiveness, efficiency, and impact of a training program. It provides insights into what worked, what didn't, and how future training can be improved.
WP-OPS-004	Implementation	User Manuals	90 Days Before Go-Live	When Changed	Procedural or reference information delivered through computer software to present information on a broad range of topics or subjects.
WP-OPS-005	Implementation	Administrative Manual	90 Days Before Go-Live	When Changed	Outlines the administrative and operational procedures for managing a specific software system, focusing on configuration, user access, system maintenance, and security for administrators.
WP-SEC-001	Implementation	Vulnerability Management Reports	30 Days Before Go-Live	Monthly during O&M	Report of all servers and systems patched proactively/timely to mitigate the vulnerabilities. Report of the application components security scanning reports for identifying OWASP TOP 10 vulnerabilities.
WP-PROJ-008	Operations	Operations Acceptance Transmittal	5 Days Prior to Go-Live	When Changed	The Vendor will submit a transmittal to the State indicating all software and systems have been designed and tested, technical documentation has been submitted and approved by the State, and that the Vendor is prepared to assume operations with State approval.
WP-SEC-002	Operations	Plan of Action and Milestones (POA&M)	Upon findings from any security assessments	As Required by Security Policy	The Vendor shall respond to all risks identified through the periodic security risk assessments with a Plan of Action and Milestones (POA&M) containing clarifying information, a proposed mitigation strategy if necessary, a timeline for implementation, and shall work with the Department to successfully execute the POA&M. Please use: https://www.fedramp.gov/resources/templates/FedRAMP-POAM-Template.xlsx

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-SEC-003	Operations	User Access Control Reports	No later than 90 Days after Go-Live	Annually during O&M or Upon Change	The list of users who have access and what level of access to the system. Ensure that only legitimate users have access to the system.
WP-SEC-004	Operations	Privileged User Access Control Reports	No later than 30 Days after Go-Live	Quarterly during O&M or Upon Change	Privileged access must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know basis. A document outlining separation of duties should be kept as a reference for who should have what access and to ensure no conflict of access or roles.
WP-SEC-005	Operations	After Action Report	After Disaster Recovery Testing	Annually during O&M or Upon Change	An After Action Report (AAR), following a disaster recovery (DR) test, is a concise summary that evaluates how well the organization responded to a simulated disaster scenario. It begins with an overview of the test, including its purpose, date, and the type of disaster simulated. The AAR outlines the objectives such as validating recovery time and data integrity and describes the scope, including systems, teams, and locations involved. It then summarizes the execution, detailing the timeline of events, actions taken, and tools used. The results section highlights what went well and what didn't, identifying any technical, procedural, or communication issues. Communication protocols are also assessed, including the use of email, SMS, and incident management tools to coordinate response efforts. While most messages were delivered effectively, some delays were noted due to outdated contact information and unclear escalation paths. The report emphasizes the need for updated contact lists, standardized message templates, and regular communication drills. Lessons learned are documented to capture key insights, and the report concludes with actionable recommendations to improve the disaster recovery plan, such as enhancing training, refining communication workflows, and automating recovery steps. Finally, it outlines next steps, including assigning responsibilities, scheduling future tests, ensuring continuous improvement in the organization's resilience strategy. The Vendor's After-Action Report format is acceptable.
WP-TURN-001	Operations	Turnover Report	30 Days after System Turnover	Monthly	The Report will document that all Vendor turnover activities have been completed on a monthly basis in accordance with the State approved Turnover Plan to include successful transfer of IT inventory, baseline

					system configuration, financial reconciliation, and operations to the State and successor Vendor, as appropriate.
--	--	--	--	--	---

ATTACHMENT X: REQUEST FOR PROPOSED MODIFICATIONS TO THE TERMS AND CONDITIONS

As provided in Section 1.3.3, Offeror may submit proposed modifications to the terms and conditions of the RFP for consideration by the Department. The proposed modifications do not alter the terms and conditions of the RFP and have no force or effect on the RFP or any resulting Contract unless accepted by the Department and incorporated through a BAFO, negotiation document, addenda to the RFP or amendment to the Contract.

The Department at its sole discretion may consider any proposed modifications submitted in this Attachment.

The Offeror must check one of the boxes below to indicate whether it is proposing modifications to the terms and conditions of the RFP:

- ☐ The Applicant **DOES NOT** propose modifications.
- ☐ The Applicant **DOES** propose modifications as provided in the following table:

	RFP Citation (i.e., section & page number)	Redline of Proposed Modification (i.e., include text as published in RFP and strikethrough words, phrases or sentences proposed to be deleted and underline words, phases, or sentences proposed to be added)
1.		
2.		
3.		
4.		
5.		

ATTACHMENT Y: MINIMUM QUALIFICATIONS

The Offeror must demonstrate it meets the Minimum Qualifications to have its response evaluated by the Department. The Offeror **MUST** complete this Attachment by selecting and checking a box under each numbered or lettered item, where indicated, and providing any necessary details and documentation to demonstrate it meets each required qualification.

Any Offeror Proposal that does not meet any of the Minimum Qualifications provided in this Attachment will be disqualified and will not be given any further consideration by the Evaluation Committee, unless it is determined that such disqualification is not in the best interest of the Department.

1. Agreement to Terms and Conditions

The Offeror agrees and accepts, without exception all terms and conditions, including confidentiality, privacy and security protections and public records and trade secrets protections, specified in *Attachment B: Department of Information Technology Terms and Conditions* and *Attachment C: Agency Terms and Conditions* of this RFP. The Offeror may suggest modifications to the terms and conditions per the instructions in *Section 1.3.3.c* and complete *Attachment X: Request for Proposed Modifications to the Terms and Conditions*, and acknowledges such suggestions are not part of any subsequent Contract unless explicitly accepted by the Department in accordance with *Section 1.3.3.c*.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

2. Eligibility to Contract

- a. As of the date of its submission of a response to this RFP, the Offeror and its subcontractors are not on the list of vendors debarred from doing business with the State of North Carolina.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

- b. As of the date of its submission of a response to this RFP, the Offeror is not on a federal list of parties that are excluded from participation in Medicare, Medicaid, or other federal health care programs, or from receiving federal contracts, or federal financial or non-financial assistance.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

- c. Offeror agrees to notify the Department immediately if it is debarred or excluded from State or federal contracting, participation in health care programs or receipt of financial or non-financial assistance, prior to the Contract Award date.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

- d. Offeror acknowledges and understands that debarment or exclusion from State or federal contracting, program participation, or assistance will result in immediate disqualification from Contract Award.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

3. **Financial Stability and Legal Disclosure**

The Offeror is financially stable and has disclosed any legal actions that could adversely affect its financial condition or ability to meet the requirements of this RFP as required by *Attachment E: Certification of Financial Condition and Legal Action Summary*.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

4. **Experience**

The Offeror has a minimum of five (5) years combined experience providing asset verification services similar to those described in this RFP to include other agencies of State government, county government, municipal government, or corporate employer in NC or in other states. All of the Offeror's experience must have occurred within the five (5) years immediately preceding the date the RFP is issued by the Department. The Offeror is required to provide vendor references and past performance information as required in *Attachment H: Vendor Reference/Past Performance*.

☐ **Offeror Confirms**

☐ **Offeror Does Not Confirm**

By completing and signing this *Attachment Y: Minimum Qualifications*, the Offeror affirms adherence to the required minimum qualifications and attests the information provided herein is accurate, and the individual signing certifies he or she is authorized to make the foregoing statements on behalf of the Offeror.

Offeror Signature

Date

Printed Name and Title

ATTACHMENT Z: SUBCONTRACTOR IDENTIFICATION FORM

The Contractor must complete this *Attachment Z: Subcontractor Identification Form* for each known Subcontractor, as defined in Attachment A: Definitions, who will be used to meet the Contract requirement or otherwise perform any services pursuant to the Contract (i.e., there should be one form for each Subcontractor). After Contract Award, the *Subcontractor Identification Form* must be submitted by the Contractor to the Department for review and approval of all new subcontractors, in accordance with Attachment C, Section 1, Paragraph 30: Subcontractors.

By executing the Contract, or submitting this Attachment after Contract Execution in accordance with Attachment C, Section 1, Paragraph 30: Subcontractors of the Contract, the Contractor:

- 1. Certifies that the information provided in this Attachment is true to the best of its information and belief; and
- 2. Acknowledges the requirements set forth in the Terms and Conditions related to Subcontractors and the resulting obligations, including requiring Department approval of any Subcontractors used in the performance of the Contract; and
- 3. Agrees to notify the Department of any material changes to the information provided in this Attachment that arise prior to execution or during the term of the Contract.

A: Subcontractor Identification	
1. Business Information. Provide the requested Information in the space provided:	
Legal Name of Subcontractor	Click or tap here to enter text.
Name Used for Business if Different	Click or tap here to enter text.
FEIN/Taxpayer ID	Click or tap here to enter text.
Address	Click or tap here to enter text.
Contract Executed	☐ Yes ☐ No
Term of Contract	Click or tap here to enter text.
Name of Contact Person Title Phone Number Email Address	Click or tap here to enter text.
2. Scope of Subcontracted Services. Identify the scope of services and activities that will be provided by the Subcontractor; cite specific Sections of the Contract as applicable:	

Click or tap here to enter text.

3. Is Subcontractor a government entity?

☐ Yes ☐ No

ATTACHMENT AA: ACQUISITION LIFECYCLE REPORTS

Contract Lifecycle Management System Reports

The following table outlines the minimum administrative reports to be generated by the Contract Lifecycle Management (CLM) system during the acquisition lifecycle. These reports must align with industry standards, include comprehensive and accurate data, and be delivered per the frequency guidelines outlined in this Attachment.

Note: All CLM Reports are not separately priced. These reports must adhere to industry standards, incorporate accurate and complete data, and reflect best practices in contract lifecycle reporting. Vendors must ensure that the time and resources needed to configure, generate, and deliver these reports are included in the overall project scope and cost. No separate pricing will be accepted for report generation.

3.0 REPORTS REQUIRED WITHIN THE CLMS SOLUTION

Number	Acquisition Phase	Category	Report Type	Report Description
RPT-001	Pre-Award	Sourcing (RFx)	RFx-to-Contract Conversion Report(s)	Provides RFx events that resulted in contracts, time from RFx initiation to contract execution, and drop-off analysis (RFx events with no resulting contract).
RPT-002	Pre-Award	Sourcing (RFx)	Cost and Savings Report(s)	Provides proposed costs versus awarded contract value and estimated savings from RFx competition and/or negotiation.
RPT-003	Pre-Award	Sourcing (RFx)	RFx Lifecycle Report(s)	Provides time taken for each RFx phase (creation, response, evaluation, and award), delays and bottlenecks, and RFx duration by category and/or Business Unit.
RPT-004	Pre-Award	Sourcing (RFx)	Compliance and Risk Report(s)	Provides contracts missing key clauses or with high-risk terms, deviation reports (from approved clause libraries / templates), insurance, certifications, and audit readiness.
RPT-005	Pre-Award	Sourcing (RFx)	Audit and Version Control Report(s)	Provides a complete audit trail of changes and approvals, redline tracking, version comparison, and user activity logs for compliance audits.
RPT-006	Pre-Award	Sourcing (RFx)	Vendor Response Analysis Report(s)	Provides the number of vendors invited/responded per RFx., a comparison of vendor scores and/or proposals, response time, and completeness.
RPT-007	Post-Award	Awarded	Contract Status Report(s)	Provides an overview of the contract status including the number of new, active, inactive, vendors, spending (or contract value), and contracts approaching renewal (or expiration), as well as their current status (e.g., new contract

Number	Acquisition Phase	Category	Report Type	Report Description
				requests, drafting in negotiation, approved, executed, terminated for cause, terminated for convenience, and non-renewal, amendments, extensions, etc.).
RPT-008	Post-Award	Awarded	Expiring Contracts Report(s)	Highlights contracts near their expiration date, allowing for timely renewal or termination decisions.
RPT-009	Post-Award	Awarded	Vendor Performance Metrics Report(s)	Tracks vendor performance against contract service level agreements (SLA), key performance indicators (KPIs), monthly report cards, scorecards, CSATs regarding quality and timeliness, ease of doing business with, and Vendor/Customer performance metrics, dispute or issue tracking, and level of continuous improvement achieved.
RPT-010	Post-Award	Awarded	Financial Report(s)	Provides insights into contract value, spending, average payments and budget utilization, allowing for more effective financial management.
RPT-011	Post-Award	Awarded	Compliance Report(s)	Tracks compliance with contract terms and regulations, such as: Deliverables, SLAs, Vendor Performance, Notice of Deficiencies, invoice/financial/overcharges, and any other contractual obligations out of compliance or not met.
RPT-012	Post-Award	Awarded	Lifecycle Report(s)	Tracks the progress of contracts through their various stages, from initiation to completion (workflows) as well as their average time to: negotiate a contract, contract terms accepted as-is vs negotiated, to execution, helping identify bottlenecks for downstream activities to escalate the resolution of problems and areas for improvement on the full process.
RPT-013	Post-Award	Awarded	Customizable Report(s)	Offers the ability to create custom reports by filtering, sorting, and grouping data based on specific criteria, such as based on tags, metadata, clause types, business unit, or contract type. Allows end-users to generate reports tailored to their unique needs and/or business requirements.
RPT-014	Post-Award	Awarded	Analytic Report(s)	Provides tools for generating reports and contract data analysis, as part of the reporting and analytics capabilities.

ATTACHMENT AB: INTERFACES – RESERVED

ATTACHMENT AC: GENAI DISCLOSURE AND FACT SHEET

Will you be using or offering GenAI technology, model, or service (collectively, “Solution”)?

☐ Yes ☐ No (If ‘No’, skip to the signature section of this form. If ‘Yes’, provide details regarding the Solution’s GenAI.)

Failure to disclose the use and purpose of GenAI technology to the State as it relates to the Solution requested in this solicitation and submittal of this completed attachment may result in disqualification and may void any resulting contract. Please provide a response to the items listed in each section where indicated.

1. **Technical Specifications:** – Address the following items in your response:

- a. **Model Name, Version & Number of Parameters:** The unique identifier or name assigned to the specific GenAI model or service.
- b. **Model Owner:** The name of the organization or entity responsible for creating or deploying the GenAI model or service.
- c. **Overview:** A concise summary of the GenAI model’s purpose, functionality, and key characteristics.
- d. **Purpose:** The intended use or goal of the GenAI model (e.g., image recognition, natural language processing, text summarization).
- e. **Intended Domain:** The context, subject matter or domain for which the GenAI model is designed to operate effectively.
- f. **Training Data:** Information used to train the GenAI model (e.g. labeled images, text corpora)
- g. **Model Information:** Details about the architecture, parameters and configuration of the GenAI model.
- h. **Inputs and Outputs:**
 - i. Inputs: The data or features provided to the model for prediction (e.g., images, text).
 - ii. Outputs: The GenAI model’s predictions or results (e.g., class labels, probabilities).
- i. **Customization and Flexibility:** Details on how the solution can be customized to meet specific needs including fine-tuning capabilities.
- j. **Integration Capabilities:** Compatibility with existing systems, API’s and platforms.
- k. **Scalability:** Details on how the solution scales with increased usage or data volume.

Vendor’s Response for Section 1

2. **Data Handling and Privacy** – Address the following items in your response:

- a. **Data Requirements:** Types of data needed for the solution to function effectively.
- b. **Data Security:** Measures in place to protect data during transit and storage, including encryption standards.
- c. **Data Privacy:** Compliance with data privacy regulations (e.g., GDPR, CCPA) and policies on data ownership and usage.
- d. **Anonymization:** Techniques used to anonymize personal data, if applicable.

Vendor's Response for Section 2

3. **Ethical Considerations** – Address the following items in your response:

- a. **Ethical Guidelines:** Adherence to ethical AI guidelines and principles.
- b. **Impact Assessments:** Regular assessments of the AI's impact on various stakeholders.
- c. **Transparency:** Level of transparency regarding how the AI models make decisions.
- d. **Accountability:** Processes in place for addressing errors or unintended consequences.
- e. **Bias and Fairness:** Methods for detecting and mitigating biases in the AI models.
- f. **Optimal Conditions:** The ideal environment or context for the GenAI model to perform optimally.
- g. **Poor Conditions:** Scenarios or conditions where the GenAI model's performance may degrade.

Vendor's Response for Section 3

4. **Operational Details** – Address the following items in your response:

- a. **Deployment Options:** Available deployment models (cloud, on-premises, hybrid).
- b. **Maintenance and Support:** Support services, including SLAs, and frequency of updates and patches.
- c. **Training and Documentation:** Availability of training materials, user manuals, and ongoing support.

Vendor's Response for Section 4

5. **Cost and Licensing** – Address the following items in your response:

- a. **Pricing Model:** Detailed breakdown of costs, including licensing fees, usage-based fees, and any additional charges.
- b. **Licensing Terms:** Terms and conditions of the software license, including duration, renewal, and termination clauses.

Vendor's Response for Section 5

6. **Performance Metrics** – Address the following items in your response:

- a. **Definition:** Quantitative measures (e.g., accuracy, F1-score) used to evaluate the GenAI model's performance.
- b. **Assessment:** Determines how well the GenAI model meets its intended purpose.
- c. **Continuous Monitoring Plan:** Establishes a plan for continuous monitoring and evaluation of the GenAI model's performance.
- d. **Benchmarks:** Performance benchmarks and KPIs used to measure the solution's effectiveness.
- e. **Case Studies and References:** Examples of previous implementations and references from existing clients.

Vendor's Response for Section 6

7. **Regulatory Compliance** – Address the following items in your response:

- a. **Regulatory Standards:** Compliance with industry-specific regulations and standards (e.g., HIPAA for healthcare, IRS Pub 1075, SSA and SAMSHA).

Vendor's Response for Section 7

8. **Innovation and Roadmap** – Address the following items in your response:

- a. **Future Plans:** Vendor's roadmap for future development and innovation in their GenAI solutions.
- b. **Partnerships and Ecosystem:** Collaborations with other technology providers and integration within a broader AI ecosystem.

Vendor's Response for Section 8

9. Explain how you are ensuring the GenAI system is not adversely affecting decisions that materially impact access to, or approval for, housing or

accommodations, education, employment, credit, health care, and criminal justice.

Vendor's Response for Section 9

10. Additional Information that you may like to share:

Offeror Signature

Date

Printed Name and Title