STATE OF NORTH CAROLINA

Department of Health and Human Services

Division of Health Benefits

Request for Proposal #30-2025-008-DHB

Data Analytics Platform

STATE OF NORTH CAROLINA

Request for Proposal

#30-2025-008-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: Kevin Barlage Contract Specialist kevin.barlage@dhhs.nc.gov Medicaid.Procurement@dhhs.nc.gov	**Request for Proposal # 30-2025-008-DHB**
	Date RFP Issued/Posted: 5/11/2026
	Date RFP Submissions due to the Department: 7/17/2026 at 2:00 p.m. EST
	Proposals will be opened: 7/17/2026 at 2:00 p.m. EST
	Contract Type: Open Market
	Commodity Number: 811620 - Cloud-based software as a service
	Description: Data Analytics Platform
	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

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 Request for Proposal (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, 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 Anticipated Procurement Schedule*.
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 Anticipated Procurement Schedule*.
c. **Submission of Proposals** will be accepted until the date and time indicated in the RFP Schedule in *Section 1.4.1 Anticipated Procurement Schedule*.

1.1.6 BIDDER'S LIBRARY

The Bidder's Library is a collection of documents, data, and reference materials that the Department provides to prospective Offerors during the RFP process. Its primary purpose is to give Offerors access to relevant background information necessary to develop informed, accurate, and compliant proposals. The contents of the Bidder's Library are provided solely for informational purposes and will not be included as part of the final contract.

The documents contained in the Bidder's Library will be available only while the solicitation remains open in the Ariba Sourcing Tool. Offerors are strongly encouraged to review the Bidder's Library section found in the solicitation in the Ariba Sourcing Tool and download the documents for review and future reference. After the solicitation closes in the Ariba Sourcing Tool, the documents in the Bidder's Library will no longer be accessible.

The content of the Bidder's Library reflects the current state of information at the time the RFP is issued and is not guaranteed to be updated throughout the procurement process.

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

1.2.6 DISCLOSURE OF ARTIFICIAL INTELLIGENCE (AI) USE

The Offeror shall disclose whether Artificial Intelligence (AI), including generative AI tools, was used in the preparation of any portion of its response to this RFP. If AI tools were utilized, the Offeror affirms that it has reviewed and verified the accuracy, completeness, and appropriateness of all AI-generated content. The Offeror shall remain solely responsible for the content of its submission, including any errors, omissions, or misrepresentations resulting from the use of AI.

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 1.4.1-1 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	5/11/2026	
Register for Pre-Proposal Conference	Offeror(s)	5/13/2026	10:00 am
Pre-Proposal Conference	Offeror(s) and Department	5/14/2026	2:00 pm
Written Questions Deadline	Offeror(s)	5/21/2026	2:00 pm
Agency's Response to Written Questions / RFP Addendum Issued	Department	6/5/2026	
Proposals Due	Offeror(s)	7/17/2026	2:00 pm
Proposals Evaluation Begins	Department	7/20/2026	
System Demonstrations	Offeror(s)	10/20/2026	
Estimated Contract Award	Department	2/26/2027	
Protest Deadline	Responding Vendors	15 days after award	

Table 1.4.1-1 RFP Schedule

1.4.2 PRE-PROPOSAL CONFERENCE

a. The Department will hold a virtual Pre-Proposal Conference on the date and time indicated in the RFP Schedule in *Section 1.4.1 Anticipated Procurement Schedule* for one hour via Microsoft (MS) Teams. No purchase is required to use the MS Teams application.

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 Pre-Proposal 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 Anticipated Procurement Schedule*.

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 of the Pre-Proposal Conference 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 Pre-Proposal Conference.

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The Purpose of this RFP is the for the North Carolina Department of Health and Human Services (NCDHHS), Division of Health Benefits (DHB or Department) to solicit offers for the acquisition of a Data Analytics Platform solution.

The Decision Support System (DSS) / Data Warehouse (DW) (DSS/DW) business area encompasses software tools used by the Department to extract and/or analyze Medicaid data to inform program and policy decisions, and to report on the delivery of the Medicaid program. The DSS/DW module has been named by the Department as the Data Analytics Platform (DAP), which will serve as the formal reference for this initiative and solution.

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 and unless otherwise terminated in accordance with the Contract.

2.2.1 OPTIONAL EXTENSIONS

After the initial term, the State shall have the option to extend the Contract for two (2) additional one (1) 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 then current term.

2.2.2 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 close-ended contract between the awarded Vendor and the State to furnish a pre-determined quantity of a good or service 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

NCDHHS manages the delivery of health- and human-related services for all North Carolinians, especially our most vulnerable citizens – children, elderly, disabled 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 to make this happen. Within NCDHHS, NC Medicaid is dedicated to providing access to physical and behavioral health care and services to improve the health and well-being of over 3 million North Carolinians.

NCDHHS is replacing the Department's Medicaid Management Information System (MMIS) with a Medicaid Enterprise System (MES), also referred to as the Medicaid Integrated Modular Solution (MIMS). MIMS will be implemented through a multi-phase initiative, the MMIS Replacement Project. The MMIS Replacement Project will implement a series of interrelated modules. These modules will have functionality designated by the Centers for Medicare & Medicaid Services (CMS) in support of obtaining compliance with Medicaid Information Technology Architecture (MITA) Framework and CMS certification for each module.

The NC MIMS system will modernize and transform North Carolina Medicaid and its sister divisions, including the Division of Mental Health (DMH), Division of Public Health (DPH), and Office of Rural Health (ORH). NC MIMS will improve the Provider and Medicaid beneficiary experience across the enterprise.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 SCOPE OF WORK

The DAP solution will be a scalable, cloud-based platform that enables faster, data-driven decisions. It will replace legacy systems with modular, secure, and automated solutions. This shift supports improved transparency, operational efficiency, and healthcare outcomes. The DAP solution will facilitate faster, data-informed decisions that improve care delivery, policy evaluation, and population health. It will enhance reporting accuracy, reduce operational delays, and support compliance with federal and legislative mandates. Overall, it advances the Department's mission to deliver high-quality, efficient, and equitable healthcare to Medicaid beneficiaries. The anticipated go-live date for the DAP solution must occur no later than July 1st, 2029.

The figure in *Attachment U: Conceptual Architectural Diagrams* provides an architectural diagram of the envisioned future state. This diagram serves as a general reference for the solution architecture envisioned by the Department and illustrates top-level information flow. Vendors are encouraged to propose innovative approaches and solutions that achieve the outcomes and functionality described in this document.

3.1.1 SOLUTION OVERVIEW

The State seeks to implement a modern, secure, cloud-based data and analytics platform built on a cloud provider such as Microsoft Azure, Amazon AWS, or Google GCP, along with a Data Warehousing solution that includes a user-friendly interface and built-in BI capabilities such as Snowflake, Databricks, or similar. The platform will provide a unified, scalable, and governed foundation for ingesting, storing, transforming, and consuming enterprise data in support of analytics, reporting, and AI-driven decision-making. The goal of the solution is to enable the State Business

Intelligence (BI) team and non-technical Business teams to easily interact with the data and generate insights using SQL and/or drag-and-drop functionalities.

The solution shall adopt an API-first, modular architecture consistent with MITA modularity principles, enforcing clear domain separation (e.g., claims, provider, eligibility services) through secure, versioned APIs while also supporting additional integration patterns such as batch data ingestion, ELT/ETL pipelines, streaming, events, and secure file-based exchanges based on the operational needs of the Department.

The Vendor will propose a technology stack with associated tools and services to meet the stated technical requirements and specifications within this document, and to ensure the overall solution remains cost-optimized, maintainable, and compliant with State and Federal security standards. The Department intends for the Solution to use the following technology elements as the foundation of the Solution:

a. Cloud hosting and infrastructure services.

b. Enterprise data warehouse and governed data sharing platform for business and technical users.

c. Business intelligence and visualization layer supporting AI-assisted analytics and self-service dashboards.

d. Primary programming languages such as Python, PySpark, and SQL, or similar for data engineering, transformation, and analytics.

e. The Solution will use existing State procured SAS EG Desktop licenses or set up Vendor procured SAS licenses initially to integrate and connect with the data warehouse for transition continuity, with a planned phased retirement as workloads migrate to the new programming languages such as Python, PySpark, and SQL.

f. Version control, CI/CD automation, and DevOps pipeline orchestration.

g. Infrastructure as Code (IaC) implementation.

The Department currently utilizes Microsoft-based analytics, Power BI, and Co-Pilot as enterprise AI assistant capabilities as part of its analytics and AI strategy. The proposed technology stack should enable a cloud-native architecture optimized for the analytics and AI platforms in use by the Department.

The project is intended to be delivered in two main stages:

1) Design, Development, and Implementation (DDI): A period during which the Vendor will provide services, including platform design, implementation, testing, and migration of reports, data, and code. This stage is intended to include a substantial period for a parallel run of the current analytics platform solution and the DAP solution;

2) Operations & Maintenance (O&M):

   i. Hypercare: A period during which the Vendor will provide training, coaching, change management support, remediation of migration-related defects, and begin to provide data engineering services for pipeline maintenance and enrichment, and full platform administration;

   ii. Steady State: The Vendor will continue to maintain and administer the platform, provide data engineering services, and continue to address any residual migration defects.

Refer to table *3.1.1-1 Stage Activities* below for a more detailed breakdown of activities across the stages.

Area of Activity	During DDI	O&M - Hypercare	O&M - Steady State
Platform / Infrastructure	Design and implementation	Maintenance and Administration	Maintenance and Administration
Data Security & Privacy	Design and implementation	Maintenance and Administration	Maintenance and Administration
DevOps	Design and implementation	Maintenance and Administration	Maintenance and Administration
Data Governance	Implement broader NC Medicaid solution, if one is adopted, or stand up and populate a data catalog /glossary if not adopted.	Maintenance and Administration of Catalog and its content	Maintenance and Administration of Catalog and its content
Data Architecture	Design and implementation	Maintenance and continuous alignment to Data Architecture	Maintenance and continuous alignment to Data Architecture
Data Engineering	Design and implementation. Provide training and change management to the State	Lead Data Engineering activities, maintain existing data pipelines, resolve data pipeline defects, coach / train State resources in this area.	Lead Data Engineering activities, maintain existing data pipelines, and resolve data pipeline defects
DataOps	Design and implementation. Provide training and change management to the State	Lead Data Ops activities and coach / train State resources in this area.	Lead DataOps activities
Data Product Management	Migrate existing data products and build new data products.	Maintain existing Data Products, deploy to production data products developed by the State, and coach / train State resources in this area.	Maintain existing data products and deploy to production data products developed by the State.
BI/Reporting	Migrate existing reports and dashboards	Resolves any new defects found on migrated reports and dashboards	Resolves any new defects found on migrated reports and dashboards
Data Science / ML / Advanced Analytics	No work required	Consult and advise the State in this area.	Consult and advise the State in this area.
Change Management & Adoption	Develop training and develop a change management plan for platform adoption	Provide training and guidance and execute the post go-live elements of the change management plan	Provide periodic training

Table 3.1.1-1 Stage Activities

3.1.2 SOLUTION DEVELOPMENT ACTIVITIES

The development of the Solution is expected to be executed in distinct phases, beginning with initiation and planning activities such as workgroup kick-off, stakeholder engagement, and development of a comprehensive project plan with finalized milestones and deliverables. Subsequent phases will include design, development, and configuration of the solution, as well as data, code, and report migrations, using an agile or similar methodology. Testing phases will encompass system integration,

user acceptance, and end-to-end validations, ensuring performance, security, and compliance with regulatory standards. The State expects to run the Solution and the existing system in parallel for several months prior to Solution go-live. The project will culminate in go-live deployment, operational transition, and post-implementation support, with ongoing operations and maintenance activities to address enhancements, change requests, and system updates. Throughout all phases, the Vendor will work closely with the State, provide regular status reporting, and adhere to project management best practices for schedule, issue, budget, and resource management.

The graphic in *Image 3.1.2-1: Development Activities Overview* below provides a representative high-level view of the activities expected to be included in the development of the Solution.

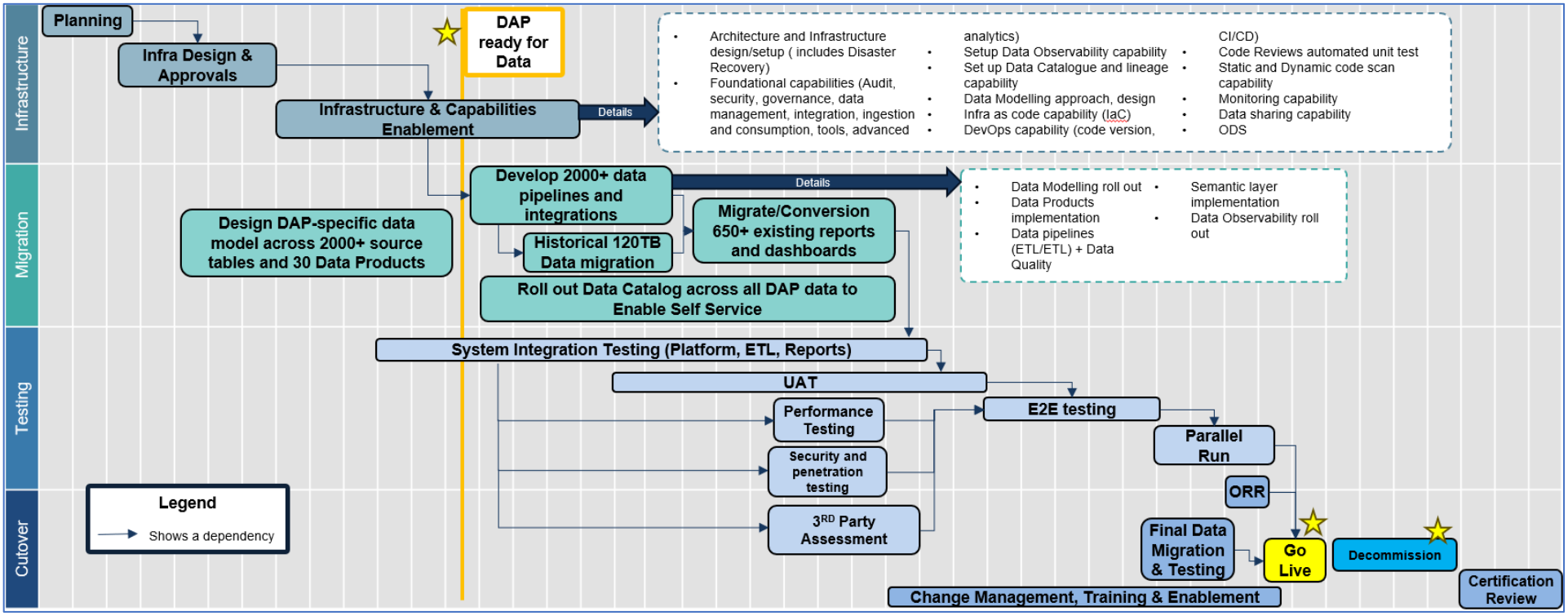


Image 3.1.2-1 Development Activities Overview

3.1.3 PLATFORM ENABLEMENT

The key elements of the work to be performed include designing, building, testing, and operationalizing a modern data platform and migrate legacy assets into the new environment prior to go-live. Work will be executed using automated, secure, and risk-controlled delivery patterns, ensuring quality, continuity, and adoption. The Vendor will provide design and implementation services during the DDI phase of the project and ongoing operational support of the platform after solution go-live.

The main elements and outcomes of the platform enablement include:

a. **Cloud Platform and Infrastructure:** The objective is to build a secure, scalable, and resilient cloud-based analytics infrastructure. This effort includes designing and deploying multiple environments across the tech stack (e.g., cloud platform, data warehouse, BI tool, Data Governance tool), with robust networking, access controls, disaster recovery, monitoring, and metadata management to support enterprise-wide data operations. This effort also includes work to develop APIs, FHIR, and HL7 interfaces to ensure secure and high-performance access to curated datasets.

b. **DevOps, Automation, and CI/CD**: The objective is to use Infrastructure-as-Code (IaC) and CI/CD pipelines to automate provisioning, testing, deployment, and promotion of environments, platform components, and data pipelines. This work includes enforcing change-control gates and sprint-based release management to ensure structured and compliant delivery.

c. **Data Architecture and Modeling:** The objective is to design a modern data architecture with subject-area-aligned data models tailored for analytics, reporting, and performance. Curated silver, gold, and consumption data layers are expected, in addition to an Operational Data Store (ODS), to support the creation of governed and high-quality data products and reports.

d. **Ingestion, Transformation, and Pipeline Modernization:** The objective is to define best-practice-aligned data ingestion and consumption patterns, build automated data pipelines, implement Change Data Capture (CDC), orchestration, and performance optimization to ensure efficient and scalable data operations.

e. **Analytics and BI Enablement:** The objective is to establish the enterprise Power BI environment, semantic models, and data marts aligned with the new architecture, accompanied by the implementation of robust governance practices. This effort also includes setting workspace standards, enforcing row-level and column-level security, and applying performance optimization techniques to ensure secure, efficient, and scalable analytics operations.

f. **Advanced Analytics Foundation:** The objective is to prepare platform services and data structures to enable advanced analytics, Machine Learning, GenAI, and AI capabilities.

g. **Analyst Workspaces and Innovation:** The objective is to provision on-demand analyst workspaces to enable self-service for approved users, offering read-only access to production data, the ability to load and analyze user-supplied data, and the capability to develop reports and queries in isolation. These analyst workspaces will be strictly restricted from writing back or modifying production data. A formal promotion workflow will be established to allow analyst workspace-developed assets to move into production.

h. **Security, Observability and SLA Monitoring**: The objective is to deploy tools to monitor pipeline health, detect data drift, track usage patterns, provide real-time alerting, and monitor the Solution to enforce adherence to the SLA's in *Attachment L: Service Level Agreements*. Dashboards will be configured to enable cost control and system performance insights. The platform is expected to be secured using modern best practices aligned with federal and state regulations for managing PII and PHI, including row- and column-level security, private endpoints, single tenancy, encryption, role-based access controls, auditing, data privacy, and data-sharing controls.

i. **Change Management, Training, and Adoption**: The objective is to deliver structured training tailored to technical staff, analysts, and business users to enable data literacy and self-service in the organization. Part of this work will include the development of standard operating procedures (SOPs), operating playbooks, governance documentation, and onboarding guides. These efforts are meant to facilitate organizational change and ensure a smooth transition to the enhanced data environment.

3.1.4 ASSETS MIGRATION AND VALIDATION

The key elements of the work to be performed involve migrating approximately 110-120 TB of historical data and metadata into the DAP environment, which includes around 2000 tables, and aligning them with the new data model. This process includes validating data completeness, structure, and business rule fidelity against legacy systems, and authenticating datasets through automated data quality checks, audit controls, and robust testing.

This work will include rewriting and modernizing legacy ETL logic, scripts, and views, including the conversion of SAS code to DAP-based programming languages (such as SQL and Python / PySpark). SAS files and datasets stored in the current analytics platform will need to be moved to DAP object storage. Additionally, over 650 reports and dashboards will need to be converted from platforms like Cognos and Tableau to Power BI, ensuring alignment with the new model. It is expected that side-by-side parallel testing and reconciliation will be conducted to ensure accuracy before final cutover.

Tables 3.1.4-1 Migration Assets, 3.1.4-2 Scripts/Views, and 3.1.4-3 Reports provide an inventory summary of the data, scripts, and reports that are expected to be migrated to DAP as a part of the effort.

			Complexity		
Migration Assets	***Migration Activity***	***Total***	***Simple (Pass Through ETL)***	***Medium (Few joins, transformations)***	***Complex (Aggregations, Transformations)***
BIDP Tables (Internal AWS Redshift Data Warehouse)	Migrated in DAP, populated into Bronze and Silver layers via new ETL/ELT logic to be written as part of this initiative	550	550	0	0
Tables	Ingested in DAP, populated into Bronze and Silver layers leveraging existing ETL/ELT (DataStage) logic	2,020	1572 (most of these are stand alone, used as intermediate tables for data processing)	186	262
ETL/ELT Jobs (DataStage)	Rewritten and optimized for DAP data model and architecture, applied to migrated tables to build Bronze and Silver layer	1,959	1,159	638	162

			Complexity		
Migration Assets	***Migration Activity***	***Total***	***Simple (Pass Through ETL)***	***Medium (Few joins, transformations)***	***Complex (Aggregations, Transformations)***
Database Procedures	Existing Jobs/Scripts/Views might reference these procedures, and the logic needs to be preserved and rewritten in DAP	36	18	2	16

Table 3.1.4-1 Migration Assets

			Complexity		
Scripts/Views	***Migration Activity***	***Total***	***Simple (<300 lines of code)***	***Medium (300 -1000 lines of code)***	***Complex (>1000 lines of code)***
PCDU ad-hoc XLS, XLSX, CSV, and TXT files	ETL/ELT scripts developed to process landing data in DAP, apply data quality (DQ) checks (currently via Python-based Data Quality Script), and generate required JSON and Excel response files with results sent to PCDU. After passing DQ checks, the scripts ingest files in DAP, and populate into Bronze and Silver layers	550	550	0	0
SQL Views (Both Materialized and regular)	Rewritten and optimized for DAP data model	2,232	53	58	2,121
Encryption / Decryption Scripts	Certain assets being migrated might use these, and they need to be correctly decrypted/encrypted using equivalent logic	53	0	52	1
SAS Macros (Functions)	No migration necessary but existing SAS reports might reference these, and the logic needs to be preserved	140	not applicable	not applicable	not applicable
SAS Program Files (.sas)	No rewrite is needed, but files need to be stored in DAP object storage as-is for archival/auditing purposes	114,699	not applicable	not applicable	not applicable
SAS Dataset Files (.sas7bdat)	No rewrite is needed, but files need to be stored in DAP object storage as-is for archival/auditing purposes	108,467	not applicable	not applicable	not applicable
SAS Project Files (.egp)	No rewrite is needed, but files need to be stored in DAP object storage as-is for archival/auditing purposes	4,517	not applicable	not applicable	not applicable

			Complexity		
Scripts/Views	***Migration Activity***	***Total***	***Simple (<300 lines of code)***	***Medium (300 -1000 lines of code)***	***Complex (>1000 lines of code)***
Existing Data Products (including intermediate tables created that are not exposed to end users)	Rewritten and optimized for DAP data model and architecture, applied to migrated tables to build Gold layer	139	130	5	4
Python-based Data Quality Script	Rewritten and optimized for DAP. Might be extended if needed	1	0	0	1

Table 3.1.4-2 Script/Views

			Complexity		
Reports	***Migration Activity (applicable to both scripts/code and dashboards)***	***Total***	***Simple (<200 lines of code)***	***Medium (200 -1500 lines of code)***	***Complex (>1500 lines of code)***
Cognos	Migrated and optimized for DAP	51	36	7	8
Excel	Migrated and optimized for DAP	1	not applicable	not applicable	not applicable
SAS	Migrated and optimized for DAP	330	83	162	85
SAS - Desktop	Migrated and optimized for DAP	6	4	2	0
Tableau	Migrated and optimized for DAP	61	11	26	24

Table 3.1.4-3 Reports

3.1.5 DATA MANAGEMENT AND GOVERNANCE

The work includes implementing a lean and native Data Governance tool for DAP and creating a unified Data Catalog featuring a technical Data Dictionary and Business Glossary. Data profiling activities can leverage the data warehouse engine directly rather than external tools. The Vendor will be expected to engage business data stewards and owners to populate the Data Catalog, align with the Medicaid Enterprise Data Governance guidelines and policies (to be shared during DDI), and curate business, technical metadata, and CDEs. A data quality framework will be defined and automated for critical data elements, validation, and stewardship workflows. It is expected that security will be enforced through role-based and attribute-based access controls (RBAC/ABAC), encryption, and key management for data at rest and in transit. Additionally, auditing and cost tracking will be enabled for platform visibility, and secure data sharing and collaboration will be supported through cloud native capabilities and managed identities. Data management will emphasize transparency, compliance, and usability across all stakeholders.

3.1.6 DATA PRODUCTS

The Vendor will be expected to design and deliver 30 new data products—curated, domain-aligned datasets created by joining multiple source tables and applying standardized transformation, validation, and business logic. These data products must serve as reusable building blocks that streamline and accelerate future reporting, analytics, and data science by providing consistent, analysis-ready views of major data domains.

3.1.7 ONGOING SUPPORT AND OPERATIONS

Upon completion of implementation, the Vendor is expected to transition to Ongoing Maintenance and Operational Support (O&M) in collaboration with the State team. This support will unfold in two stages: 1) Hypercare stage, a two-year period focused on training, coaching, change management, defect remediation, and full platform administration including data engineering services; and 2) Steady State stage, where the Vendor continues platform and pipeline maintenance and addresses any remaining migration issues, though without dedicated BI developer support.

Following go-live, the State will assume ownership of new Data reporting development, while the Vendor will be responsible for the continued operation, optimization, and enhancement of the cloud environment, DevOps toolchains, data engineering workflows, data integration pipelines, and underlying platform services. The Vendor is expected to ensure high availability, performance tuning, incident response, and continuous improvement of all production data pipelines and platform components in accordance with the Department's enterprise architecture and operational governance standards.

Hypercare and Steady State O&M stages both include the following key elements of work:

a. **Platform and Infrastructure Management:** Administer and maintain the platform, including periodic review and implementation of performance and cost optimization recommendations.

b. **Security and Compliance:** Ensure continuous monitoring, patching, vulnerability management, and preventive maintenance, including enforcement of security posture management and adherence to NIST 800-53 controls.

c. **Data Engineering and DataOps:** Maintain and continuously optimize all production data pipelines, enhance Bronze/Silver layers, provide guidance to the State in developing new data products, and deploy the State developed data products to production.

d. **Monitoring and Optimization:** Provide continuous monitoring, alerting, and incident response.

e. **Training and Knowledge Transfer**: Provide documentation, training sessions, and mentoring to ensure the State team is enabled for self-service and can independently sustain operations.

f. **General Administration:** Support user onboarding, access management, testing, and cost reporting.

g. **Ad-Hoc Data Needs:** The Department may require the Vendor to perform supplemental data ingestion, integration pipeline development, transformation logic updates, semantic layer modifications, and support reporting conversions on an ad-hoc basis. All such requests shall be executed in alignment with the State approval processes and governance committees.

3.1.8 CONSULTING SERVICES

During the Operations and Maintenance phase of the work, the Department expects the Vendor to provide consulting services, upon request, that may include activities such as advanced analytics, statistical analysis, AI/ML/Gen AI use case development and support, and other similar ad-hoc requests. The Department expects to have consulting resources available on a fully burdened hourly rate basis to use toward these services activities. For example, the Vendor may support initial GenAI and Machine Learning use cases and transition eventual ownership of the activities to the Department. Additionally, the Department expects the Vendor to provide hands-on training in topics such as Data

Science tools, algorithms, techniques, GenAI, and others. Any consulting services must be proposed and adjudicated through the change request management process as provided in *Section 7.14.2 Change Request Management Process*.

3.1.9 STAFFING

The Vendor is expected to provide a multidisciplinary team capable of delivering across design, build, migration, and O&M phases. The Vendor resources will work in close partnership with the State staff throughout the Design, Development, and Implementation (DDI) phase, continue to provide operational support and guidance during the O&M period, and transition responsibilities to the State as the contract end date approaches. Key personnel roles are included in *Attachment K: Vendor Key Personnel*.

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 Department 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 Department maintains a comprehensive set of Enterprise Architecture artifacts that must be created and maintained by Vendors. The Department's Enterprise Architecture is based on the Federal Enterprise Architecture framework and is aligned with the MITA framework. The Department's framework will leverage the MITA standards and additionally use standard conventions such as Unified Modeling Language (UML) 2 and Business Process Modeling and Notation (BPMN). The Department maintains the right to add or change its Enterprise Architecture artifacts as its needs change. The Vendor will be required to provide and maintain standard documentation. The details are referenced in *Attachment J: Enterprise Architecture*.

3.3 SECURITY SPECIFICATIONS

3.3.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE - RESERVED

3.3.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

The Data Analytics Platform 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 agrees to meet all requirements as part of the technical proposal as referenced 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. Platform Architecture

Requirement #	Requirement Description
DAP-REQ-ARC-002	The Solution must implement cost optimization, including tiered storage, autoscaling, idle compute shutdown, and usage dashboards visible to NCDHHS leadership.
DAP-REQ-ARC-015	The Solution must allow administrators to configure resource quotas (compute hours, storage size, concurrency limits) per analyst workspace user or group.
DAP-REQ-ARC-016	The Solution must enable creation of shared analyst workspace projects where multiple business users can collaborate on the same datasets.
DAP-REQ-ARC-017	The Solution must enforce data egress controls, including approval gates or data loss prevention (DLP) scanning for data exports from analyst workspaces inside of the Production environment.
DAP-REQ-ARC-018	The Solution must implement analyst workspace lifecycle management, including automated detection of inactive or expired analyst workspace and datasets based on business rules such as last accessed timestamp, and notification to data and environment owners prior to automated clean up.
DAP-REQ-ARC-019	The Solution must log all analyst workspace activity, including queries, dataset access, and data exports in an auditable format.
DAP-REQ-ARC-020	The Solution must provide a governed workflow to promote select analyst workspace-created code into curated or production layers.
DAP-REQ-ARC-021	The Solution must provide a self-service, governed data upload capability for analyst workspace users, supporting multiple file formats with automated metadata capture and schema validation.
DAP-REQ-ARC-022	The Solution must provide secure, governed analyst workspace for ad-hoc work and experimentation, with isolated compute, enabling access to approved production datasets and user-uploaded data, while preventing direct writes or changes to production systems and cross-user data contamination, supporting iterative development, version control integration, and an on demand IaC deployment model.
DAP-REQ-ARC-023	The Solution must support just-in-time (JIT) access provisioning that allows users to request and receive temporary elevated privileges (e.g., administrative or contributor access) only for a defined time period and specific purpose. The system must automatically revoke or expire such elevated access once the approved duration ends.
DAP-REQ-ARC-024	The Solution's architecture must support metadata-driven orchestration and transformation, including parameterization, schema evolution, and dynamic pipeline generation.
DAP-REQ-ARC-025	The Solution's architecture must support versioning of data and the retention of historical data versions in accordance with documented policies, ensuring full auditability, reproducibility of all analytics, and compliance with Medicaid requirements.
DAP-REQ-ARC-026	The Solution must support environment separation with consistent configuration, RBAC policies (including least privilege permissions), and secure promotion between environments.
DAP-REQ-ARC-027	The Solution must have a geospatial analytics capability, including geocoding, calculating time and distance between members and providers, and supporting related analytics use cases.
DAP-REQ-ARC-029	The Solution must provide REST APIs, SDKs, and CLI tools for programmatic access and automation.

Requirement #	Requirement Description
DAP-REQ-ARC-030	The Solution must support certified connectors for BI, ETL, and notebook tools, including Power BI, Tableau, and Jupyter.
DAP-REQ-ARC-031	The Solution must support containerization and orchestration (e.g., Docker/Kubernetes) for portability, resilience, and autoscaling.
DAP-REQ-ARC-032	The Solution must support data integration patterns that enable loading data into medallion architecture layers as well as directly into analyst workspaces.
DAP-REQ-ARC-033	The Solution must support geospatial visualization capabilities similar to ArcGIS functionality, either natively or through integration with the visualization layer.
DAP-REQ-ARC-034	The Solution must support multi-environment deployments (e.g. Dev, Test, Prod) using reusable and parameterized IaC modules that ensure parity across environments.
DAP-REQ-ARC-035	The Solution must support scheduling specific queries or reports to be processed at a specifically stated time and/or with event or other triggers (Dependency-based, Data-change (CDC)-based, Manual (ad-hoc), Conditional (rule-based)).
DAP-REQ-ARC-036	The Solution must support workload management features including query prioritization, timeouts, and resource pools.
DAP-REQ-ARC-037	The Solution must be deployed on a cloud-native architecture using managed services and must support scalability, elasticity, and modular growth.
DAP-REQ-ARC-038	The Solution must include cloud-native object storage to support scalable, secure, and governed storage of structured, semi-structured (e.g., JSON, XML, FHIR, HL7), and unstructured (e.g., PDFs, Free-text documents) data, with integration into the metadata catalog, data lineage, and data lifecycle management framework.
DAP-REQ-ARC-039	The Solution must support a modular, layered data architecture (e.g., Bronze → Silver → Gold → Semantic) to promote scalability, domain alignment, and governance.
DAP-REQ-ARC-040	The Solution must support open and interoperable data exchange by adhering to widely accepted industry standards such as X12, EDI, FHIR, JSON, XML and RESTful APIs using JSON as the standard data interchange format.
DAP-REQ-ARC-041	The Solution must execute advanced analytics workloads, including PySpark and SQL-based scripts, within scalable cloud-native compute environments.
DAP-REQ-ARC-043	The Solution must support automatic query-plan optimization and result caching for frequently accessed dashboards and datasets.
DAP-REQ-ARC-044	The Solution must enable accurate chargeback reporting and clear accountability by supporting logical separation of all resources—such as compute, storage, and analyst workspaces—by internal divisions (e.g., DMH and DPH) and other authorized entities. Each compartment must allow for independent governance, usage tracking, and cost/billing management.
DAP-REQ-ARC-045	The Solution must provide functionality to create a complex query using Structured Query Language (SQL) program code or importation of ANSI standard SQL code.
DAP-REQ-ARC-046	The Solution must provide functionality to view query, report, algorithms; or model results into a wide variety of user defined graphical formats (e.g., scatter plots, bell curves, pie charts) both as a part of a Business Intelligence Solution and during data exploration.
DAP-REQ-ARC-047	The Vendor must communicate the availability of new features for all Solution capabilities and assist the Department to test and enable the new functionality.
DAP-REQ-ARC-049	The Vendor must provide sufficient environments and configurations (e.g., multiple environments, multiple application layers, hub architecture) necessary to perform all required functions (e.g., testing, training, production operations, modeling, disaster recovery).
DAP-REQ-ARC-050	The Solution must detect and alert on anomalous usage patterns, including excessive compute usage or unusual data access (e.g., geolocation, time, date).
DAP-REQ-ARC-052	The Solution must provide a Development (DEV) environment for building and unit testing data platform components and pipelines, using mock or sample data, supporting iterative development, version control integration, governed promotion to Testing (SIT) environment, automated test execution, and an IaC deployment model.

Requirement #	Requirement Description
DAP-REQ-ARC-053	The Solution must provide Testing (SIT) environments to enable system integration testing using masked or obfuscated scaled down production-like data, replicating production configurations, adjusted down for size, to validate end-to-end workflows, data flows, and system interoperability while ensuring data privacy compliance, and supporting version control integration, governed promotion to Pre-Production (PREPROD), automated test execution, and an IaC deployment model.
DAP-REQ-ARC-054	The Solution must provide a Pre-Production (PREPROD) environment that mirrors production controls, configurations, networking, security, and data, enabling activities such as user acceptance testing, performance testing with regularly refreshed datasets, and security/penetration testing, while supporting version control integration, governed promotion to Production (PROD), automated test execution, and an Infrastructure as Code (IaC) deployment model.
DAP-REQ-ARC-055	The Solution must provide an isolated, secure, scalable, and highly available Production (PROD) environment for live business operations.
DAP-REQ-ARC-056	The Solution must provide a Disaster Recovery / Business Continuity (DR/BC) environment with cloud-managed backups of production data, enabled for annual disaster recovery testing that meets RTO and RPO targets as defined in the SLAs.
DAP-REQ-ARC-057	The Solution must provide an on-demand End to End Testing (E2E) environments that can be stood up as needed to perform full end-to-end validation of data platform components and workflows using production data.
DAP-REQ-ARC-058	The Solution must replicate the Production environment security controls in any lower environment where production data is loaded.
MES-REQ-ARCH-002	The Solution's user interfaces must be compliant with Section 508 of the Rehabilitation Act and 45 CFR part 170, subpart B.
DAP-REQ-ODS-002	The Solution's Operational Data Store (ODS) must apply short-term retention policies (e.g., current state plus three (3) years of history) with automated archival or purging of older data to downstream systems. The Solution’s Operational Data Store (ODS) must implement automated data lifecycle management to retain current operational data and a configurable short-term historical window. Data exceeding the ODS retention period must be automatically archived to downstream analytical or archival systems.
DAP-REQ-ODS-003	The Solution's ODS must preserve transaction-level operational data with minimal redundancy, ensuring data consistency, efficient ingestion, and support for operational reporting.
DAP-REQ-ODS-004	The Solution's ODS must enforce operational reconciliation controls (e.g., record counts, totals, balances) between source systems and the ODS, with automated alerts for discrepancies.
DAP-REQ-ODS-005	The Solution's ODS must implement near real time synchronization mechanisms to update only changed records, ensuring synchronization with source systems without full reloads.
DAP-REQ-ODS-006	The Solution's ODS must include automated entity resolution to reconcile identifiers across disparate source systems.
DAP-REQ-ODS-007	The Solution's ODS must include role-based access controls and audit logging specific to operational data domains, aligned with enterprise security and compliance standards.
DAP-REQ-ODS-009	The Solution's ODS must support time-variant storage with effective dating or snapshots (e.g., current record + recent history of changes) to allow “as-of” reporting.
DAP-REQ-ODS-010	The Solution must provide a subject-oriented, integrated data store that consolidates data from multiple operational systems into consistent domains (e.g., Claims, Eligibility, Encounters, Providers).
DAP-REQ-ODS-011	The Solution must support Low-Latency Ingestion (streaming or micro-batch) and refresh cycles (near real-time where feasible, or sub-hourly for batch) to keep ODS data closely aligned with source systems.
DAP-REQ-ODS-012	The Vendor must work with data owners and stewards as directed by the Department for each source system to understand specific requirements for data elements that need to be brought into ODS and enable a connection to ODS from the module (API or file transfer) to enable their ingestion in ODS.

Table R2. Data Flow Architecture

Requirement #	Requirement Description
DAP-REQ-CONS-003	The Solution must allow users to download filtered datasets in common formats (e.g., CSV, Excel, Parquet) on demand from governed interfaces.
DAP-REQ-CONS-004	The Solution must expose a governed semantic layer of metrics and dimensions for consistent query access.
DAP-REQ-CONS-005	The Solution must expose REST or GraphQL APIs with secure authentication and support for filtering, pagination, and versioning.
DAP-REQ-CONS-006	The Solution must implement usage limits, data egress limits, throttling, or monitoring to safeguard performance and prevent misuse of data extraction features.
DAP-REQ-CONS-007	The Solution must offer certified connectors for BI and ETL tools (e.g., ODBC, JDBC, Power BI, Tableau).
DAP-REQ-CONS-008	The Solution must provide both SQL-based, code-first, and low-code/no code data exploration tools, including notebooks, visualization capabilities, and drag and drop capabilities, without requiring IT intervention.
DAP-REQ-CONS-009	The Solution must provide functionality for users to create and share data snapshots or filtered datasets with expiration controls and access restrictions.
DAP-REQ-CONS-010	The Solution must provide isolated, secure analyst workspaces for data exploration and AI/ML experimentation that prevent unauthorized access or writes to production systems.
DAP-REQ-CONS-011	The Solution must have the ability to provide data access through a Change Data Capture (CDC) mechanism.
DAP-REQ-CONS-012	The Solution must support embeddable BI dashboards or APIs that allow data or insights to be integrated into third-party applications and public-facing websites.
DAP-REQ-CONS-013	The Solution must support scheduling recurring data extracts or reports to approved destinations such as email, object storage, or secure FTP.
DAP-REQ-CONS-014	The Solution must allow users to render any query or report output as a chosen visualization type (e.g., pie, bar, line, heat-map).
DAP-REQ-CONS-016	The Solution must provide functionality to allow users to independently adjust visualization style, scale, colors, and text.
DAP-REQ-CONS-017	The Solution must provide functionality to allow users to independently create view-ready and print-ready reports, charts, graphs, dashboards, and maps.
DAP-REQ-CONS-018	The Solution must provide a governed report-lifecycle service that versions dashboards and automates refresh schedules.
DAP-REQ-CONS-019	The Solution must provide a self-service graphical query designer that exposes table structures and relationships, includes an expression builder and templates, and supports drag-and-drop, sort, copy, and paste actions.
DAP-REQ-CONS-020	The Solution must provide logs usage metrics to track usage of dashboards and reports for user, duration of interaction, and a frequency level.
DAP-REQ-CONS-021	The Solution must support interactive exploration, including drill-down to detail, drill-up to summary, drill-across related tables, and parameter-based filtering.
DAP-REQ-CONS-022	The Solution must provide functionality to view, print or download reports, text, tables, maps, and charts/graphs.
DAP-REQ-CONS-023	The Solution must provide business intelligence and visualization functionalities to manage and evaluate enterprise data and programs with graphical user interface capabilities and an interface for external user access.
DAP-REQ-CONS-024	The Solution must support BI dashboards with full functionality and consistent rendering and performance across modern browsers such as Edge, Chrome, Firefox, and Safari without using additional plug-ins.
DAP-REQ-CUR-002	The Solution must allow users to define and enforce schemas during ingestion and transformation to ensure data consistency.

Requirement #	Requirement Description
DAP-REQ-CUR-003	The Solution must be capable of ingesting and transforming data from a variety of data sources, including relational, document-based, graph, flat files, API endpoints, and third-party cloud Solutions.
DAP-REQ-CUR-004	The Solution must capture and expose basic data lineage and operation metadata for query auditing and impact analysis.
DAP-REQ-CUR-005	The Solution must maintain audit logs of data access, modification, and operational activity.
DAP-REQ-CUR-007	The Solution must provide basic data profiling, including column-level stats, null counts, and value distributions.
DAP-REQ-CUR-008	The Solution must provide independently scalable compute and storage layers to optimize performance and cost.
DAP-REQ-CUR-009	The Solution must provide query optimization techniques including automatic indexing, caching, or pruning strategies.
DAP-REQ-CUR-010	The Solution must support CI/CD workflows for publishing curated datasets with pre-deployment validation.
DAP-REQ-CUR-011	The Solution must support common open data formats (e.g., Parquet, ORC, JSON, XML, and CSV) for interoperability.
DAP-REQ-CUR-012	The Solution must support configurable schema evolution policies, including options to allow, block, or alert on changes.
DAP-REQ-CUR-013	The Solution must support declarative data pipeline definitions (e.g., SQL, YAML, JSON, or similar) syntax.
DAP-REQ-CUR-014	The Solution must support domain-based data ownership and decentralized stewardship using access controls and metadata.
DAP-REQ-CUR-015	The Solution must support multi-cloud data replication and access.
DAP-REQ-CUR-016	The Solution must support time travel or versioned access to data for auditing, rollback, or reproducibility.
DAP-REQ-CUR-017	The Solution must adopt statewide standard data definitions, data semantics, and harmonization strategies.
DAP-REQ-CUR-018	The Solution must provide functionality to link standard data warehouse tables and subject area data marts with imported data tables.
DAP-REQ-CUR-019	The Solution must facilitate data processing including data cleansing, data loading, data brokerage, integration, validation, reconciliation, and synchronization with the data coming from other MES modules.
DAP-REQ-CUR-020	The Solution must allow users with appropriate RBAC read-only access to archived data.
DAP-REQ-DMD-006	The Solution must allow data quality rules to be embedded into data models and transformations.
DAP-REQ-DMD-007	The Solution must include a centralized semantic layer that standardizes metric definitions, business logic, and metadata across the enterprise, accessible across all reporting tools.
DAP-REQ-DMD-008	The Solution must support visual representation of data models to aid business understanding and governance reviews.
DAP-REQ-DMD-009	The Solution must enforce data integrity and referential integrity.
DAP-REQ-DMD-010	The Solution must validate foreign key relationships during data processing.
DAP-REQ-DMD-011	The Vendor must adopt standardized naming conventions and metadata tagging for objects (databases, schemas, tables, columns, views), which are developed during the DDI phase, and ensure these are documented and enforced.
DAP-REQ-DMD-012	The Vendor must align data model design with the layered architecture (bronze → silver → gold → semantic) of the Solution, document business-to-technical data mappings, and validate them with business owners.

Requirement #	Requirement Description
DAP-REQ-DMD-013	The Vendor must apply a standardized data modeling methodology (e.g., 3NF, Data Vault, dimensional/star schema) that is appropriate for the use case as mutually agreed upon with the State.
DAP-REQ-DMD-014	The Solution must use conceptual and logical data models that reflect business definitions and terminology that are mutually agreed upon with the State business stakeholders.
DAP-REQ-DMD-015	The Solution must enforce workload isolation and data distribution patterns in model design to prevent cross-team performance issues.
DAP-REQ-DMD-016	The Vendor must design models to enable row-level, column-level, and object-level security aligned with governance policies.
DAP-REQ-DMD-017	The Vendor must design models to optimize query performance and scalability in the cloud Solution (e.g., data clustering, partitioning strategies, or similar techniques).
DAP-REQ-DMD-018	The Vendor must design models with extensibility in mind, allowing new attributes and entities to be added without major rework.
DAP-REQ-DMD-019	The Vendor must document data models in the enterprise data catalog, including definitions, lineage, relationships, and key business attributes.
DAP-REQ-DMD-020	The Solution must ensure sensitive attributes (PII/PHI) are clearly flagged in metadata management tool and aligned with data classification policies.
DAP-REQ-DMD-021	The Vendor must ensure that business rules and transformation logic are explicitly captured in a metadata management tool and reviewed with data product owners.
DAP-REQ-DMD-022	The Vendor must ensure that data models support enforcement of business rules through derived attributes, validation constraints, and standardized data types.
DAP-REQ-DMD-023	The Vendor must follow a governed change management process for all data model updates, including impact analysis and business sign-off.
DAP-REQ-DMD-024	The Vendor must follow consistent modeling patterns across domains to ensure interoperability of data products and ease of integration.
DAP-REQ-DMD-025	The Vendor must incorporate primary keys, foreign keys, constraints, and referential integrity rules into the logical and physical models where appropriate.
DAP-REQ-DMD-026	The Solution must maintain version history of data models to track evolution, audits, and support rollback if needed.
DAP-REQ-DMD-027	The semantic layer must support multi-grain modeling, allowing both aggregated and detailed-level reporting from curated datasets while preserving query performance.
DAP-REQ-DMD-028	During DDI, The Vendor must align with the state on a data organizational structure across Cloud Data Lake Storage and the Data Warehouse to enable Addressability (by assigning each dataset/table a permanent, unique, and standardized address). This ensures consistent, automated access for downstream users across the data platform.
DAP-REQ-DPR-002	The Solution must establish enterprise data interoperability by ensuring that all data products: • Use standardized metadata and data types, • Can be easily combined or integrated with other data products, • Follow common schemas and formats to support seamless data exchange across domains and systems.
DAP-REQ-DPR-004	The Solution must adhere to an approved data products' service-level objectives such as: Interval of change and timeliness, general availability and performance, freshness, completeness & quality, lineage, stewardship.
DAP-REQ-DPR-005	The Solution must allow archiving or retiring of unused data products.
DAP-REQ-DPR-006	The Solution must allow assignment of product owners with clear accountability.
DAP-REQ-DPR-007	The Solution must enable data access via SQL, APIs endpoints, or other standard interfaces.
DAP-REQ-DPR-008	The Solution must enable domain teams to manage data products independently.

Requirement #	Requirement Description
DAP-REQ-DPR-009	The Solution must ensure all data products adhere to the established data contracts and any deviation is automatically captured in error tables with the ability to reprocess the data once the error is fixed.
DAP-REQ-DPR-010	The Solution must ensure all the data contracts are version controlled and go through the multi-level approval process including stakeholders from source systems producing the data and downstream system consuming the data.
DAP-REQ-DPR-011	The Solution must ensure all the data products are scheduled to be refreshed at predefined frequency which ranging from real time, every few mins or hour, intraday, daily, weekly, monthly, quarterly, or annually.
DAP-REQ-DPR-012	The Solution must ensure all the data products have the ability to be scheduled with proper dependencies in place.
DAP-REQ-DPR-013	The Solution must support modular design, enabling data products, pipelines, and analytics components that can be re-used, and assembled into new products without re-engineering, while aligning to shared business metadata.
DAP-REQ-DPR-014	The Solution must establish a reusable automated framework to onboard data products into the Solution.
DAP-REQ-DPR-015	The Solution must include dashboards for data products usage analytics, utilization metrics, data refresh frequency, audit function such as access, last used by, owner, performance, and error tracking.
DAP-REQ-DPR-016	The Solution must provide tools for data product creation and deployment.
DAP-REQ-DPR-017	The Solution must register all data products in a centralized catalog where it is possible to search and explore. Needs to include the following: domain, ownership, lineage including source to target mapping, quality metrics, business glossary, and technical glossary.
DAP-REQ-DPR-018	The Solution must support CI/CD pipelines for data workflows.
DAP-REQ-DPR-019	The Solution must support versioning and change tracking of data products.
DAP-REQ-DPR-020	The Vendor must lead the discovery efforts and requirements gathering with the State to define the purpose and target consumers of each data product.
DAP-REQ-DPR-021	The Vendor must communicate deprecation plans and timelines for the data products developed by the Vendor.
DAP-REQ-DPR-022	The Vendor must offer training for data products covering the topics below: • Role-based onboarding: Tailored for analysts, engineers, business users, etc. • Live or recorded sessions: Covering how to use the self-service tools. • Hands-on labs or demos: Practice using data products in real scenarios. • Q&A or support channels: For ongoing learning and troubleshooting.
DAP-REQ-DPR-023	The Vendor must use consistent data formats and schemas in defining and maintaining data products.
DAP-REQ-DPR-024	Then Vendor must establish processes and frameworks to triage and escalate if there are problems with data or access.
DAP-REQ-DPR-025	The Vendor must develop, implement, test, and deploy Data Products to production.
DAP-REQ-INTG-002	The Solution must allow authorized NCDHHS users to perform ad-hoc data loads in non-production environments under mutually agreed standards and procedures.
DAP-REQ-INTG-006	The Solution must ensure all incoming data adheres to the established interface contracts and report errors as per the established error tracking mechanisms.
DAP-REQ-INTG-007	The Solution must identify incoming data records that have previously been processed and not process them downstream to avoid creating duplicates.
DAP-REQ-INTG-008	The Solution must support low code/ no code data ETL/ELT capability to be leveraged by Data Scientists, Analysts and Business Data users.
DAP-REQ-INTG-009	The Solution must support integration through API, file ingestion, CDC ingestion from source systems, streaming, batch, and micro batch.

Requirement #	Requirement Description
DAP-REQ-INTG-010	The Solution must accept, transform, and load both structured, semi-structured, and unstructured data formats.
DAP-REQ-INTG-011	The Solution must employ an automated cloud hosted ETL tool capable of mapping and loading high-volume data feeds.
DAP-REQ-INTG-012	The Solution must include audit controls that reconcile source-to-target record counts and flag data-quality exceptions.
DAP-REQ-INTG-013	The Solution must integrate data from all NCDHHS-approved sources, supporting the refresh frequency (business driven) specified by each source.
DAP-REQ-INTG-015	The Vendor must establish data interface contracts with the source system owners covering data types, SLA agreements, timeliness, refresh frequency and keys, along with business glossary.
DAP-REQ-INTG-017	The Vendor must provide the State with an automated daily dashboard showing records received, successfully loaded, and rejected (with error codes) for every source feed.
DAP-REQ-INTG-019	The Solution must include an integration pattern for AWS S3 to read from and write to the AWS S3.
MES-REQ-INT-001	The Solution must interface through the Medicaid Integration Services using APIs for real-time and secure file transfer for batch data exchanges.
MES-REQ-INT-002	The Solution must integrate with other MES modules as needed utilizing the Medicaid Integration Services (MIS) via batch or real-time data exchanges.
MES-REQ-INT-003	The Solution must send and receive real-time discrete transactions between modules and other entities designated by the Department through the State's Medicaid Integration Services (MIS) integration Solution, where necessary, using the provided standards and protocols to reduce the need for bulk data transfers and duplicate communications. Direct data entry into the Vendor's web Solution is exempt.
MES-REQ-INT-004	The Vendor must identify and provide all tools and software intended to maintain interfaces, environments, and data models as a component of its Information Systems Development Methodology (ISDM).
MES-REQ-INT-006	The Solution must provide the functionality to access raw daily interface files for up to sixty (60) calendar days. Archive raw daily interface files after sixty (60) calendar days and maintain for up to six (6) months.
MES-REQ-INT-007	The Solution must provide the ability to access raw weekly, monthly, and quarterly interface files for up to one year (365 calendar days). Archive raw monthly and quarterly interface files for two years (730 calendar days) and maintain for up to two (2) years.

Table R3. Migration

Requirement #	Requirement Description
DAP-REQ-MIGR-002	The Vendor must participate in ongoing data governance meetings and processes as required by the Department.
DAP-REQ-MIGR-004	The Vendor must validate all converted reports by comparing outputs and logic against legacy reports, documenting, and resolving discrepancies.
DAP-REQ-MIGR-006	The Vendor must account for current encryption and decryption mechanisms and ensure all migrated data supports encryption at rest, encryption in transit, and authorized decryption mechanisms based on defined encryption standards.
DAP-REQ-MIGR-007	The Vendor must document and map lineage from legacy reports/scripts to equivalent objects in the new environment.
DAP-REQ-MIGR-008	The Vendor must migrate the current Data Quality Script, ensuring no existing functionality is lost, and to expand it to address data needs in the cloud platform.
DAP-REQ-MIGR-009	The Vendor must obtain business approval of all existing BIAO reports migrated from the current analytics system to the Solution before the current system can be decommissioned. See Attachment AA: Reports for all affected reports.

Requirement #	Requirement Description
DAP-REQ-MIGR-010	The Solution must generate a Data Quality excel summary file for each file with submission made by a plan coming from PCDU that contains errors and write this back to PCDU in real time.
DAP-REQ-MIGR-011	The Vendor must ensure existing keys, such as Oracle incrementing columns (e.g., Sequence, identity keys), are migrated to the solution with uniqueness maintained and sequence continuity preserved across historical and incremental loads.
DAP-REQ-MIGR-012	The Vendor must replicate existing security and row/column-level filters from legacy reports in the Solution and support a review and update of these controls to align with current security and business requirements.
DAP-REQ-MIGR-013	The Solution must generate in real time a JSON file with each submission file received from PCDU, that contains an acknowledgement of the receipt by the Solution, and includes criticality of any errors, as well as additional integration metadata that should be sent back to PCDU in real time. The Bidder's Library contains a sample.
DAP-REQ-MIGR-014	The Vendor must ensure the new Data Quality framework is integrated with current PCDU as defined in the Bidder's Library.
DAP-REQ-MIGR-015	The Vendor must optimize data models, queries, and dashboards for the Solution instead of using legacy models.
DAP-REQ-MIGR-016	The Vendor must perform a full production data migration prior to cutover.
DAP-REQ-MIGR-017	The Solution must provide the capability to preserve historical report outputs for audit and compliance continuity.
DAP-REQ-MIGR-018	The Vendor must provide a design document detailing the migration technical design (e.g. encryption, data model mapping, entity relationships, security controls), migration processes, assumptions, and mappings for auditability and future reference, which would incorporate input and insights from the State.
DAP-REQ-MIGR-019	The Vendor must provide functional equivalence documentation showing how legacy features map to new Solution features.
DAP-REQ-MIGR-020	The Vendor must update metadata/catalogs to reflect migrated data assets, lineage, and usage.
DAP-REQ-MIGR-021	The Vendor must use standard template and formatting, as mutually agreed upon with the State, in the report/dashboard migration.
DAP-REQ-MIGR-022	The Vendor must convert all historical data from the State's current analytics system that is required to support reporting, analytics, and regulatory needs.
DAP-REQ-MIGR-023	The Vendor must provide designated Department staff access to an environment to provide support or validate converted data.
DAP-REQ-MIGR-024	The Vendor must adhere to state-provided BI dashboard style guide and theme during report migration, to ensure consistent look and feel for all migrated reports.
DAP-REQ-MIGR-025	The Vendor must integrate the Solution with the PHP Contractual Data Utility (PCDU).
DAP-REQ-MIGR-026	The Vendor must migrate, develop, or rewrite all migration assets, ETL processes, scripts, views and reports listed in the inventory tables found in Section 3.1.4 Assets Migration and Validation.
DAP-REQ-MIGR-027	The Vendor must create a complete backup of all historical data migrated from the legacy system into the Solution before any transformations are applied. This backup must reflect the data exactly as received and must be stored in secure object storage in a read-only state.

Table R4. Workflow Management and Performance

Requirement #	Requirement Description
DAP-REQ-DEV-004	The Solution must log version history and access activity for all code, pipeline, and model artifacts.
DAP-REQ-DEV-005	The Solution must support automated dependency management for code and model environments (e.g., Conda, pip, requirements.txt, environment.yml).

Requirement #	Requirement Description
DAP-REQ-DEV-006	The Solution must support the integration of automated testing framework for data pipelines and ML workflows, into the DevOps pipeline for unit, integration, regression, and expectation-based tests.
DAP-REQ-DEV-008	The Solution must support gated approval workflows for high-risk operations (e.g., promotion to production, schema changes, security policy updates).
DAP-REQ-DEV-009	The Solution must support Git-based agentic code reviews that automatically validate coding standards, enforce documentation/commenting, and flag issues.
DAP-REQ-DEV-010	The Solution must support Infrastructure-as-Code (IaC) using tools such as Terraform, Pulumi, and similar or native cloud templates (e.g., ARM, Bicep) to define, deploy, and manage compute, storage, networking, and access configurations.
DAP-REQ-DEV-011	The Solution must support integration of ML models into CI/CD workflows, including validation, staging, rollback, and monitored deployment to inference endpoints.
DAP-REQ-DEV-012	The Solution must support isolated, role-scoped environments for development, testing, and production workloads to avoid cross-contamination of data and compute resources, with defined promotion workflows.
DAP-REQ-DEV-013	The Solution must support modular pipeline development, allowing users to package reusable transformation or modeling components.
DAP-REQ-DEV-014	The Solution must support parameterized and templated definitions for code, pipelines, and infrastructure to enable environment-specific configurations and reuse.
DAP-REQ-DEV-015	The Solution must support rollback or undo capabilities for deployed pipelines, models, and infrastructure configurations.
DAP-REQ-DEV-016	The Solution must use a Git-based tool for version control for all code artifacts—including notebooks, pipelines, configuration files, and infrastructure definitions, leveraging branching strategies agreed on with the state during DDI phase.
DAP-REQ-DEV-017	The Solution must adhere to a standard schedule-based keys and certificate rotation in all environments, and it must alert two weeks ahead of scheduled expirations to avoid break in operations.
DAP-REQ-ORC-001	The Solution must allow workflow versioning, controlled promotion across environments and integration with CI/CD pipelines.
DAP-REQ-ORC-002	The Solution must expose APIs and UI to trigger, pause, resume, or cancel data pipelines manually or programmatically.
DAP-REQ-ORC-003	The Solution must integrate with enterprise alerting systems (e.g. Teams, ServiceNow, Outlook) for pipeline success/failure notifications.
DAP-REQ-ORC-004	The Solution must log job execution metadata including start time, duration, status, errors, and retry attempts.
DAP-REQ-ORC-005	The Solution must support event-driven pipeline execution triggered by external systems, file drops, or API calls.
DAP-REQ-ORC-006	The Solution must support orchestrating data workflows including ingestion, transformation, validation, and publishing using native or integrated tools, and enforce dependencies so each system receives prerequisite data before execution.
DAP-REQ-ORC-007	The Solution must support parameterized workflows that allow dynamic input values (e.g., run date, environment).
DAP-REQ-ORC-008	The Solution must support scheduling and orchestration across the layers, up to and including in the BI solution.
DAP-REQ-ORC-009	The Solution must support task scheduling, chaining of dependent steps, failed job alerting, and retries for failed jobs.
DAP-REQ-SP-004	The Solution must expose Solution-level SLAs (e.g., query latency guarantees) and provide health dashboards for monitoring system and job performance.
DAP-REQ-SP-005	The Solution must include built-in query optimization techniques such as predicate pushdown, partition pruning, query caching, and cost-based optimization.

Requirement #	Requirement Description
DAP-REQ-SP-006	The Solution must provide query explain plans or visual execution graphs for understanding query performance and diagnosing bottlenecks.
DAP-REQ-SP-007	The Solution must support adaptive compression and encoding strategies that automatically optimize storage formats based on data patterns.
DAP-REQ-SP-008	The Solution must support automatic suspension of idle compute resources and automatic resume on-demand.
DAP-REQ-SP-009	The Solution must support data file optimization features such as compaction, clustering, z-ordering, small-file merging, or coalescing operations to optimize storage layout and performance.
DAP-REQ-SP-010	The Solution must support elastic compute scaling, including auto-scaling clusters or serverless execution, to dynamically adjust resources based on workload demand.
DAP-REQ-SP-011	The Solution must support micro-batch ingestion via file arrival detection, directory polling, or scheduled triggers.
DAP-REQ-SP-012	The Solution must allow multiple users or workloads to run queries and jobs simultaneously without performance degradation.
DAP-REQ-SP-013	The Solution must support incremental processing techniques that allow pipelines and transformations to run only on changed data.
DAP-REQ-SP-014	The Solution must support job scheduling, resource throttling, and execution windows.
DAP-REQ-SP-015	The Solution must support materialized views, result caching, or acceleration layers to improve performance for repeated or dashboard-driven queries.
DAP-REQ-SP-016	The Solution must support parallel reading and writing of data during ingestion, transformation, and query execution.
DAP-REQ-SP-017	The Solution must support partitioning of datasets by common keys (e.g., date, region) and leverage this structure for faster query execution.
DAP-REQ-SP-018	The Solution must support serverless execution or multi-cluster options to accommodate variable workloads without pre-provisioning.
DAP-REQ-SP-019	The Solution must support storage tiering or lifecycle policies that automatically move older data to lower-cost storage classes.
DAP-REQ-SP-020	The Solution must support workload tagging and policy enforcement for job duration, size, or user limits.

Table R5. Data Governance and Management

Requirement #	Requirement Description
DAP-REQ-DG-002	The Solution must enforce configurable data quality rules (e.g., completeness, uniqueness, validity, timeliness), with automated exception reporting.
DAP-REQ-DG-003	The Solution must enforce consistent use of reference data within the Solution and must align to reference data from upstream modules when they are the system of record (e.g., billing codes, diagnostic codes).
DAP-REQ-DG-004	The Solution must include a searchable data catalog with data descriptions, and business glossaries, canonical business definitions and calculation logic for metrics that are published as Single Version of Truth, and which tracks the metadata for all data elements in the Solution, enabling users to find data quickly using keyword searches, metadata attributes, or specific filters such as date ranges, data sources, or ownership.
DAP-REQ-DG-005	The Solution must identify and manage Critical Data Elements (CDEs) across all data domains, enforce standardized definitions and formats, and any changes to CDE definitions must follow a documented governance workflow with impact analysis, version controlling, and State approval.
DAP-REQ-DG-008	The Solution must support automated data discovery that populates the data catalog upon new dataset curation and integration.
DAP-REQ-DG-009	The Solution must support automated remediation workflows (e.g., quarantine, reject, or flag records) when CDEs fail quality checks.

Requirement #	Requirement Description
DAP-REQ-DG-010	The Solution must define and maintain a governed inventory of Critical Data Elements (CDEs), including business definition, data lineage, ownership, and applicable data quality rules.
DAP-REQ-DG-011	The Solution must expose only the certified Single Version of Truth datasets to downstream applications and analytics unless an exception is approved.
DAP-REQ-DG-012	The Solution must establish a governed reference data repository (e.g., code sets, lookup values, master lists) that is accessible and authoritative.
DAP-REQ-DG-013	The Vendor must align with data classification standards, provided by State team, to ensure that appropriate controls are applied to each category of data before it is accessed or used.
DAP-REQ-DG-016	The Solution must provide functionality to apply effective dates to maintain previous versions, to track changes and to append any changes made to the Data Catalog.
DAP-REQ-DG-018	The Vendor must obtain NCDHHS approval of all data model designs and model changes.
DAP-REQ-DG-019	The Solution must provide the functionality to insert user-defined metadata attributes into the data catalog.
DAP-REQ-DG-020	The Vendor must create and maintain a business data glossary by working with the business to collect data glossary elements such as a standard data element name, a narrative business definition of the data element, Synonyms / Aliases, Domain, related terms, tags, sensitivity, data quality expectations, associated data assets, business rules/policies, and last reviewed date.
DAP-REQ-DG-023	The Solution must provide native connectors and APIs for the data catalog to integrate with databases, data warehouses, ETL tools, BI platforms (Power BI, Tableau), cloud services (Azure, AWS, Google Cloud), and other data catalogs to automate metadata ingestion and keep the catalog up to date.
DAP-REQ-DG-024	The Solution data catalog must provide granular control over who can view, modify, or manage specific datasets within the catalog based on user roles, ensuring that sensitive data is protected.
DAP-REQ-DG-025	The Solution must provide insights into how data is being used across the Solution, including which data is most frequently accessed and by whom.
DAP-REQ-DG-026	The Solution data catalog must support a wide variety of data sources including structured, semi-structured, and unstructured data.
DAP-REQ-DG-027	The Solution data catalog must handle thousands of unique data assets and metadata as organization data grows, ensuring performance and usability are maintained as more data is cataloged.
DAP-REQ-DG-035	The Solution data catalog must integrate with data governance workflows, data pipelines, and analytics tools to ensure that data governance processes are embedded in daily operations.
DAP-REQ-DG-036	The Solution data catalog must facilitate workflows for users to request access to restricted datasets, with approvals managed through data owners or stewards.
DAP-REQ-DG-038	The Solution data catalog must generate reports on the status of data assets, such as their quality, ownership, lineage, and usage trends.
DAP-REQ-DG-041	The Solution data catalog must provide the capability to adjust configurations to meet the organization’s specific data management and governance requirements.
DAP-REQ-DG-044	The Solution data profiling capability must automatically scan data sets to provide insights into their structure, quality, and content, identifying patterns, duplicates, anomalies, and missing data.
DAP-REQ-DG-045	The Solution data profiling capability must provide automated tools to clean, standardize, and enrich data by correcting or removing inaccurate entries, filling missing data, and ensuring consistency across data sets.
DAP-REQ-DG-046	The Solution data profiling capability must offer advanced matching algorithms to identify and tag duplicates across different sources, improving the accuracy of data records.
DAP-REQ-DG-047	The Solution data profiling capability must implement rules for validating data based on pre-set or custom conditions to ensure data meets specific quality criteria.
DAP-REQ-DG-048	The Solution data profiling capability must help manage and integrate master data across various systems, maintaining a single source of truth for key entities.

Requirement #	Requirement Description
DAP-REQ-DG-049	The Solution data profiling capability must provide a unified platform that supports data stewardship, allowing for the implementation of governance policies, workflows, and access controls.
DAP-REQ-DG-050	The Solution data profiling capability must provide shared dashboards, workflows, and reporting to enable collaborative work for data stewards, analysts, and business users.
DAP-REQ-DG-051	The Solution data profiling capability must manage metadata for better data understanding, lineage tracking, and to maintain data consistency across the Solution.
DAP-REQ-DG-052	The Solution data profiling capability must continuously track and monitor data quality metrics, offering real-time alerts and customizable reports for stakeholders to monitor data health over time.
DAP-REQ-DG-053	The Solution data profiling capability must integrate with various databases, cloud platforms, and enterprise systems, offering scalability for datasets and environments.
DAP-REQ-DG-054	The Solution must provide automated, policy-driven data lifecycle management across the platform. Lifecycle management must apply to all platform layers, including the Operational Data Store (ODS), Data Lake / Analytical Storage, Data Warehouse / Curated Analytics, metadata, logs, and derived datasets while preserving data integrity, metadata, and lineage.
DAP-REQ-DQ-003	The Vendor must define strategies and provide Solution functionality for imputing or handling missing data.
DAP-REQ-DQ-004	The Solution must enforce schema validation during data ingestion.
DAP-REQ-DQ-005	The Solution must provide automation for detecting and resolving data quality issues and anomalies starting with integration and throughout the entire platform.
DAP-REQ-DQ-006	The Solution must establish a daily reconciliation summary reporting between the source systems and the Solution on record counts and specified data attributes (e.g. claim count, dollar amounts).
DAP-REQ-DQ-007	The Solution must implement automated validation checks based on defined field business rules, during ingestion and transformation.
DAP-REQ-DQ-008	The Solution must enforce standardized, authoritative reference data so that the same codes, values, and definitions are used consistently across all systems, data products, analytics, and reporting.
DAP-REQ-DQ-009	The Solution must monitor and report on a defined set of basic data quality rules, as agreed on with data owners/ data stewards, and apply those to all relevant datasets doing ETL/ELT.
DAP-REQ-DQ-010	The Solution must monitor data delivery schedules and send alerts for any delays.
DAP-REQ-DQ-011	The Solution must monitor for duplicate records and anomalies and implement deduplication logic in ETL/ELT pipelines in alignment with business requirements.
DAP-REQ-DQ-012	The Solution must provide DQ email alert notifications that are triggered when a data quality issue is detected within a dataset or system. These alerts can be configured to notify relevant stakeholders such as data engineers, data analysts, data scientists, or business users.
DAP-REQ-DQ-013	The Solution must standardize data formats and units across systems.
DAP-REQ-DQ-014	The Vendor must assist users with their execution of data quality rules and/or data quality reports as requested.
DAP-REQ-DQ-015	The Vendor must work with the Department to develop a consistent method of addressing data quality issues in the source systems when the issues originate in the source system.
DAP-REQ-DQ-017	The Vendor must work with State business stakeholders to define business rules for validating data quality.
DAP-REQ-DQ-018	The Vendor must work with State business stakeholders to identify critical data elements, define and enforce Completeness Rules.
DAP-REQ-DS-001	The Solution must provide standards-based (e.g., HL7 FHIR, X12, REST/JSON) APIs and messaging interfaces to access data.
DAP-REQ-DS-002	The Solution must monitor and track the cost for external data shares.

Requirement #	Requirement Description
DAP-REQ-DS-005	The Solution must allow authorized users to create row- and column-level filtered dataset shares, enforced by role-based access controls, data masking policies, and data classification rules.
DAP-REQ-DS-006	The Solution must provide functionality to create immutable, point-in-time snapshots of datasets that can be shared or referenced to ensure auditability and reproducibility.
DAP-REQ-DS-007	The Solution must enforce authentication, authorization, and row-/column-level security for all API-driven access.
DAP-REQ-DS-008	The Solution must ensure that data masking, redaction, or anonymization rules applied to shared datasets cannot be bypassed or reversed by end users.
DAP-REQ-DS-009	The Solution must include a data catalog or marketplace where users can discover, request access to, and subscribe to shared datasets, along with associated metadata, lineage, business glossary terms, and custom defined metadata fields.
DAP-REQ-DS-010	The Solution must log and monitor all usage, access patterns, and data egress volumes for each shared dataset, and support alerting for anomalous activity.
DAP-REQ-DS-011	The Solution must provide a governed process for requesting large or exceptional data extracts, including temporary workspaces or analyst workspaces.
DAP-REQ-DS-012	The Solution must provide consumption monitoring on the shared data sets (e.g., API usage, query logs) to track who is accessing which datasets and when.
DAP-REQ-DS-013	The Solution must provide fine-grained audit logs capturing who accessed, modified, or reshared shared datasets—including timestamp, IP address, and method of access.
DAP-REQ-DS-014	The Solution must provide programmatic APIs for data consumers to subscribe or unsubscribe to data that has been shared and supports instant revocation for all subscribed consumers.
DAP-REQ-DS-015	The Solution must provide secure, governed APIs and governed query endpoints for exposing data products, CDEs, and reference data to authorized consumers.
DAP-REQ-DS-016	The Solution must restrict data sharing to authenticated and authorized users or systems, and enforce access through secure mechanisms such as signed URLs, Scoped API tokens, or federated identities.
DAP-REQ-DS-017	The Solution must support event-driven and streaming data sharing mechanisms (e.g., publish/subscribe, CDC), allowing consumers to subscribe to and receive updates in real time.
DAP-REQ-DS-018	The Solution must support publishing datasets so the data as well as documented schema, service-level expectations, ownership metadata, and change notification policies are accessible via APIs.
DAP-REQ-DS-019	The Solution must support secure, scoped service accounts or access tokens for machine-to-machine sharing or system-level data access, with automatic time-bound credential rotation and permission boundaries.
DAP-REQ-DS-020	The Solution must support Zero Copy Data Sharing through modern protocols —across internal teams and external partners without duplicating or moving data.
DAP-REQ-DS-021	The Solution must expose bulk data-export APIs to support downstream consumption.
DAP-REQ-DS-022	The Solution must provide the ability to import/export data in generally accepted formats such as .csv and .txt.
DAP-REQ-DS-023	The Solution must provide inbound and outbound interface raw data files when requested by the State on a mutually agreed timeline.
DAP-REQ-MMM-001	The Solution must have the configuration ability to run the data monitoring checks at certain frequency and producing output report.
DAP-REQ-MMM-003	The Solution must log all deployment events, test results, and runtime errors in a centralized location, with support for integration into observability Solutions (e.g., Datadog, Prometheus, Grafana).
DAP-REQ-MMM-005	The Solution must allow tagging/classification of sensitive data (e.g., PII, PHI) and enforce policies for access and usage monitoring.
DAP-REQ-MMM-006	The Solution must automatically capture technical metadata (schemas, tables, columns, data types, lineage, query history) across ingestion, transformation, and consumption layers.

Requirement #	Requirement Description
DAP-REQ-MMM-008	The Solution must log all metadata changes (e.g., schema updates, definition changes, lineage updates) in an auditable format for 24 months.
DAP-REQ-MMM-009	The Solution must log and visualize privilege escalations, failed login attempts, and cross-region data sharing.
DAP-REQ-MMM-010	The Solution must monitor pipeline executions, scheduling, and system-specific SLAs, showing success/failure rates and execution times.
DAP-REQ-MMM-011	The Solution must monitor system availability, errors, latency, and API call health across Data Warehouse and Cloud platform services.
DAP-REQ-MMM-012	The Solution must provide APIs for extracting and publishing metadata into enterprise governance and analytics tools (e.g., Collibra, Alation, Purview, Power BI or similar).
DAP-REQ-MMM-013	The Solution must provide dashboards for monitoring compute, storage, and data transfer usage across accounts, warehouses, and workloads.
DAP-REQ-MMM-014	The Solution must provide monitoring of pipeline executions, data freshness, schema changes, and data quality rule adherence.
DAP-REQ-MMM-015	The Solution must support anomaly detection in data flows (e.g., unexpected volume spikes, schema drift, failed transformations).
DAP-REQ-MMM-016	The Solution must support budget thresholds, anomaly detection, and alerts (e.g., runaway queries, unexpected egress).
DAP-REQ-MMM-017	The Solution must support monitoring of sensitive data access (PII/PHI) with alerts for unauthorized or unusual queries.
DAP-REQ-MMM-018	The Solution must ensure metadata supports compliance with regulations (e.g., HIPAA) through traceability and retention policies.
DAP-REQ-MMM-019	The Solution must provide monitoring dashboards to highlight long-running or resource-intensive queries that require tuning.
DAP-REQ-MMM-020	The Solution must provide monitoring dashboards to provide visibility into key operational KPIs (pipeline schedule adherence, data latency, quality scores).
DAP-REQ-MMM-021	The Solution must provide monitoring to highlight stuck, delayed, or failing jobs with recommended remediation steps.
DAP-REQ-MMM-023	The Solution must ensure that business metadata (definitions, business rules, ownership, CDE flags) is linked to technical metadata in the enterprise catalog.
DAP-REQ-MMM-024	The Solution must provide workflows for metadata curation, review, and approval by data stewards and owners.
DAP-REQ-MMM-025	The Solution must provide dashboards for incident tracking and SLA compliance reporting.
DAP-REQ-MMM-026	The Solution must provide functionality to monitor database performance to include the status of an active search or query and identify the initiating user.
DAP-REQ-MMM-027	The Solution must provide the functionality to notify pre-selected addressees (e.g., email attachment, Web message board, etc.) that queries, or reports are available for review.
DAP-REQ-MMM-028	The Solution must provide continuous monitoring through the selected enterprise observability tool. Outages in this observability tool must be treated as a P2-High Priority issue.
DAP-REQ-MMM-029	The Solution must include capabilities that continually monitor system utilization for resource contentions, high traffic volumes, and slowed response times.
MES-REQ-DATA-002	The Solution must have a means to deal with data received from other sources that fall outside of the validations: to reject a file or record based on business rule validations, or accept the data but report an error, or a combination of these means as approved by the Department.
MES-REQ-DATA-012	The Solution must maintain its own reference data. This includes ongoing management, validation, and updating reference data within the Solution.
MES-REQ-DATA-013	The Solution must consume the reference data from the State designated systems of record and enforce its consistent use across all business domains.

Requirement #	Requirement Description
MES-REQ-DATA-014	The Solution must not maintain independent or conflicting versions of the State designated system reference data and must remain aligned with the systems of record.
MES-REQ-DATA-015	The Solution must provide all its reference data to other State systems via the Medicaid Integration Services (MIS).

Table R6. Operations

Requirement #	Requirement Description
DAP-REQ-MS-009	Vendor must proactively make adjustments to ensure connectivity and database availability.
DAP-REQ-MS-013	The Vendor must follow agreed upon Release Management processes to submit and schedule all releases.
DAP-REQ-MS-014	The Vendor must follow standardized development practices, including version control, peer reviews, automated testing, adherence to agreed programming standards, and CI/CD for all pipeline deployments.
DAP-REQ-MS-016	The Vendor must maintain adequate operations staff to action service requests and perform operational functions.
DAP-REQ-MS-017	The Vendor must meet with the State monthly to review Solution performance and other relevant issues (e.g., planned changes, work in progress, SLAs performance metrics).
DAP-REQ-MS-018	The Vendor must notify the State within twenty-four (24) hours of any changes to the regularly agreed upon scheduled maintenance and loads.
DAP-REQ-MS-020	The Vendor must perform capacity and performance management, including forecasting storage/compute needs, scaling resources as volumes grow, and addressing performance bottlenecks.
DAP-REQ-MS-022	The Vendor must proactively monitor and maintain Solution health, including infrastructure checks, cost optimization, and performance tuning.
DAP-REQ-MS-023	The Vendor must proactively optimize and monitor data warehouse performance and notify State team of any issues and coordinate with them to remediate.
DAP-REQ-MS-024	The Vendor must propose continuous improvement initiatives (e.g., new Solution features, performance optimizations, automation opportunities) and present them quarterly to the State.
DAP-REQ-MS-028	The Vendor must provide an impact analysis of escalated problems and issues and must provide resulting analysis to the State.
DAP-REQ-MS-029	The Vendor must maintain and optimize existing pipelines and resolve failures.
DAP-REQ-MS-031	The Vendor must provide DAP performance metrics via BI Dashboards, Scorecards, and report cards in Excel.
DAP-REQ-MS-032	The Vendor must provide functionality to develop and maintain benchmark techniques for monitoring system performance.
DAP-REQ-MS-033	The Solution must provide functionality to track and report performance and response times on user queries.
DAP-REQ-MS-034	The Vendor must provide ongoing operations and maintenance (O&M) services for the entire cloud data Solution, including Cloud, Data Warehouse, and any other components of the Solution.
DAP-REQ-MS-036	The Vendor must provide Solution maintenance including service changes, system upgrades, correction of deficiencies, performance enhancements, script changes, system parameters, configuration changes, patching, upgrades, and version updates as released by the Solution vendors (Azure, AWS, Google, Databricks, Snowflake, etc.), with appropriate testing, change management, review and approval from the State prior to deployment to production.
DAP-REQ-MS-037	The Vendor must provide its staff the training in NCDHHS programs and data to support the Solution.
DAP-REQ-MS-041	The Vendor must track and document user-reported defects or problems, from identification through corrective action, including all testing performed to ensure the defect is resolved.

Requirement #	Requirement Description
DAP-REQ-MS-043	The Vendor must support NCDHHS in explaining and defending data results to external and internal NCDHHS Stakeholders, auditors, or other parties, as requested by NCDHHS.
DAP-REQ-MS-044	The Vendor must work directly with business users and analysts to define requirements for new pipelines, deploy them to production, and provide troubleshooting support for existing jobs.
DAP-REQ-MS-047	Vendor must partition and optimize all migrated datasets as needed using native cloud warehouse features (e.g., micro-partitioning design, clustering keys, compression, search optimization service, materialized views and similar) to ensure performance, scalability, and cost efficiency for analytics workloads.
MES-REQ-OM-001	The Vendor must perform operations and maintenance on all system environments (i.e. production and pre-production environments), following change control, defect management, configuration management, release management, and testing processes that are approved by the Department.
MES-REQ-OM-002	The Vendor must provide comprehensive 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 operations requirements.
MES-REQ-OM-003	The Vendor must obtain approval by the Department prior to scheduling non-emergency system downtime/maintenance.
MES-REQ-OM-004	The Vendor must request any planned Downtime due to scheduled upgrades or Maintenance, outside the normal Maintenance Window, to the Department 5 Business Days prior to Downtime. Unless the Department consents, it does not qualify as approved Downtime.
MES-REQ-OM-005	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 on how the changes or upgrades will impact the operation and functionality of the Solution and provide the documented testing results.
MES-REQ-OM-006	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 configuration changes.
MES-REQ-OM-007	The Vendor must include documentation of Solution components and procedures such that the Solution could be operated by a variety of contractors or other users.
MES-REQ-OM-008	Vendor must maintain Solution documentation to include configuration, system design, enterprise architecture, user manual, operations procedures manual, training manual, and data dictionary within 10 business days of an implementation change to the Solution.
MES-REQ-OM-011	The Vendor must utilize and report into the IT Incident Management tool that is designated by the Department to track all Incidents and Problems.
MES-REQ-OM-012	The Vendor must resolve all service defects and service disruptions. Defects are not considered resolved until approved by the State.
MES-REQ-OM-013	The Vendor must collect, prioritize, manage, and report on all defects and must include defect aging information to track how long defects are taking to resolve throughout the Software Development Lifecycle.
MES-REQ-OM-014	The Vendor must provide a report for all Critical and High-Level incidents, as defined in RFP Section 3.3.3 Vulnerability Risk Ratings and Remediation, on a monthly basis for the previous month and must provide a Root Cause Analysis for each of the Critical and High-Level incidents.
MES-REQ-OM-017	Vendor must ensure maintenance of licenses and appropriate permitted usage with all licensing agreements, including software licensing, to support the proposed Solution and services.

Table R7. Project Management

Requirement #	Requirement Description
DAP-REQ-PM-001	The Vendor must ensure that no functionality, configuration, or code of the Solution is moved into production without prior review and formal approval by the State or its designated authority.

Requirement #	Requirement Description
DAP-REQ-PM-002	The Vendor must support joint prioritization, scheduling, and approval of all sprint and release plans of the Solution as part of a common backlog and roadmap managed with the State.
DAP-REQ-PM-003	The Vendor must implement standard DevSecOps controls for all production deployments of the Solution, including peer reviews, automated testing, change tickets, deployment approvals, and rollback procedures.
DAP-REQ-PM-004	The Vendor must maintain traceability from sprint backlog items through testing and deployment and provide the State with advanced visibility into upcoming releases prior to production implementation.
MES-REQ-OM-009	The Vendor must comply with the Departments reporting and resolution timelines for standard production incident and problem turnaround times.
MES-REQ-OM-010	Vendor must provide initial recommended production issue severity and incident priority levels that address both the business impact and business urgency. Production issues will be categorized based on the Department's urgency, severity, and priority definitions. The Department reserves the right to elevate the Vendor's recommendations.
MES-REQ-PM-001	The Vendor must participate in key project/program milestones such as: SIT, User Acceptance Testing (UAT) Sign-Off, End to End Testing (E2E), Operational Readiness Review (ORR), Go-Live, and Certification Review (CR).
MES-REQ-PM-002	The Vendor must coordinate module milestone walkthroughs and participate in other module walkthroughs as required by the Department.
MES-REQ-PM-003	The Vendor must provide a written acknowledgment of any potential compliance issues formally communicated by the Department, its Vendors, or other stakeholders. Formal communication must be submitted through documented channels such as email or official correspondence. The Vendor's acknowledgment must be submitted to the Contract Administrator within two business days of receiving the formal notification.
MES-REQ-PM-005	The 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.
MES-REQ-PM-006	The Vendor must organize and participate in project-related meetings with the Department as required by the Department.
MES-REQ-PM-007	The Vendor must distribute meeting agendas to invitees at least one business day before the start of a scheduled meeting involving project stakeholders. Scheduled meetings include any reoccurring project meetings; meetings identified in the Work Plan or any meeting requested by the Department with at least two business days' notice. Vendor must distribute meeting minutes to meeting attendees within two business days of the scheduled meeting.
MES-REQ-PM-008	The Vendor must follow the Department processes and tools for the escalation of risks, issues and decisions during the project implementation and operations phases.
MES-REQ-PM-009	The Vendor must include a risk mitigation strategy for all risks and issues identified during the projects' implementation and operations.
MES-REQ-PM-010	The Vendor must draft and execute Department approved mitigation strategies for logged project risks and issues, within defined timeframes, throughout the project lifecycle. These plans must be maintained and monitored until risk/issue closure. The Vendor also must participate in the development and execution of risk/issue mitigation strategies owned by the Department.
MES-REQ-PM-011	The Vendors must include the following in risk/issue mitigation strategies: • Risk Assessment: An evaluation of the likelihood and impact of each identified risk. • Mitigation Strategies: Specific strategies and actions the Vendor is taking to resolve/close identified risks, including contingency plans. The Vendor must also include their plans for monitoring progress. • Timeline: when the Vendor expects certain mitigation activities occur and when the risk/issue overall is expected to be resolved.
MES-REQ-PM-012	The Vendor must manage requirements and demonstrate requirements traceability throughout the life of the contract, to include providing product demonstrations, sprint reviews (post-development/configuration reviews), and Requirement Traceability Matrix (RTM) maintenance, to support project implementation, operations, certifications, contract close out, and audits.

Requirement #	Requirement Description
MES-REQ-PM-013	The Vendor must provide the Department with 24x7, real-time, view-only access to their RTM tool and export its contents upon request in an excel/CSV.
MES-REQ-PM-014	The Vendor must provide all Deliverables to be approved by the Department in accordance with its formal deliverable review process and tools outlined in Attachment N: Deliverables and Milestones Schedule of the RFP.
MES-REQ-PM-015	The Vendor must provide a Deliverable Expectation Document (DED) for deliverables as requested by the Department, using the Department's preferred template as applicable.
MES-REQ-STAF-003	The Vendor must work with the Department to plan for and identify any policy, programmatic, and technology changes to ensure the success of the program.

Table R8. Testing

Requirement #	Requirement Description
DAP-REQ-TST-001	Vendor must ensure Go-live occurs only after UAT sign-off, successful completion of E2E and parallel runs, and State approval of readiness criteria (including performance, security, and data quality).
DAP-REQ-TST-002	Vendor must conduct structured UAT cycle following successful SIT completion with State users to validate business requirements and usability. Vendor must support defect resolution and retesting until UAT sign-off.
DAP-REQ-TST-003	Vendor must continue to perform peer code reviews, SIT, and UAT for all infrastructure changes, new or modified data pipelines, and other technical work during the Operations & Maintenance (O&M) phase.
DAP-REQ-TST-004	Vendor must provide support end-to-end (E2E) testing, including regression testing, dry runs of operational processes, and validation of data quality across the full ecosystem.
DAP-REQ-TST-005	The Vendor must provide test data strategies, including synthetic data where needed to protect PHI while preserving statistical properties.
DAP-REQ-TST-006	The Solution must support automated testing of data pipelines and ML workflows using unit, integration, regression, and expectation-based tests.
DAP-REQ-TST-007	Vendor must perform the Production cutover only after State approval, using an approved plan that includes reconciliation checks, rollback procedures, parallel run, go/no-go checkpoints, and a defined post-cutover hyper care support period.
DAP-REQ-TST-008	Vendor must perform security vulnerability assessments and penetration testing for the entire Solution (Solution configuration, data pipelines, code) and provide remediation prior to go-live.
DAP-REQ-TST-009	The Vendor must conduct peer reviews of all code (Solution configurations, data pipelines, reports, transformations) with the State prior to deployment to ensure adherence to standards, maintainability, and quality.
DAP-REQ-TST-010	The Vendor must perform a full migration in the Pre-Production environment with all end-to-end validations and data ETL/ELT pipeline testing completed.
DAP-REQ-TST-011	The Vendor must perform SIT covering end-to-end workflows across the Solution, ETL/ELT pipelines, security controls, and reporting layers.
DAP-REQ-TST-014	The Vendor must conduct comprehensive performance/load testing to validate that the Solution, data pipelines, and reports meet agreed-upon SLAs for latency, throughput, and concurrency prior to go-live.
DAP-REQ-TST-015	The Vendor must support 3 months of parallel run after E2E testing completion, where the new Solution runs side-by-side with the current system, validating outputs and building user confidence. Defects must be tracked and resolved during this period.
DAP-REQ-TST-018	The Vendor must support 5 months of E2E testing after UAT completion. Defects must be tracked and resolved during this period.
MES-REQ-TST-001	The Vendor must coordinate testing processes, activities and schedules with the State.

Requirement #	Requirement Description
MES-REQ-TST-002	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.
MES-REQ-TST-003	The Vendor must update the Master Test Plan, which is a living document, throughout all DDI phases within 30 calendar days of a change being implemented prior to SIT, change in scope, and changes to access to testing tools.
MES-REQ-TST-004	The Vendor must schedule, coordinate and support all testing activities to ensure that each test is prepared and performed in accordance with the Master Test Plan.
MES-REQ-TST-005	The vendor must lead, support and report status for all applicable test phases and all associated environments. This includes the test phases listed in Section 7.17 Testing.
MES-REQ-TST-006	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 before testing is considered complete. In addition, Vendors must perform system demonstrations after each sprint showing the State what was completed and successfully tested during that Sprint.
MES-REQ-TST-007	The Vendor must ensure it meets the State's Exit and Entrance criteria set for each phase of testing.
MES-REQ-TST-008	The Vendor must support all testing efforts with other Solutions (both internal and external).
MES-REQ-TST-009	The Vendor must utilize a Department approved automated testing tool.
MES-REQ-TST-010	The Vendor must participate in verification of non-system elements of the overall Solution, such as manual processes, as directed by the State.
MES-REQ-TST-011	The Vendor must make time-sensitive recommendations to support the specific Software Development Life Cycle (SDLC) activities (e.g., recommending for or against deployment of a new increment of functionality).
MES-REQ-TST-012	The Vendor must make recommendations concerning test execution activities based on the results of testing.
MES-REQ-TST-013	The Vendor must employ a testing escalation process that allows for criticality classification to determine frequency of reporting and/or meetings with the Department.
MES-REQ-TST-014	The Vendor must support the Department in all testing activities by providing support staff and technical expertise.
MES-REQ-TST-015	The Vendor must provide the Department access as needed to all test management software and test data including defect tracking, test execution status, test results and test traceability.
MES-REQ-TST-016	The Vendor must propose solutions for all issues, problems, and defects for the Solution identified through Operational Readiness Review.
MES-REQ-TST-017	The Vendor must identify test configurations and environment.
MES-REQ-TST-018	The Vendor must submit and obtain approval from the Department, of a Requirements Traceability Matrix (RTM) to ensure that all requirements are met with the appropriate evidence and artifacts. The RTM is a living document that will be submitted on a schedule approved by the Department.
MES-REQ-TST-019	The Vendor must design and document detailed test cases for each sub-phase of testing.
MES-REQ-TST-020	The Vendor must develop test cases that 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 cases must provide step-by-step instructions for executing test cases, including the identifications, expected results and actual results.
MES-REQ-TST-021	The Vendor must present all test cases to the Department for review and approval by the Department prior to the start of testing execution. The Department may provide additional test cases as agreed to by both parties.
MES-REQ-TST-022	The Vendor must 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.

Requirement #	Requirement Description
MES-REQ-TST-023	The Vendor must utilize a well-established and Department approved or supplied defect tracking tool and process for the management and reporting of all defects identified during testing.
MES-REQ-TST-024	The Vendor must provide a functional demonstration of the system including any changes or enhancements prior to UAT.
MES-REQ-TST-025	The Vendor must perform SIT sprint demos to the Department for each completed sprint. Additional demos can be requested as need.
MES-REQ-TST-026	The Vendor must implement version control in all environments.
MES-REQ-TST-027	The Vendor must provide authorized users access to necessary testing environments as required for testing during DDI and throughout the life of the contract.
MES-REQ-TST-028	The Solution's test environment(s) must mirror the production system in its size, files, databases, processing, and reporting. Any exceptions must be Department-approved and documented.
MES-REQ-TST-030	The Solution's test environment(s) data refresh must be scheduled per the Department approval for E2E testing.
MES-REQ-TST-031	The Solution improvements or enhancements must be deployed to test environments before they are deployed to the production environment.
MES-REQ-TST-032	The Vendor must plan and execute testing for all inbound and outbound interfaces, ensure accurate and secure data transmission between the solution and the MIS or an interface protocol determined by the department. The Vendor must also validate the file names, file format, and data integrity within the file.
MES-REQ-TST-033	The Vendor must perform regression testing for changes to the application, including defects and enhancements.
MES-REQ-TST-034	The Vendor must automate their regression suite and provide those results to the state at agreed-upon intervals.
MES-REQ-TST-035	The Solution must provide the ability to execute performance tests of a simulated user load consistent with the actual load projected or used in production.
MES-REQ-TST-036	The Vendor must have a process for and the capability to mask, sanitize, scramble, or desensitize sensitive data (e.g., PII/PHI) when extracting data from the Solution's production environment for use in non-production environments.
MES-REQ-TST-037	The Vendor must manage security, ad-hoc, or other specialized testing.
MES-REQ-TST-038	The Vendor must perform Operational Readiness Testing (ORT) that includes a test of actual data processing in a fully operational environment.
MES-REQ-TST-039	The Solution must provide the ability for the tester to perform temporal testing within all testing environments by manipulating the system date.
MES-REQ-TST-040	The Vendor must provide training for all testing participants that includes: the system, processes, procedures, and tools used to execute testing.
MES-REQ-TST-041	The Vendor must support all aspects including resources, scheduling, data, environments, and defect remediation as appropriate, for State-led testing.
MES-REQ-TST-042	The Vendor must support State-led UAT testing during planning and execution to include: • Assist the Department in developing UAT test cases. • Refresh data, execute processes, and migrate releases or code fixes as requested or on an agreed-upon schedule. • Provide UAT test data including masked production data.
MES-REQ-TST-043	The Vendor must ensure that UAT is conducted on a fully tested and operations-ready module component, including all software features.
MES-REQ-TST-044	The Vendor must participate in all E2E testing with other Department partners as directed by the Department. This will include E2E testing prior to launch and may include periodic E2E testing as other technical processes and systems are modified or brought online.
MES-REQ-TST-045	The Vendor must document test results and provide to the Department prior to implementing any changes in the production environment.

Table R9. Security and Compliance

Requirement #	Requirement Description
DAP-REQ-AUDT-009	The Solution must provide functionality to filter all required audit logs to identify and report on State-specified events.
DAP-REQ-DR-007	The Solution must support high availability and disaster recovery, including defined RTO and RPO targets, backup policies, and documented DR procedures.
DAP-REQ-SEC-002	The Solution must automatically enforce column-level data masking and policy-based redaction of protected or sensitive data across all identified environments and analyst workspaces. Controls must be applied dynamically based on user personas to ensure consistent, role-appropriate data access.
DAP-REQ-SEC-007	The Solution must support differentiated user personas (e.g., analysts, data engineers, data scientists, etc.) with configurable permissions aligned to their roles and responsibilities.
DAP-REQ-SEC-008	The Solution must support fine-grained, role-based access control (RBAC), including column- and row-level security, to protect confidential and sensitive data during data exploration, model development and analysis, and in the BI tools and visualizations. These access levels must be configured by the Vendor to meet the needs of the Department.
DAP-REQ-SEC-009	The Solution's Identity and Access Management (IAM) service must enforce centralized authentication and authorization across the Solution.
DAP-REQ-SEC-038	The Vendor must provide access to any configured user role to specified users following access processes to be established, and upon approval from appropriate NC Medicaid staff.
DAP-REQ-SEC-040	The Solution must operate in a fully isolated, single-tenant environment dedicated to the State of North Carolina.
DAP-REQ-SEC-041	The Solution must implement secure, role-based and/or attribute-based access controls (RBAC/ABAC) that enforce least-privilege principles, support role mapping from the identity provider (IdP), and enable just-in-time access. The Solution must restrict access to queries, reporting, configuration changes, code updates, and data uploads based on assigned roles, and must ensure that users are accurately assigned to appropriate security groups, as approved by the State.
MES-REQ-DATA-006	The Vendor must provide access to archived data to the Department within 48 hours of request.
MES-REQ-SEC-001	The Vendor must comply with the Federal, State and Department Security Policies and Standards.
MES-REQ-SEC-002	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.
MES-REQ-SEC-003	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.
MES-REQ-SEC-005	The Solution’s services and infrastructure must adhere to best practices and use open security standards and frameworks, such as: • Policy: WS-Policy, WS-Trust, WS-Privacy, Security Assertion Markup Language (SAML), Enterprise Privacy Authorization Language (EPAL) • Federation: WS-Secure Conversation, WS-Federation, WS-Authorization, XML Key Management (XKMS) • Mechanism: Extensible Access Control Markup Language (XACML), XML Encryption, XML-Digital Signatures, Extensible rights Markup Language (XrML), X.509 certificates
MES-REQ-SEC-006	The Vendor must implement the risk management framework in compliance with the NIST Risk Management Framework or equivalent.
MES-REQ-SEC-007	The Vendor must implement the Web Application Firewall (WAF) to mitigate the application security vulnerabilities such as OWASP TOP 10.
MES-REQ-SEC-008	The Vendor must run weekly vulnerability scans on all Vendor and subcontractor networks and systems that will access or host State data and information.

Requirement #	Requirement Description
MES-REQ-SEC-009	The Vendor must implement encryption for data in transit and data at rest using FIPS 140-2 or FIPS 140-3 compliant crypto material.
MES-REQ-SEC-010	The Vendor must ensure encryption of email transmissions, including attachments, that contain sensitive and confidential information.
MES-REQ-SEC-011	The Vendor must make its facilities reasonably available for inspection by NCDHHS PSO security staff, or a third party acting on NCDHHS's behalf when requested.
MES-REQ-SEC-012	The Vendor must comply with privacy and security related assessments or audits findings, conducted by NCDHHS, the State of NC, and Federal, including security audits, third party security assessments, and annual audits.
MES-REQ-SEC-013	The Vendor must perform internal risk assessment annually and share the assessment findings and corresponding CMS Information Security Program Plan of Action and Milestones (POA&M) / Corrective Action Plans (CAPS) with the Department.
MES-REQ-SEC-014	The Vendor must cooperate fully and completely with all Quality Assurance audits, evaluations, studies, investigations, surveys, reviews, and findings conducted by the Department, State, Centers for Medicare & Medicaid Services, or other auditing entities
MES-REQ-SEC-015	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 auditors from the U.S. Department of Health and Human Services (HHS) Office of the Inspector General, the State of NC or NCDHHS Internal Audit, or any other authorized auditors as determined by Department.
MES-REQ-SEC-016	The Vendor must remediate findings from security audits and assessments as per the guidelines described in the State Security Policies and must adapt to evolving controls as standards change.
MES-REQ-SEC-017	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.
MES-REQ-SEC-019	The Vendor must produce and maintain for ten (10) years, robust audit trails and audit logs of all applications and engineering activities (including inquiry transactions) on the environments wherever the production data is accessible.
MES-REQ-SEC-020	The Vendor must retain all records, electronic documents, and reports relating to this Contract for a period of ten (10) years after final payment is made under this Contract. When an audit, litigation, or other action involving or requiring access to records is initiated prior to the end of said period, records must be maintained for a period of ten (10) years following resolution of such action or longer if such action is still ongoing.
MES-REQ-SEC-021	The Solution must retain all system data, logs, correspondence, and reports of the past 180 calendar days of activity. Access to this data should be online, secure, and readily available to authorized State personnel during this period.
MES-REQ-SEC-022	The Vendor must conduct a 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).
MES-REQ-SEC-023	The Vendor must coordinate disaster recovery activities with the Department, application business owner, system owner and division Business Continuity Plan Coordinator.
MES-REQ-SEC-024	The Vendor must restore the Solution availability, in the event of unscheduled downtime, following the protocols and timing provided in the Disaster Recovery Plan.
MES-REQ-SEC-025	As part of Go-Live/Operational 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 recovery the Solution in accordance with the Disaster recovery Plan and in support of all Service Level Agreements.
MES-REQ-SEC-026	The Vendor must perform Disaster Recovery testing each year. 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.
MES-REQ-SEC-027	The Vendor must submit an After-Action Report that includes the DR testing results and issues experienced during DR testing.

Requirement #	Requirement Description
MES-REQ-SEC-028	The Vendor must obtain approval from the Department's Privacy and Security Office before storing or processing production data in lower environments such as development, test, UAT, and E2E.
MES-REQ-SEC-029	The Vendor must incorporate Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) in their SDLC.
MES-REQ-SEC-030	The Vendor must incorporate Interactive Application Security Testing (IAST) and Runtime Application Self Protection (RASP) techniques to improve the security posture of the application.
MES-REQ-SEC-031	The Vendor must provide the necessary access to the systems and required support to the Department or its authorized contractors to conduct an annual third-party privacy and security assessment including Whitebox penetration testing.
MES-REQ-SEC-032	The Vendor must provide the necessary access to the systems and required support to the Department or its authorized contractors to conduct third-party privacy and security assessment including Whitebox penetration testing for Operational Readiness Review (ORR).
MES-REQ-SEC-033	The Vendor must conduct annual independent third-party penetration testing and submit the test results and reports to the Department.
MES-REQ-SEC-034	The Vendor must maintain dedicated test environments adequate to support multiple testing workstreams concurrently, for example multiple concurrent cycles of internal testing and E2E Testing. In addition, for the E2E environment and testing specifically, the Vendor must maintain a test environment provisioned with the same privacy and security controls that are required by the Federal, State, and Department privacy and security requirements. As part of E2E testing, this environment must support and secure production data including production volumes.
MES-REQ-SEC-035	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.
MES-REQ-SEC-036	The Vendor must provide a disaster recovery (DR) site that is geographically separated from the primary site by at least 100 miles and not reliant on the same power or network utilities.
MES-REQ-SEC-037	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.
MES-REQ-SEC-038	In the event the Solution’s production environment 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 Department approves a return to normal operations.
MES-REQ-SEC-039	The Vendor must determine when the primary production site is inoperable due to a disaster and execute the Disaster Recovery Plan.
MES-REQ-SEC-040	The Vendor Solution must integrate identity and access management with NCID and support one of the following protocols: • Security Assertion Markup Language (SAML v2) • OAuth/OIDC
MES-REQ-SEC-041	The Vendor Solution must leverage Multi-Factor Authentication (MFA) provided by NCID when logging into the module system applications.
MES-REQ-SEC-042	The Vendor Solution must provide links to users of the State MFA documentation and guidance for installing MFA options to work with NCID.
MES-REQ-SEC-044	The Vendor must provide at least two Department individuals with administrative accounts to provide continuity of operations.
MES-REQ-SEC-046	The Vendor must certify that all Confidential (PHI/PII) and sensitive 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 Security Awareness training.
MES-REQ-SEC-047	The Solution’s disaster recovery environment must fully support production-level availability, capacity, and capabilities while maintaining adherence to all contract SLAs.

Table R10. Cost & Resource Management

Requirement #	Requirement Description
DAP-REQ-BILL-004	The Solution must track and report compute and storage costs at the analyst workspace level to both administrators and end users.
DAP-REQ-BILL-005	The Solution must allow administrators to configure hard or soft budget limits at the warehouse, project, or environment level, with the ability to throttle or pause workloads, and raise alarms when thresholds are breached.
DAP-REQ-BILL-006	The Solution must allow workload isolation across teams, projects, or environments by enabling separate compute pools, warehouses, or job clusters.
DAP-REQ-BILL-007	The Solution must enforce standardized resource tagging (e.g., cost center, project ID, environment, owner) for all compute, storage, and integration resources to ensure traceable cost attribution.
DAP-REQ-BILL-008	The Solution must expose monitoring data programmatically (APIs/exports) for integration into enterprise cost management tools (e.g., FinOps dashboards, Power BI or similar).
DAP-REQ-BILL-009	The Solution must integrate with enterprise alerting and collaboration tools (e.g., Azure Monitor, Amazon Cloud Watch, Google Cloud Monitoring, ServiceNow, Teams, email) for automated budget and usage notifications.
DAP-REQ-BILL-010	The Solution must provide budget forecasting tools and configurable alerts when projected usage is expected to exceed thresholds.
DAP-REQ-BILL-011	The Solution must provide differentiated cost thresholds based on State prescribed percentages (warning, critical, shutdown) to support progressive enforcement of budget controls.
DAP-REQ-BILL-012	The Solution must provide real-time dashboards and usage reports for compute and storage consumption, with the ability to configure budget alerts or anomaly notifications and also allow drill-down from aggregate cost dashboards into warehouse, job, query, or user-level detail to identify cost drivers.
DAP-REQ-BILL-013	The Solution must support anomaly detection beyond thresholds (e.g., sudden spikes in compute, unexpected cross-region data egress).
DAP-REQ-BILL-014	The Solution must support enforcement of cost controls through RBAC/ABAC (e.g., restricting who can spin up XL warehouses or cross-region data transfers).
DAP-REQ-BILL-015	The Solution must support per-user, per-project, or per-workspace cost attribution and chargeback reporting.
DAP-REQ-BILL-016	The Solution must support trend analysis (e.g., 7-day, 30 day, YTD) to track consumption patterns and forecast future spend.
DAP-REQ-BILL-017	The Vendor must configure the Solution to provide recommendations for right-sizing compute (e.g., warehouse auto-suspend/auto-resume, scaling policies, spot vs. reserved capacity).
DAP-REQ-BILL-018	The Vendor must enable lifecycle management policies for unused or underutilized resources (e.g., orphaned warehouses, stale datasets).
MES-REQ-STAF-001	The Vendor must provide sufficient personnel to administer and execute required project activities during the development, implementation, and operations phases of the project. This includes completing the project within the required timeframe, meeting the quality standards outlined in this RFP, and maintaining the adequate staffing levels throughout the life of the project.
MES-REQ-STAF-002	The Vendor is solely responsible for and incurs all the costs related to recruiting, hiring, training, monitoring the performance of, and managing qualified professional and other staff to meet contractual requirements.
MES-REQ-STAF-004	The Vendor's staff, working remotely, must be available to work in the State's primary project location at the Department's request for functions necessary to support the scope of work (e.g., risk review meetings, root cause analysis sessions, integration planning, release planning, operational readiness reviews, user acceptance testing, implementation, and production deployment).
MES-REQ-STAF-005	For any work performed at a location other than the primary Project site, the Vendor must identify the specific location (city, state, country), describe the type of work to be performed, and the percent of the total hours for that type of work at that location.
MES-REQ-STAF-006	The Department reserves the right to request removal of any Vendor key personnel, assigned to the project, and the Vendor must comply with any such request immediately.

Requirement #	Requirement Description
MES-REQ-STAF-007	The Vendor may not fill two key personnel roles with the same resource without approval from the Department.

Table R11. Training & User Adoption

Requirement #	Requirement Description
DAP-REQ-ENB-001	The Vendor must provide a Data Operations Coach, for a period of two (2) years after Solution go-live, to serve as a Data Engineering coach to the State's analyst team.
DAP-REQ-ENB-011	The Vendor must provide training to selected State staff on maintaining migrated reports and data architecture pertaining to the consumption layer or other layers.
DAP-REQ-ENB-012	The Vendor must provide user guides, playbooks, office hours during standard business hours, and a community of practice to build data literacy and self-service.
MES-REQ-TRN-002	The Vendor must design and conduct all training in collaboration with the department and in accordance with the approved solution Training Plan.
MES-REQ-TRN-003	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.
MES-REQ-TRN-004	The Vendor must create and maintain all training materials in such a way as to account for any system, policy, and operational modifications that are made throughout operations and maintenance.
MES-REQ-TRN-005	The Vendor must provide training that describes the features, functions, limitations, standards and governance processes, tools, and other relevant items.
MES-REQ-TRN-006	The Vendor must analyze, define, and tailor training to each specific user role and group (including external and internal user roles and groups).
MES-REQ-TRN-007	The Vendor must ensure that the end users (state authorized users, Applicant users, Provider users, Vendor users) receive the training, education and technical assistance necessary for successful implementation, integration, and downstream operations. This training activity will be measured using the training evaluation and end user experience as included in the Training Plan. Post implementation training must be performed by the Vendor.
MES-REQ-TRN-008	Vendor must provide, maintain, and update a training environment to design training and conduct training for each user, role, and group during DDI and O&M. Users and Department staff must have access to this environment.

Table R12. Advanced Analytics & AI

Requirement #	Requirement Description
DAP-REQ-AA-002	The Solution must allow authorized users to build, test, and validate models using governed workflows, while maintaining compliance with data and model governance policies.
DAP-REQ-AA-003	The Solution must enable users to access curated, production-grade analytical data—such as data from a governed gold or semantic layer—for use in AI/ML workflows.
DAP-REQ-AA-004	The Solution must ensure that any outputs or artifacts generated by AI/ML experimentation are stored in staging or isolated areas and do not overwrite production datasets.
DAP-REQ-AA-005	The Solution must implement audit logging and data lineage tracking for all AI/ML activities, including data access, model development, and deployment actions.
DAP-REQ-AA-006	The Solution must offer support for both AutoML and code-first machine learning workflows to accommodate a wide range of end users, from analysts to data scientists.
DAP-REQ-AA-007	The Solution must provide integrated model monitoring capabilities to track model performance, drift, and usage over time.
DAP-REQ-AA-008	The Solution must provide native or integrated model training environments (e.g., notebooks, ML Pipelines, Managed Compute) that support reproducibility and version control.
DAP-REQ-AA-009	The Solution must restrict model deployment to production endpoints to authorized users and through an established change control process.

Requirement #	Requirement Description
DAP-REQ-AA-010	The Solution must support integration with a feature store for machine learning model input reuse.
DAP-REQ-GEN-002	The Solution must allow users to develop and fine-tune their own AI models (Including LLMs) using organization-specific data, guardrails, and standards.
DAP-REQ-GEN-003	The Solution must augment BI insights with GenAI to generate, explain, and recommend insights (e.g., narratives, KPIs, visualizations) in an intuitive, easy-to-navigate interface.
DAP-REQ-GEN-005	The Solution must include integrated GenAI-powered tools to assist with tasks such as writing SQL, building dashboards, and generating documentation, aligned with state AI COE policies.
DAP-REQ-GEN-006	The Solution must integrate with collaboration tools (e.g., Service Now, JIRA, SharePoint) to embed GenAI into daily workflows.
DAP-REQ-GEN-007	The Solution must maintain audit trails of GenAI interactions and outputs.
DAP-REQ-GEN-008	The Solution must provide governed, multi-channel conversational interfaces for querying data and analytics assets in natural language, with context retention, provenance, and auditable transcripts.
DAP-REQ-GEN-009	The Solution must provide orchestration capabilities for chaining and managing multi-step AI agent workflows.
DAP-REQ-GEN-010	The Solution must provide persistent agent workspaces with task memory and user context awareness.
DAP-REQ-GEN-011	The Solution must securely connect GenAI tools to governed enterprise data sources with role-based access control and masking where needed.
DAP-REQ-GEN-012	The Solution must support Agentic AI capabilities, including AI agents for code writing and reviews that are aware of the data catalog and data model.
DAP-REQ-GEN-013	The Solution must support human-in-the-loop feedback and correction loops for AI agents.
DAP-REQ-GEN-014	The Solution must support integration of GenAI agents with the semantic layer or governed business logic models.
DAP-REQ-GEN-015	The Solution must support multi-modal input and output (e.g., text, charts, images, documents) in GenAI workflows.
DAP-REQ-GEN-016	The Solution must support native or pluggable Retrieval-Augmented Generation (RAG) pipelines.
DAP-REQ-GEN-017	The Solution must support policy-governed AI agents that can plan and execute multi-step tasks using approved tools/APIs, with simulation (“dry run”) options, execution budgets, and full auditability.
DAP-REQ-GEN-018	The Solution must support tiered GenAI access controls based on user roles and organizational policies.

Table R13. Transition

Requirement #	Requirement Description
MES-REQ-OM-016	The Vendor must provide authorized users access to all environments as required for transition activities and throughout the lifecycle of the contract.
MES-REQ-OM-018	The Vendor must provide licenses to the Solution as required by the Department to allow users access to perform all necessary business functions.
MES-REQ-OM-019	The Vendor must provide licenses, services, and accounts for the Solution that are transferable to the state.
MES-REQ-OM-020	The Vendor must transition all licenses, services, and accounts procured for the Solution to the State in the event of a transition.
MES-REQ-OM-021	All transfers of software licenses and subscriptions must be completed 90 days after the notification of transfers as provided by NCDHHS to the Vendor.
DAP-REQ-TRNS-001	In the event of Contract transfer or termination, the Vendor must provide transition assistance in the migration of the cloud-based DAP from the Vendor provided cloud environment to a State provided cloud environment. Such assistance must include a complete transfer of all solution

Requirement #	Requirement Description
	assets such as source code, configuration details, data pipelines, transformation logic, any new models and reports, documentation, IaC scripts, code repository assets, and all data in usable formats.

Table R14. Certification

Requirement #	Requirement Description
MES-REQ-CERT-001	The Solution must comply with the CMS Seven conditions and standards.
MES-REQ-CERT-002	The Solution must meet the conditions for enhanced federal funding and other federal regulations required for Centers for Medicare & Medicaid Services certification as defined in Section 7.14.6 CMS Certification.
MES-REQ-CERT-003	The Solution must meet all federal Medicaid Information Technology Architecture (MITA) requirements.
MES-REQ-CERT-004	The Vendor must provide evidence to show how the Solution achieves the state-defined MITA maturity level AND achieves at least MITA Maturity Level 3.
MES-REQ-CERT-005	The Vendor must support the Department Agency with CMS Reviews including planning activities, meetings, presentations, demonstrations, required artifacts, and development of evidence packaging to meet CMS and State-specific outcomes.
MES-REQ-CERT-006	The Vendor must prepare system documentation for submission to the Department and CMS in a secured location in conjunction with the state for review no later than one month before to CMS certification milestone reviews.
MES-REQ-CERT-007	The Vendor must provide the data required for the Intake Form and supporting evidence for CMS reviews. This data must be accessible to the State on an ad-hoc basis through reports in the Solution, the functionality of which can be updated as directed by CMS. When completing the Intake Form, the Department will use the latest template published by CMS at https://cmsgov.github.io/CMCS-DSG-DSS-Certification-Staging/.
MES-REQ-CERT-008	The Vendor must enable the development of an Operational Reporting Workbook through a flexible solution that can be updated as directed by CMS that allows the state to pull the reports as needed for system performance oversight that demonstrates the continuous achievement of required and desired outcomes and metrics.
MES-REQ-CERT-009	The Vendor must participate and support, as needed, in the CMS certifications of the other modules.

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.

3.6.1 SPECIFICATIONS

Table S1. Platform Architecture

Specification #	Specification Description
DAP-SPC-ARC-001	Describe any proprietary apps or solution components you are proposing to bring in as a part of the Solution.

Specification #	Specification Description
DAP-SPC-ARC-003	Describe how the cloud Solution supports API-first design, modular deployments, in line with MITA modularity, and is enabling API domain separation (e.g., Claims, Providers, Eligibility) with secure API contracts and integration.
DAP-SPC-ARC-005	Describe how the Solution supports secure, auditable external access for third-party tools and partners while maintaining data sovereignty and audit traceability.
DAP-SPC-ARC-006	Describe how the Solution will allow for secure Vendor-specific storage zones or Data Landing Areas, where external parties data can be deposited, accessed, or processed within the Medicaid Solution environment. Include how the Solution supports cost attribution, storage isolation, and access controls for those external zones.
DAP-SPC-ARC-007	Describe how the proposed architecture manages schema evolution in a way that ensures backward compatibility (e.g. existing reports, integrations, and code do not break when data schemas change). Additionally, explain how the architecture supports the coexistence of slowly changing dimensions and real-time data updates.
DAP-SPC-ARC-008	Describe how the Solution decouples services for better maintainability.
DAP-SPC-ARC-009	Describe how the Vendor will provision and configure the infrastructure to support the Department's use of its own SAS EG Desktop licenses (bring-your-own-license model), and how this will be integrated into the overall Solution without relying on Vendor-provided SAS licensing.
DAP-SPC-ARC-012	Describe the overall architecture of the data Solution, including all cloud-native features (e.g., containerization, elasticity, disaster recovery) that are leveraged, and how data flows through it.
DAP-SPC-ARC-028	Describe how the Solution will provide low-code/no-code data exploration capabilities. Include in your narrative the tools used to achieve this functionality.
DAP-SPC-ARC-042	Describe how the Solution would integrate security and compliance scans into the IaC deployment pipeline to detect misconfigurations before deployment.
DAP-SPC-ARC-048	Describe the process you would follow to configure and install new tools (e.g. open source, third party, custom developed) the State deems necessary.
DAP-SPC-ARC-051	Describe what Infrastructure-as-Code (IaC) tool you are proposing to use (including if there are any proprietary components in it that you would bring in) and describe how the IaC code will be structured, stored, versioned, and have any changes approved by state, as well as how state management and backend storage (e.g. Azure ADLS, AWS S3,Google Cloud Storage) will be configured, including state locking, versioning, and remote access control.
DAP-SPC-ARC-058	Describe your methodology in identifying and documenting current and future states of the Solution prior to design and development activities.
DAP-SPC-ARC-059	Describe how the Vendor will integrate Power BI into the Solution—using either the State-owned instance on Microsoft Government Cloud 365 or a Vendor-provided instance—to ensure effective dashboard performance.
DAP-SPC-ODS-001	Describe how the Solution provides an Operational Data Store (ODS) within curated layer in the Data Warehouse (Snowflake, Databricks or similar) and what its architecture is, to support near-real-time integration of operational data.
DAP-SPC-ODS-008	Describe how Solution's ODS can provide APIs or service endpoints to expose curated ODS data for consumption by operational applications and services, in addition to BI/analytics tools.
MES-SPC-ARCH-001	Describe the approach to how the Solution can be hosted on: • A State hosted environment. Refer to State hosting capabilities at https://itservices.nc.gov/services/hosting/cloud-services. • A Vendor hosted environment. A narrative for both hosting options listed above must be included in your response.
MES-SPC-ARCH-006	Describe the future roadmap for your Solution for the next 1-3 years.
MES-SPC-DATA-002	Describe how the Vendor will provide real-time access to transactional data for integration with other MES Modules.

Specification #	Specification Description
MES-SPC-INT-002	Describe how the Vendor Solution's technical capabilities will support the services, protocols, standards, capabilities, and functionality of the core MIS Services referenced in Attachment V: Medicaid Integration Services Core Capabilities.
MES-SPC-INT-003	Describe the proposed Solution capabilities to integrate with other systems. Identify the standards supported, integrations Solutions, adaptors, APIs, etc.
MES-SPC-PM-007	Describe the Vendor's approach to production implementation and cutover.
MES-SPC-PM-008	Describe the Vendor's approach to collaborating with the existing analytics platform vendor to identify interfaces, capabilities, and processes, for seamless cutover.

Table S2. Data Flow Architecture

Specification #	Specification Description
DAP-SPC-CONS-001	Describe how the Solution will deliver secure, self-service analytics capabilities—including BI dashboards, ad-hoc queries, and AI/ML tools—accessible to business, clinical, and operational users without technical analyst support. Response should specify proposed tools, expected query performance, and how the design ensures usability, scalability, and data security.
DAP-SPC-CONS-002	Describe the tools available to both technical and non-technical users to explore, analyze, report, and visualize the data.
DAP-SPC-CONS-015	Describe how the Solution delivers geo-analytic capabilities such as: • display aggregates for user-selected geographic units (state, county, ZIP code, municipality, health district, managed-care region, LME service area, or user-defined area) • overlay political boundaries, streets, and major topographic features • plot individual records or record groups using street address, ZIP+4, or latitude/longitude • enable graphical drill-down from map features to underlying source data. • geocode records based on address.
DAP-SPC-CUR-001	Describe how the Solution handles data transformation, validation and curation especially for Medicaid data. Explain how you would provide ways to streamline and templatize moving the data from the Bronze Layer to the Silver Layer (for structured, semi-structured and unstructured data). Also include how you propose to handle any errors in the pipeline execution to ensure minimal disruption to operations.
DAP-SPC-CUR-006	Describe your approach to a visual or low-code interface for defining validation rules and thresholds.
DAP-SPC-DMD-001	Describe how the proposed Solution will support multiple data modeling approaches (e.g., Star Schema, Data Vault 2.0, Medallion, 3NF) and explain how the architecture will enable future transitions between modeling paradigms with minimal rework by using logical separation of layers, metadata-driven pipelines, and reusable data contracts or views. Include how the Solution's data model aligns with CMS guidelines (e.g., T-MSIS, MITA) and the state's Medicaid-specific reporting needs.
DAP-SPC-DMD-002	Describe how you would design the semantic layer, how it fits in the overall architecture, and its integration with BI tools (Power BI or similar), including any challenges you anticipate based on past experience, and how you propose to overcome them.
DAP-SPC-DMD-003	Describe how the Solution would use identity resolution techniques for cross agency data matching (e.g. would the Solution include open-source tools, custom scripts, etc.).
DAP-SPC-DMD-004	Describe the approach the Solution model uses to accommodate new programs or evolving policy requirements, which are anticipated to occur as other Medicaid modules serving as upstream or downstream systems, are modernized.
DAP-SPC-DMD-005	Describe whether the Solution leverages any pre-built, Medicaid-optimized data model tailored to the state's reporting and analytical needs or if it will be developed collaboratively.
DAP-SPC-DPR-001	Describe how the Solution establishes data interface contracts as a code for all data products across layers with the source system owners covering data types, SLA agreements, timeliness, refresh frequency and keys, along with business glossary.
DAP-SPC-DPR-003	Describe how the Solution provides domain driven design for data products.

Specification #	Specification Description
DAP-SPC-INTG-003	Describe how the Solution implements incremental (“delta”) loading—adding or updating only new or changed records/fields—instead of full-table overwrites. Include in your narrative how the Solution supports soft and hard deletes with proper auditing protocols.
DAP-SPC-INTG-004	Describe how the Solution provides real-time/streaming, near-real time and batch ingestion capabilities with clearly defined patterns for processing structured, semi-structured, and unstructured data.
DAP-SPC-INTG-005	Describe how the Solution supports robust error and exception handling mechanisms with detailed logging of failed records, or data load issues. Also describe how errors would be captured in an audit/error repository to support root cause analysis, and reprocessing. Lastly, describe how the Solution supports graceful recovery from ETL failures, including automatic restart or full rollback with no data loss.
MES-SPC-INT-001	Describe any import/export and/or extraction translation and load tools included in your solution.

Table S3. Migration

Specification #	Specification Description
DAP-SPC-MIGR-003	Describe the approach and process to convert, validate, and migrate existing types of reports and dashboards as identified in Section 3.1.4 Assets Migration and Validation, from the current State analytics system to the Solution while preserving business logic and historical continuity. Include in your narrative any proprietary or AI-based tools you would use.
DAP-SPC-MIGR-005	Describe how the Solution aligns with state IT on security controls, workspace architecture, global variables and other BI tool configurations, and ensure that all migration is done observing those guardrails.
DAP-SPC-MIGR-006	Describe the approach and process to convert, validate, and migrate existing types of ETL processes, scripts and views as identified in Section 3.1.4 Assets Migration and Validation, from the current State analytics system to the Solution while preserving business logic. Include in your narrative any proprietary or AI-based tools you would use.
DAP-SPC-MIGR-007	Describe the approach and process to convert, validate, and migrate existing types of migration assets as identified in Section 3.1.4 Assets Migration and Validation, from the current State analytics system to the Solution while preserving business logic and historical continuity. Include in your narrative any proprietary or AI-based tools you would use.
MES-SPC-DATA-001	Describe approaches available for data conversion and/or data migration to load current data into proposed Solution.

Table S4. Workflow Management and Performance

Specification #	Specification Description
DAP-SPC-DEV-001	Describe how GitHub Actions (or similar tool) will automate workflows, along with approvals and rollback triggers.
DAP-SPC-DEV-002	Describe how a Git-based tool will be used to store and manage all version-controllable assets (IaC templates, ETL scripts, semantic model, BI dashboards), including branching strategy, pull request policies, version control, approvals, and lifecycle tracking, ensuring stable promotion between environments.
DAP-SPC-DEV-007	Describe how the Solution supports drift detection between declared infrastructure (Infrastructure Drift) definitions (e.g., Terraform state or similar) and the actual deployed state using automated Git-based workflows and logging integrations (e.g., Teams, Datadog, Azure Monitor or similar).
DAP-SPC-ORC-010	Describe how the Solution will enable a robust scheduling and data orchestration capability.
DAP-SPC-SP-001	Describe the levels of service offered for system uptime, support response times, and issue resolution. Include in your narrative the metrics and definitions for each service level.
DAP-SPC-SP-002	Describe the tools or support available for improving query speed and Solution performance. Indicate whether you offer tools for performance analysis of slow queries or jobs.

Table S5. Data Governance and Management

Specification #	Specification Description
DAP-SPC-DG-001	Describe how the Solution provides a single Data Catalog that stores technical, business, and governance metadata and is searchable by all authorized users.
DAP-SPC-DG-006	Describe how the Solution would provide end-to-end data lineage and its visualization across ingestion, transformation, and reporting layers, with visibility into column-level transformations and business rules.
DAP-SPC-DG-017	Describe how the Vendor would collaborate with State to incorporate metadata quality feedback into data governance.
DAP-SPC-DG-021	Describe how the Solution enforces policy-as-code controls for retention, classification, and purpose limitation.
DAP-SPC-DG-022	Describe how the Solution would allow users to apply tags to datasets for better categorization, making it easier to group and discover related data assets.
DAP-SPC-DG-028	Describe how the Solution data catalog adapts to maturing Medicaid organizational level data governance policies and requirements.
DAP-SPC-DG-029	Describe how the Solution uses machine learning to automatically classify data based on content (e.g., identifying PII or sensitive data) to enhance governance and compliance.
DAP-SPC-DG-030	Describe how the Solution suggests related datasets or relevant metadata fields based on user queries, improving data discovery and productivity.
DAP-SPC-DG-031	Describe your approach to engage the business data stewards and owners to align the Solution's data governance with the Medicaid Enterprise Data Governance guidelines and policies.
DAP-SPC-DQ-001	Describe how the Solution provides a reusable automated data-quality framework, tool, and/or library for DQ validation, monitoring and publishing quality metrics dashboards to improve data quality by leveraging both rule-based and AI-driven techniques to tackle data quality challenges, anomaly detections, and enhance data integrity, consistency, accuracy, uniqueness, timeliness, completeness, validity, conformity.
DAP-SPC-DQ-002	Describe how the Solution recognizes abnormal patterns and data outliers that can signify data quality issues.
DAP-SPC-DS-003	Describe how the Solution will securely enable the sharing of data —internally or externally—in ways that are discoverable, governed, auditable, and reusable, without duplicating it or losing control.
DAP-SPC-DS-004	Describe how the Solution will enable governed data sharing with external entities (e.g., MCOs, CMS, researchers, third-party Vendors), including support for access-controlled data views, API endpoints, time-bound sharing (include renewal options, and revocation controls), protocols, and audit logging of external access events.
DAP-SPC-MMM-002	Describe how the Solution implements data monitoring and alerting on all data pipelines to ensure data is flowing correctly in production which includes throughput checks covering both basic ZCC (Zero count check), and their upgrade to SPC (Statistical Process Control) checks, as well as monitoring job failures, data latency, data quality anomalies, or report refresh status. Include how the Solution provides automated hooks for notifying downstream dependencies to allow users of the data (e.g., those writing SQL, or consuming data), and report builders who subscribe to monitoring alerts, to be notified.
DAP-SPC-MMM-004	Describe how the architecture will support monitoring, observability, and logging, including collection of telemetry from storage, pipelines, cost, APIs, and compute workloads with alerting capabilities by leveraging automated metadata collection from cloud-native sources (Snowflake, Databricks, Azure, AWS, Google Cloud, APIs, etc.).
DAP-SPC-MMM-007	Describe how the Solution would integrate with enterprise observability tools (e.g. Azure Monitor, Amazon Cloud Watch, Google Cloud Monitoring, App Insights, ServiceNow, PagerDuty).
DAP-SPC-MMM-022	Describe how the Solution integrates monitoring and metadata with enterprise observability Solutions (e.g. SIEM) and FinOps dashboards.
MES-SPC-DATA-004	Describe how the Solution would provide context sensitive help to view definitions of all data on system.

Table S6. Operations

Specification #	Specification Description
DAP-SPC-MS-001	Describe how the Solution provides 24x7 monitoring and alerting for Solution availability, performance, and pipeline failures. Describe how Solution will provide responsive and proficient operations customer services.
DAP-SPC-MS-004	Describe how efficiencies are provided in the form of fully automated operational services where appropriate.
DAP-SPC-MS-007	Describe your approach to manage software updates, patches, and change requests with minimal disruption. Include the processes used to support Continuous Integration / Continuous Delivery (CI/CD) with managed, governed and automated process including code quality, coverage and security scan, version control and rollback activities.
DAP-SPC-MS-026	Describe how the Vendor provides a Solution for conducting application maintenance that will have minimum impact during the State's business hours.
DAP-SPC-MS-027	Describe your strategy for ensuring minimal disruption to end-user access to tables and queries if data loads occur during the State's business hours.
DAP-SPC-MS-048	Describe how you would develop and maintain a process to archive and access archived data (including legacy MMIS component data).
DAP-SPC-MS-049	Describe how the Solution provides an auditable change management and service request logging and management workflow, which supports requests for platform changes and access provisioning for end users, minimizes manual effort, allows for State approvals of the requests, and enables end-user self-service.
MES-SPC-OM-001	Describe your plan to provide NCDHHS the ability to transition from the Vendor solution to State/New Vendor and maintain the continuity of operations.
MES-SPC-OM-002	Describe your approach to ensure the Solution and all included portals and interactions are available for NC users with an annual availability with the stated SLA uptime.
MES-SPC-OM-003	Describe your approach to address and resolve customer support and technology disruptions impacting the ability to maintain a fully working Solution. Include in your narrative: • The timeframe required to accomplish full recovery from the point of interruption. • Strategies for addressing longer disruptions resulting from natural disasters or cyberattacks. • A detailed communication strategy to ensure stakeholders are informed during disruptions.
MES-SPC-OM-004	Describe how the Solution promotes sharing, leveraging, and reuse of healthcare technologies and systems within and among states in accordance with the CMS Standards and Conditions (Leverage Condition) in force during the period of the contract.
MES-SPC-PM-009	Describe how the Vendor will identify and acquire the licenses necessary for any software, services, and accounts to support the requirements defined in the RFP. Include in your narrative how the State can own or be named on the license of any software that is designed, developed, installed, improved, or configured with enhanced Federal Funding Participation (FFP), in accordance with § 433.112(b)(5).

Table S7. Project Management

Specification #	Specification Description
MES-SPC-PM-001	Describe your requirement management methodology during the DDI and O&M phases based on the RTM deliverable. Include in your response the approach to connecting requirements to their evidence and vice versa (bidirectionality).
MES-SPC-PM-002	The Solution will become one module in the State's Medicaid Enterprise Solution (MES), where multiple vendors and the State may need to coordinate activities during development and as the different modules are prepared, tested and implemented. Describe your approach to this coordination and your availability for onsite meetings during DDI or special circumstances if requested by the State.
MES-SPC-PM-004	Describe the Vendor's quality assurance policies procedures, and practices it will implement to ensure quality, completion, and validation of the accuracy of the documentation and services required in the RFP.
MES-SPC-PM-005	Describe how you will measure, track and document the quality of deliverables.

Specification #	Specification Description
MES-SPC-PM-006	Describe the approach for participation in Department initiated reviews and incorporation of feedback and recommendations.

Table S8. Testing

Specification #	Specification Description
DAP-SPC-TST-017	Describe how the Solution supports parallel run comparisons.
MES-SPC-TEST-001	Describe the testing environments you will maintain in order to support all appropriate testing phases as listed in Section 7.17 Testing.
MES-SPC-TEST-002	Describe how your Solution's test environment mirrors the production environment in its size, files, databases, processing, data protection, and reporting. Include how this state of the environment is maintained in the response.
MES-SPC-TEST-003	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.
MES-SPC-TEST-004	Describe the Vendor's approach to ensuring independence and separation between the development and testing organizations.
MES-SPC-TEST-005	Describe how the Vendor Solution will create and load test data and utilize it during the testing process. Include how PHI and PII data is protected or masked during testing and how participants are notified if testing involves confidential, PHI, or PII data.
MES-SPC-TEST-006	Describe how you conduct testing using automation testing tools, level of test automation, interactive testing, and interactive debugging available in the test environment.
MES-SPC-TEST-007	Describe how you would develop, maintain, and automate your regression suite. Include pertinent details on the tools that will be used.
MES-SPC-TEST-008	Describe how your Solution provides performance tests, and reporting of a simulated load consistent with the actual load projected or used in production.

Table S9. Security and Compliance

Specification #	Specification Description
DAP-SPC-DR-016	Describe the Solution back-up and retention recommended policies.
DAP-SPC-AUDT-002	Describe the audit capabilities within the Solution to enable the audit of all activities, reports, and analytics by user ID, activity, time frame, and by report, as well as providing authorized users access to this information.
DAP-SPC-SEC-004	Describe how the Vendor works with the state team to design user personas and their corresponding security roles and permissions in order to implement role-based data access and catalog transparency so that users obtain data relevant to their roles within defined SLAs.
MES-SPC-INT-004	Describe how the Solution's data exchanges (including inbound and outbound interfaces) comply with industry standards (such as NIEM, NIST, HIPAA, HL7, FHIR, CCDA, and CSV) where applicable. Include in the narrative how non-standard formats required by State are covered.
MES-SPC-SEC-001	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.
MES-SPC-SEC-002	Describe how your Solution supports the State’s Identity and Access Management protocols referenced in Section 3.4.3 Identify, Credential, and Access Management (ICAM).
MES-SPC-SEC-003	Describe how the proposed Solution manages user provisioning process to access the system functionalities.
MES-SPC-SEC-005	Describe the frequency and test procedures for end-to-end disaster recovery testing.

Table S10. Cost & Resource Management

Specification #	Specification Description
DAP-SPC-BILL-001	Describe how the overall architecture is designed for cost-effectiveness, including how the proposed Solution will manage total cost of ownership (TCO) across compute, storage, user access, Vendor participation, and scalability. Include support for forecasting, billing transparency, and FinOps reporting for NCDHHS budgeting purposes.
DAP-SPC-BILL-002	Describe how the Solution would support granular cost attribution and chargeback by enabling visibility into resource consumption at both the team and component levels. This includes the ability to allocate costs based on team ownership (e.g., via tags, projects, or organizational units) and to break down expenses by specific architectural components such as compute, storage, networking, and managed services.
DAP-SPC-BILL-003	Describe how the Solution would provide policies and controls that prevent untagged or mis-tagged resources from being provisioned.
DAP-SPC-STAF-003	Describe your detailed proposed staffing approach for each phase of the proposed work before and after go live. Include in your narrative additional resources beyond the key personnel listed in Attachment K: Vendor Key Personnel, who will be supporting this project, and list number of hours / percent dedication for each resource.
MES-SPC-STAF-001	Describe how the Vendor will hire and retain staff and key personnel with the qualifications and experience necessary to perform the requirements of this RFP.
MES-SPC-STAF-002	Describe the physical locations where the main office and satellite offices (if satellite offices are applicable) are located in North Carolina.

Table S11. Training & User Adoption

Specification #	Specification Description
DAP-SPC-ENB-002	Describe how the Solution provides a comprehensive training and change-management program, including ongoing coaching and role-based curriculum, hands-on workshops, and reference materials—to upskill NC Medicaid staff and analysts on the new Solution.
MES-SPC-TRN-001	Describe the curriculum and training documents used for training external users. Include in your narrative help screens, descriptions of online or printable materials, use of knowledge bases, etc.
MES-SPC-TRN-002	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.

Table S12. Program Integrity

Specification #	Specification Description
DAP-SPC-FRD-001	Describe how you provide a SURS solution certified by CMS.
DAP-SPC-FRD-002	Describe how the Solution supports provider surveillance by enabling peer group analysis, including the ability to define peer groups, perform statistical comparisons across provider types and programs, identify outliers based on configurable thresholds, and generate ranked or scored reports of anomalous provider behavior.
DAP-SPC-FRD-003	Describe how the Solution enables ongoing and scheduled monitoring of provider billing patterns to detect anomalies such as unusual spikes or deviations in claim submissions, including support for user-defined parameters, trend analysis, and the generation of clear, user-friendly reports.
DAP-SPC-FRD-004	Describe how the Solution identifies relationships and shared characteristics among providers, including linked ownership, common contact information (e.g., addresses, phone numbers, email addresses), business affiliations, and suspicious or high-risk locations. Include how the Solution also surfaces providers and owners with prior investigative or adverse history.
DAP-SPC-FRD-005	Describe how the Solution supports automated profiling of providers, provider groups, and beneficiaries to detect patterns of potential fraud, abuse, or excessive billing. Include how the Solution enables analysis by National Provider Identifier (NPI), diagnosis codes, and provider roles (e.g., primary care case managers), and generates reports that classify treatment modalities, track service utilization, and support suppression of specific individuals or categories from analysis on a run-to-run basis.

Specification #	Specification Description
DAP-SPC-FRD-006	Describe how the Solution supports fraud and abuse investigations by enabling retrospective claims and encounter data retrieval, focused reviews, and generation of investigative reports. Include how the Solution allows monitoring of provider payments, replication of remittance advice with enhanced data elements, and identification of provider relationships, including shared ownership, contact information, business affiliations, and prior investigative or adverse history.
DAP-SPC-FRD-007	Describe how the Solution applies clinically approved guidelines to episodes of care to identify deviations from expected treatment patterns, minimizes manual effort in detecting deficiencies, and generates reports on quality and level of care by provider type. Include how the Solution also supports monitoring of access to specialists for enrollees with special health care needs using encounter data.
DAP-SPC-FRD-008	Describe how the Solution supports exception processing by enabling automated analysis and reporting in response to leadership and Medicaid fraud control unit requests, using computerized techniques to identify and prioritize outliers. Include also how the Solution applies weighting and ranking to exception items to highlight the highest deviators and generates detailed reports on provider practices identified as exceptions.
DAP-SPC-FRD-009	Describe how the Solution supports automatic outlier detection by continuously monitoring claims, billing, and utilization data to identify significant deviations from expected patterns, including high-cost services, aberrant provider behavior, and service misutilization. Include also how the Solution generates early warning alerts, analyzes electronic visit verification (EVV) data, detects fraudulent billing practices (e.g., drug misbranding or timing anomalies), and supports fiscal oversight through automated reporting and trend analysis.
DAP-SPC-FRD-010	Describe how the Solution monitors beneficiary utilization to identify deviations from established norms or quality standards, including the ability to track service use across programs, diagnoses, and time periods, regardless of changes in beneficiary identifiers. Include also how the Solution supports profiling of beneficiaries, providers, and MCOs; generates unduplicated counts and trend reports by demographic and program attributes; and enables the detection of under-utilization, lock-in program activity, and the generation of customized beneficiary communications such as EOB notices.
DAP-SPC-FRD-011	Describe how the Solution supports routine monitoring of claims and encounter data by enabling flexible reporting by provider type, beneficiary classification, and other key variables, with configurable timeframes and exportable outputs. Include also how the Solution supports exception identification (e.g., emergency services without prior authorization, pay-and-chase pharmacy claims, TPL override scenarios, and 340B billing anomalies), and allows for algorithm testing and refinement prior to report generation.
DAP-SPC-FRD-012	Describe how the Solution supports program management by providing data and analytics to assess provider network adequacy, service utilization, and payment distribution. Include also how the Solution generates counts of services, claims, beneficiaries, and providers using meaningful units; analyzes cost-effectiveness of managed care versus fee-for-service; identifies payments by type (e.g., abortions, sterilizations); clearly reports the Federal Share of each claim; and evaluates the accuracy and effectiveness of claim edits.
DAP-SPC-FRD-013	Describe how the Solution supports scheme-based analysis by identifying providers with billing patterns indicative of specific risks, schemes, or program violations, using configurable analysis measures. Include also how the Solution detects other providers exhibiting similar billing behaviors to those previously confirmed as fraudulent or suspicious through investigations or law enforcement actions.

Table S13. Advanced Analytics & AI

Specification #	Specification Description
DAP-SPC-AA-001	Describe how the architecture enables end-to-end ML/AI workflows, incorporating data versioning, feature stores, and a centralized model registry integrated with code version control, metadata tracking, and model lifecycle management (e.g., development, staging, production). Include support for CI/CD pipelines with policy-driven approval gates for promoting models to production.
DAP-SPC-GEN-001	Describe how the Solution provides access to foundational models (e.g., LLMs) via APIs or native services for text, summarization, and content generation tasks, and how it would enable Retrieval-Augmented Generation (RAG) based use case development.

Specification #	Specification Description
DAP-SPC-GEN-004	Describe how the Solution enforces AI guardrails through moderation filters, validation steps, and policy-based controls and similar.

Table S14. Transition

Specification #	Specification Description
DAP-SPC-TRNS-008	Describe how the Vendor ensures an issue-free transition to the State or another vendor at the end of the contract term of all processes, workflows, and tasks.
MES-SPC-PM-010	Describe how the software licenses associated with the Solution can be assigned to NCDHHS as part of the base Software agreement with the Vendor and resellers. Please include in your narrative how you will include NCDHHS Terms and Conditions in found in Attachments B and C in any master service agreements or contracts for the purchase of third-party software to simplify the assignment of the licenses. This applies to all software licenses, subscriptions and maintenance contracts associated with the Solution.

Table S15. Certification

Specification #	Specification Description
DAP-SPC-CERT-001	Describe the compliance standards or certifications that the Solution supports. (e.g., HIPAA, PHI, PII, SOC 2).
MES-SPC-CERT-001	Describe your experience with the MITA framework, and how that supports the State's achievement of MITA Level 3 or higher capability levels. Include in your narrative the information and technical architectures that support the solution while conforming with both the MITA Framework and Seven Standards and Conditions.

3.7 OPTION REQUIREMENTS AND SPECIFICATIONS - RESERVED

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must provide a complete cost proposal that is inclusive of all of the 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:

a. **Total Implementation (DDI) Costs**: The DDI milestone costs, DDI run rate costs, and software related costs associated with planning, development, and implementation effort necessary to deliver the solution and services outlined in this RFP.

   i. Each milestone provided in the Cost Proposal Workbook must have a cost associated with producing deliverables and achieving the milestone in the contract year that the milestone is anticipated to be achieved.

   ii. The Vendor may submit an invoice for a milestone after acceptance of the milestone by the Department.

   iii. DDI Run Rate and DDI Software Related costs will be billed as one-twelfth ($1/12^{th}$) of the annual cost for the cost item for the upcoming month.

   iv. Actual DDI Variable Use costs incurred in a month will be billed in the following month.

b. **Operations and Maintenance (O&M) Costs:** The O&M Deliverable costs, O&M run rate costs, and software related costs for ongoing services and support necessary to provide the solution and services outlined in this RFP after the initial implementation.

   i. O&M Costs must be provided for each year of the contract term where operations and maintenance costs are expected to be billed.

   ii. O&M Costs will begin after Solution implementation is complete and approved by the Department.

   iii. O&M Run Rate costs and O&M Software related costs including cloud hosting, application software licensing, and maintenance fees will be billed monthly as one-twelfth (1/12th) of the annual cost for the cost item for the upcoming month.

   iv. O&M Deliverable costs will be billed by the Vendor upon delivery and approval of the deliverable by the Department.

   v. Actual O&M Variable Use costs incurred in a month will be billed in the following month.

c. **Other Cost Information**

   i. Fully Burdened Hourly Off-site Labor Rates for all Key Personnel and other project staff must be provided.

   ii. Fully Burdened Hourly Off-site Labor Rates for all Consulting services labor categories must be provided.

   iii. 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.

   iv. The Vendor must provide any assumptions made in their cost proposal.

For additional information regarding the cost proposal content, see *Attachment E: Cost Form* and the instructions provided in the Cost Proposal Workbook.

4.2 PAYMENT SCHEDULE

The Vendor must propose its itemized payment schedule based on the content of its offer.

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. While all responsive proposals will be evaluated in accordance with the stated criteria, consideration will be given to the impact on the State's technical and business resources and environments.

a. Business and Technical Specifications of this RFP. Within the business and technical specifications listed in *Section 3.6.1 Business and Technical Specifications,* 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 Platform Architecture category is more important than the Migration category. The specifications listed within a major category, such as Platform Architecture, are all of equal importance. In addition to the business and technical specifications, vendors in the competitive range will be required to perform a system demonstration as defined in *Section 5.6 System Demonstrations* after 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 including the Fixed Price Costs and the Not-To-Exceed Variable Use Costs for the duration of the contract including the base years and option years, in the formatted cost worksheets provided in the Cost Proposal Workbook of this RFP.

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

5.2.1 EVALUATION OF OPTIONS - RESERVED

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 Vendors whose proposals are determined to be reasonably susceptible of being selected for award based on the stated evaluation criteria. Only those Vendors within the competitive range will be invited to participate in additional evaluation activities, to include a System demonstration.

5.6 SYSTEM DEMONSTRATIONS

System demonstrations will be conducted only with Vendors 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 evaluation criteria in *Section 5.2 Evaluation Criteria* and will be factored into the 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. The availability of this information is 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 shall respond to the protesting Vendor in writing with a final agency decision.

c. If a protest is determined by the agency head 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 Contract Specialist listed for this RFP may be grounds for rejection of said Vendor's offer.

Written questions concerning this RFP must be received by the stated deadline. Questions must be submitted to the Contract Specialist listed for this Solicitation via the Ariba Sourcing Tool's Event Messages page. Please enter "Questions Solicitation #30-2025-008-DHB" as the subject for the message.

Questions should be submitted in a Excel document 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. 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 "**#30-2025-008-DHB, Alternate Offer, Name of Vendor**" and numbered sequentially with the first offer if separate offers are submitted.

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

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] [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Contract Manager	[NAME OF VENDOR] [STREET ADDRESS] [CITY, STATE, ZIP] 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:

a. 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.

b. 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.

c. 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.

d. 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:** Description of Offeror 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 entire body of the RFP** and signed receipt pages of any addenda released in conjunction with this RFP;
3. **Completed Attachment T:** Technical / Management Proposal to be provided in accordance with the instructions provided for completion;
4. **Completed Attachment H:** Completed Past Performance Questionnaires from References in accordance with instructions provided for completion;
5. **Completed Cost Proposal Workbook:** Completed in accordance with *Section 4 Cost of Vendor's Offer***,** and instructions provided in *Attachment E: Cost Form* and the Cost Proposal Workbook;
6. **Completed** and **signed** version of **Attachment F**: Vendor Certification Form;
7. **Completed Attachment G:** Location of Workers Utilized by Vendors – Disclosure Statement;

8. **Completed Attachment I:** Financial Review Form and copies of Financial Statements as further described in *Section 7.2 Financial Statements*;
9. **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;
10. **Completed Attachment K:** Vendor Key Personnel in accordance with the Instructions provided for completion;
11. **Completed Attachment M:** Contract Administrators;
12. **Completed Attachment N:** Deliverables and Milestones Schedule in accordance with the instructions provided for completion in paragraph 2.0 Milestones;
13. **Completed Attachment O**: Business Continuity Plan in accordance with the Instructions provided for completion;
14. **Completed Attachment P**: Disaster Recovery Plan in accordance with the Instructions provided for completion;
15. **Completed** and **signed** version of **Attachment Q**: State Certifications;
16. **Completed** and **signed** version of **Attachment R**: Federal Certifications;
17. **Completed** and **signed** version of **Attachment S**: Business Associate Agreement;
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. **Completed** version of **Attachment Z:** Subcontractor Identification Form for each known Subcontractor;
21. **Completed** and signed version of **Attachment AC**: GenAI Disclosure and Fact Sheet;
22. Current independent 3rd party assessment report in accordance with *Section 3.3.2*, *paragraph b, subparagraphs i)-iii);*
23. Completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") in accordance with *Section 3.3.2, paragraph a*.

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 #30-2025-008-DHB, Vendor's Name, Proposal**) and (e.g. **RFP #30-2025-008-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 #30-2025-008-DHB, Vendor's Name, Proposal 1 of 2**; **RFP #30-2025-008-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 #30-2025-008-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 #30-2025-008-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 – Disclosure Statement* and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed *Attachment I: Financial Review Form*, 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 must employ a robust project management methodology tailored to the scope of work and complexity of the engagement described in the RFP. The Vendor must 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 must describe and provide the project management methodology (agile, or agile-based 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.

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 must 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 must follow the Department's severity, occurrence, and risk score metrics. Reporting of the risks and issues must 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 must be presented through the Vendor's weekly status meeting. As applicable, the risks and issues must be presented through a weekly RAID meeting as well.
    iv. The risks and issues must be reviewed at least weekly to ensure they reflect current status and any changes in mitigation or resolution plans. The Vendor must promptly notify the Department when a threshold is exceeded, or resolution is delayed.
    v. The Vendor must 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 with the State during the DDI/Implementation/Closeout and monthly status meetings during Operations & Maintenance (O&M) Phases of the project. The status meetings will review SLAs, performance, upcoming releases, and planned changes.

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 by the Vendor, 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 REQUEST MANAGEMENT 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 (NSC). 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) calendar days for approval. The Division's assigned project manager will determine the appropriate governance committee and present the CR information.

iv. CR's of an administrative nature 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. All approved CR's will be incorporated into the Contract with a subsequent Amendment.

v. Any new solution scope change from approved CRs, 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

The Medicaid Information Technology Architecture (MITA) is an initiative of the Centers for Medicare & Medicaid Services (CMS). It is intended to foster integrated business and IT transformation across the Medicaid enterprise and to improve the administration of the Medicaid program. The MITA framework has been adopted by the Agency to provide guidance in improving business operations and supporting Information Technology (IT). To advance the alignment of the MITA Maturity Model (MMM), the Agency has developed a Concept of Operations document which describes the operational needs, desires, visions, and expectations of the Medicaid Enterprise Systems. The vendor must support the State's conformance with the MITA Framework and the Seven Standards and achieve Level 3 or higher MITA capability levels.

7.14.4 PERFORMANCE MANAGEMENT

The Vendor is responsible for the performance and quality of all contracted work required by the Contract. NCDHHS 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 standards outlined in the Service Level Agreements (SLAs), NCDHHS 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. Outcomes provided in Table 7.14.6-1 Outcomes and Metrics
c. 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
d. Approval of contract deliverables
e. Review of contract deliverables
f. Operations Reviews
g. Comprehensive Business Reviews
h. 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

The Centers for Medicare and Medicaid Services (CMS) requires that all federally funded Medicaid Enterprise Systems (MES) adhere to federal regulations to achieve CMS certification and thereby qualify for enhanced federal funding participation (FFP). Certification is the procedure by which CMS validates that the MES are designed to support the efficient and effective management of the program and satisfy specific requirements and regulations to achieve enhanced Federal Funding Participation (FFP).

The Department requires each Vendor to adhere to Title 42, Chapter 4, Subpart C of the Code of Federal Regulations and other statutes governing the implementation of Mechanized Claims

Processing and Information Retrieval Systems. The Department and Vendor will leverage the Streamlined Modular Certification for Medicaid Enterprise Systems Certification Guidance for MES IT projects and adopt updates released by CMS upon publication or as advised by the Department.

CMS requires that all federally funded systems regularly report their performance using the CMS-required outcomes and metrics. The Department may add state-specific outcomes for unique circumstances or characteristics not reflected within those metrics.

Failure to meet CMS Certification criteria may result in loss of Federal Funding Participation (FFP). Inadequate performance or non-performance of the required services by the Vendor shall be subject to contractual remedies.

A certifiable system must also meet all applicable standards and conditions, including modularity. Modularity requires acquisition of loosely coupled modules with open, documented interfaces, including COTS solutions. CMS defines a module as a packaged, functional business process or set of processes implemented through software, data, and interoperable interfaces that are enabled through design principles in which functions of a complex system are partitioned into discrete, scalable, and reusable components. The CMS Certification requirements are provided in *Table R14: Certification* requirements.

Table 7.14.6-1 Outcomes and Metrics provides the outcomes and the metrics the Vendor will produce using the CMS Operational Reporting Workbook template. The Operational Reporting Workbook will be updated by the State and Vendor prior to go-live.

Reference #	Outcome	Default Metrics	Regulatory Sources
Outcome 1	The Solution supports various business processes' reporting requirements.	Verify and validate the CMS annual report provisions from 431.428 (1) through 431.428 (11) are met annually.	42 CFR 431.428
Outcome 2	The Solution includes analytical and reporting capabilities to support key policy decision making.	Produce data-driven reporting on transaction data and performance to meet 433.112 (b) (15).	42 CFR 433.112
Outcome 3	The Solution provides federal reporting of Medicaid program expenditures.	% federal reports produced on time for the measurement period, FFY for Medicaid reporting.	N/A
Outcome 4	T-MSIS files are submitted timely and meet the Outcomes Based Assessment (OBA).	% T-MSIS production files submitted to CMS timely and meets the target for OBA.	N/A
Outcome 5	The Solution produces quality performance measurement reports to support managed care.	% managed care data received and usable in the Solution to produce Medicaid quality measures delivered on time for the measurement period.	N/A
Outcome 6	The Solution produces reports on measurable health disparities in our communities.	% health disparities data received and loaded into in the Solution on time during the measurement period.	N/A

Table 7.14.6-1 Outcomes and Metrics

7.14.7 FUNDING TO IMPLEMENT NECESSARY SYSTEM CHANGES (NSC)

The Parties agree that a quantity of hours provided at a specific not-to-exceed cost per year to allow flexibility for implementing necessary system changes. It is an administrative and budgeting estimate for executing work that is not included in the scope of this Contract but is determined by the State as necessary to expand the DAP Solution functionality. During the Operations & Maintenance (O&M) Phase of the Contract, the Contractor shall make one pool of optional additional labor available to the State to implement changes or add functionality to the DAP Solution in ways not specified in this Contract. The State may use these hours to make such changes or additions to the DAP Solution functionality at the State's discretion.

During the O&M phase of the Contract, the Contractor shall perform modifications to the DAP Solution, as requested by the State, such as new features, programs, and services, legislative changes to the extent applicable to the DAP Solution, associated with these modifications. There shall be a set number of hours at fixed labor rates (onsite and offsite) in the Cost Proposal Workbook of an O&M Phase to accommodate such changes. During the O&M Phase, the Vendor shall make available up to the total dollar value of additional labor hours indicated in the line item in the Cost Proposal Workbook for the O&M Phase. At the conclusion of each O&M year, the State may carry forward the unused balance of O&M Phase Modification dollars to the following O&M year to increase the total dollar value of the O&M Phase. Each change or new functionality to the DAP Solution using these hours shall be governed by the processes set form in *Section 7.14.2 Change Request Management Process* of this RFP. Accomplishing approval during a Change Order's Governance stage means that each change must meet the contractual and legal standards, including CMS approvals.

The State shall have no obligation to use any pool labor or to pay the Vendor for non-utilized pool labor. NCDHHS reserves the right to forego resorting to these labor hours, to obtain competitive bids, and to award the work to outside vendors, if NCDHHS is advised or directed to do so by other State or Federal authorities, or if resorting to the Contractor would be unacceptable due to anticipated problems with scheduling, resources, prior performance, and/or excessive estimated costs. For the avoidance of doubt, any changes to the DAP Solution must be performed by the Vendor. Key Personnel costs are not authorized for billing against these labor hours.

The Vendor shall provide a "firm fixed price" for the work; however, if the Parties mutually agree that work on an activity utilizing these labor hours shall be charged on a "time and materials" or "cost not to exceed" basis, the State's payment obligation shall accrue only for hours worked at rates bid by the Vendor. If the State requests in a particular instance that the fee for these labor hours shall be a "firm fixed price" for a result rather than a quantity of labor, that price shall be subject to negotiation.

Regardless of the basis on which the State is charged for activity under these set-aside labor hours, the contractual documentation that authorizes and specifies each change activity may set forth service levels, performance standards and/or deliverables relating to the activity, as well as a percentage of compensation that is to be withheld until such standards are met or such deliverables are provided in acceptable form.

The dollar value for these labor hours is established as a budgeting and administrative convenience to the Parties and shall not be construed as a limitation to the Contractor's obligation under *Attachment B: Department of Information Technology Terms and Conditions, Section 1. Paragraph 40: Unanticipated Tasks"* of this Contract, not to unreasonably refuse amendments to the Contract that may involve additional costs. The amount set aside for these labor hours shall not exceed $800,000 annually.

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 NCDHHS 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 NCDHHS.

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 NCDHHS 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 NCDHHS 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.

7.14.11 CONSULTING SERVICES POOL

The Parties agree that a not-to-exceed cost per year to allow flexibility for providing consulting services. It is an administrative and budgeting estimate for executing work that is within the scope of the Contract for use, as needed, to support advanced analytics and statistical analysis including AI/ML/Gen AI use case development, training and support.

During the O&M Phase, the Vendor shall make available up to the total dollar value of additional labor hours indicated in the Cost Summary line item for Operations and Maintenance - Consulting Services Pool in the Cost Proposal Workbook.

The State shall have no obligation to use any pool labor or to pay the Vendor for non-utilized pool labor. NCDHHS reserves the right to forego resorting to these labor hours, to obtain competitive bids, and to award the work to outside vendors, if NCDHHS is advised or directed to do so by other State or Federal authorities, or if resorting to the Contractor would be unacceptable due to anticipated problems with scheduling, resources, prior performance, and/or excessive estimated costs. Key Personnel costs are not authorized for billing against these labor hours.

The Parties mutually agree that work on an activity utilizing these labor hours shall be charged on a fully burdened hourly rate basis. The State's payment obligation shall accrue only for hours worked at rates provided in the Cost Proposal Workbook referenced in *Attachment E: Cost Form*.

The amount set aside for these labor hours shall not exceed $500,000 annually.

7.15 TECHNICAL OPERATIONS

a. Processes - The Vendor must comply with all NCDHHS 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 processes as described in *Section 7.14.2 Change Request Management Process* of this RFP. 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 NCDHHS 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 processes as described in *Section 7.14.2 Change Request Management Process* of this RFP. 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 and environments 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 *Table 7.17-1 Testing Phases* 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.

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

Testing Phase	Environment	Owner	Description
Unit	Development (DEV)	Vendor	Tests individual components of the software to validate expected behavior.
SIT	Testing (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)	Testing (SIT)	Vendor	Executed to confirm that new configurations and developments do not adversely affect existing system design and functionality.
Performance (includes automated testing)	Pre-Production (PREPROD)	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	Pre-Production (PREPROD)	Vendor and NCDHHS	Performed to uncover vulnerabilities, threats, and risks in the application to prevent system weaknesses and potential loss of sensitive and/or confidential information.
Disaster Recovery	Disaster Recovery / Business Continuity (DR/BC)	Vendor	Verifies that the Department can restore data and applications according to the defined RTO and RPO.
UAT	Pre-Production (PREPROD)	NCDHHS (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)	Production (PROD)	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)	Pre-Production (PREPROD)	Vendor	Validates the successful and accurate transfer of existing production data to the target system, ensuring data integrity and continuation of business operations.
E2E	End to End Testing (E2E)	NCDHHS (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	Pre-Production (PREPROD) / Production (PROD)	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), Annual Penetration Testing, Third Party Security Assessment during O&M to uncover any potential vulnerabilities, threats and risks in the application

Testing Phase	Environment	Owner	Description
			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 Testing Phases

7.18 INCIDENT PRIORITIZATION

For any issues that are encountered whereby an incident is formally submitted during the performance of the operations and maintenance phase of this contract, the incident will be prioritized by the State based on its operational impact, urgency, and context of the issue as provided in *Table 7.18-1 Incident Prioritization Matrix*. The examples provided in the Incident Prioritization Matrix are for reference purposes only. The State reserves the right to assess and assign the priority level for any incident.

Priority Level	Definition	Impact	Examples
P1 – Critical	Complete system outage or security breach with no workaround and no ability to conduct business	Business-critical services are down; Affects all users or critical systems; Regulatory, legal, or safety risk	Data platform down, breach of PHI, Data Ingestion Failure; Critical Data Quality failure
P2 – High	Major functionality impaired; Frequent disruptions to production; workaround exists but is inefficient	Significant user impact; Affects a major component of operations; Involves data integrity or performance degradation	API failure; Data sync errors. Monitoring and Alerting services not working; Power BI reports failure; Substantial query performance degradation
P3 – Medium	Minor functionality issue; workaround available	Moderate user impact; does not block core operations; affects efficiency or usability for some users	Report formatting issues, non-critical alerts, RBAC configuration issues; slow query performance; data sync lag;
P4 – Low	Cosmetic or enhancement request	No operational impact; background or planned task; UI updates, documentation changes, minor enhancements.	Label changes, tooltip updates, UI/UX changes, report updates, user documentation updates.

Table 7.18-1 Incident Prioritization Matrix

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) **ABAC:** Attribute-Based Access Control - A security model that grants access to resources based on policies that evaluate the attributes of the user, the resource, and the environment.

3) **ACID transaction:** A database principle ensuring transactions are Atomic, Consistent, Isolated, and Durable—guaranteeing reliable and secure data operations.

4) **Addressability:** The ability to uniquely identify, locate, and access a data element within the platform through a standardized pointer, identifier, or endpoint.

5) **Agency:** The term "Agency" within this RFP is referring to the North Carolina Department of Health and Human Services (NCDHHS). Synonymous with Department.

6) **Agentic AI:** AI systems capable of autonomous reasoning and multi-step decision-making, acting proactively toward defined goals.

7) **Analyst Workspace:** A dedicated area within the Production environment that enables end users to perform self-service data exploration, reporting, and analytics. It provides read-only access to production data, while allowing read and write access to a separate analyst workspace data lake and data warehouse. Users can load and analyze their own data, develop reports and queries in isolation, and are restricted from writing back or modifying production environments. Promotion workflows are established to move analyst-developed assets to production, pending State review and approval. Additionally, the workspace supports building APIs, FHIR, HL7 interfaces, semantic layers, and data marts to ensure secure and efficient access to curated datasets.

8) **ANSI:** American National Standards Institute - Organization that coordinates the development and use of voluntary consensus standards in the U.S., ensuring products, systems, and processes are safe, reliable, and efficient by accrediting organizations that create these guidelines.

9) **API:** Application Programming Interface - An interface that provides programmatic access to service functionality and data within an application or a database.

10) **AutoML:** Automated Machine Learning - Tools and frameworks that automate the ML model lifecycle, including data preprocessing, feature selection, algorithm selection, and hyperparameter tuning—enabling faster model development with minimal manual coding.

11) **BAA**: Business Associate Agreement, as that term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

12) **BAFO**: Best and Final Offer - Submitted by a Vendor to alter its initial offer, made in response to a request by the issuing agency.

13) **Beneficiary:** An individual eligible to receive services from the North Carolina Department of Health and Human Services, Division of Health Benefits (NC Medicaid).

14) **Best Value:** Has the same meaning as defined in N.C.G.S. 143-135.9.

15) **BI:** Business Intelligence - Tools and processes for analyzing data and presenting insights through dashboards and reports to support decision-making.

16) **BIDP:** Business Intelligence Data Platform – A cloud-based data warehouse system used by NCDHHS to integrate and analyze data sourced from multiple divisions within NCDHHS.

17) **BIA:** Business Impact Analysis - A systematic process to identify and evaluate the effects of business disruptions (e.g., disasters, outages) on critical operations, determining financial/operational impacts,

and prioritizing recovery efforts to create effective Business Continuity Plans and Disaster Recovery Plans.

18) **BIAO:** Business Information Analytics Office – NC Medicaid Business Unit that delivers reports, analytics, and dashboards to internal and external stakeholders.

19) **BPM**: Business Process Modeling is the activity of representing processes of an enterprise so they can be analyzed, improved, and automated.

20) **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 involves 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).

21) **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.

22) **Business Glossary:** A centralized repository that defines key business terms, metrics, and data elements to ensure consistent understanding and usage of data across the organization—linking business definitions to their corresponding technical metadata.

23) **BCP:** Business Continuity Plan - Plan to ensure that business processes continue during a time of emergency or disaster.

24) **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.

25) **CAP**: Corrective Action Plan - A written document describing the deliberate set of actions and steps to be taken by an entity to fix identified problems, errors, or non-compliance issues.

26) **CDC:** Change Data Capture - A method for detecting and capturing changes (inserts, updates, deletes) in source data for real-time or incremental processing.

27) **CDE:** Critical data element - A data element that is essential for business operations, reporting, or compliance, and therefore subject to stricter governance, quality, and stewardship controls to ensure its accuracy and reliability.

28) **Certification Plan**: Plan that defines the Vendor's approach to CMS certification.

29) **Change control process:** A formal process requiring documentation, review, and approval before changes (such as deployments or configuration updates) are moved into production.

30) **Change Management Plan**: Plan defined to manage the changes while executing a project.

31) **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.

32) **Change Request:** Formal proposal for an alteration to some product or system.

33) **CHIP**: Children's Health Insurance Program. Provides low-cost health coverage to children in families that earn too much money to qualify for Medicaid.

34) **CI/CD:** Continuous Integration / Continuous Deployment - A software development practice that automates the process of integrating code changes (CI) and delivering or deploying them to production (CD). Continuous Integration ensures that code changes are automatically tested and merged frequently, while Continuous Delivery/Deployment automates the release process, enabling faster, more reliable updates with minimal manual intervention.

35) **CLI:** Command Line Interface - A text-based interface for executing commands to control or interact with systems and cloud services.

36) **Cloud-Based**: Solution approach 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.

37) **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.

38) **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.

39) **Cognos**: A software application that provides for creating, delivering, and managing interactive reports, dashboards, and analytical content, allowing users to explore data, monitor performance, and make data-driven decisions.

40) **Communication 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.

41) **Completeness Rules:** Data quality checks that ensure all required fields, records, or attributes are present and populated verifying that datasets are not missing critical information needed for accurate analysis or processing.

42) **Contract Effective Date**: The date the Department accepts the Vendor's proposal by signing the RFP Execution Page.

43) **Contractor**: The Vendor awarded the Contract to perform the services and requirements defined therein.

44) **COTS**: Commercial Off the Shelf - A ready-made solution that is adapted to the specific needs of the State's business.

45) **CSV:** Comma-Separated Values - A text-based file format where data is stored in rows separated by commas.

46) **Cybersecurity Incident (N.C.G.S. 143B-1320(4a)):** 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.

47) **DAST:** Dynamic Application Security Testing - A black-box security testing method that analyzes a running application (typically from the outside, without access to source code) to find vulnerabilities by simulating external attacks.

48) **Data Glossary:** See Business Glossary.

49) **Data Landing Area:** The initial storage location where raw, ingested data is first received from source systems before transformations are applied.

50) **Data products:** Curated, reusable datasets or analytical outputs designed, governed, and delivered with a product mindset—including defined ownership, documentation, quality standards, and APIs for easy consumption by other teams or systems.

51) **Data Quality Script:** Proprietary script that detects and remediates data quality issues.

52) **DDI**: Design, Development, and Implementation is a phase in the project cycle.

53) **DED**: Deliverable Expectation Document. Document provides a brief explanation of tasks, activities, and methods to be used to develop the deliverable.

54) **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.

55) **Delta:** A data table stored in Delta Lake format, which supports ACID transactions, versioning, and time travel, enabling reliable data updates and analytics directly on cloud storage.

56) **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.

57) **Dev**: Development, Referring to the Development stage of the Software Development Lifecycle.

58) **DevOps pipeline:** An automated workflow that integrates development, testing, and deployment to deliver code or data changes continuously and reliably.

59) **DevSecOps:** Development, Security, and Operations - a software development approach that integrates security practices into every phase of the DevOps lifecycle, ensuring that security is a shared responsibility from planning through deployment and operations. It is used to automate and embed security controls without slowing down development or delivery.

60) **DHB**: Division of Health Benefits. The division within the NCDHHS responsible for implementing Medicaid transformation and administering the transformed Medicaid program.

61) **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.

62) **DLP**: Data Loss Prevention – A security strategy and set of tools that identifies, monitors, and protects sensitive data from unauthorized use, transfer, or disclosure.

63) **DMH:** Division of Mental Health. The division within NCDHHS that provides quality support to achieve self-determination for individuals with intellectual and/or developmental disabilities and quality services to promote treatment and recovery for individuals with mental illness and substance use disorders.

64) **DPH:** Division of Public Health - The division within the NCDHHS responsible for promoting disease prevention, health services and health promotion programs that protect communities from communicable diseases, epidemics, and contaminated food and water.

65) **DQ:** Data quality - The measure of data's condition based on factors such as accuracy, completeness, consistency, reliability, and timeliness.

66) **DRP:** Disaster Recovery Plan - A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

67) **E2E:** End-to-End - Can refer to a testing methodology or a comprehensive solution. It can encapsulate testing of an application from start to finish or a product / service that handles a process from beginning to end.

68) **Encounters:** Medical information submitted by health care providers (physicians, hospitals, Ancillaries, etc.) which document both the clinical conditions, services, and items delivered to the member to treat their conditions.

69) **Encryption at rest:** The process of encrypting data stored on storage medium to protect it from unauthorized access when not actively being used or transmitted.

70) **Encryption in transit:** The practice of encrypting data while it is being transmitted over a network (e.g., between client and server) to prevent interception or tampering during transfer.

71) **Enterprise Architecture:** Conceptual blueprint that defines the structure and operation of an organization; governs data strategy, models, and management; maps out software systems and their interactions; and details the underlying hardware and network infrastructure.

72) **ETL:** Extract, Transform, Load - A data integration process where data is extracted from sources, transformed, and then loaded into a target system (e.g., warehouse).

73) **Feature store:** A centralized repository for storing, managing, and serving ML features consistently across training and inference environments.

74) **Federated identities:** A single sign-on (SSO) and identity federation capability that lets users authenticate across multiple systems or domains using a common identity provider (e.g., Azure AD, Okta). It ensures consistent access control and auditing across hybrid or multi-cloud environments.

75) **FFP:** Federal Financial Participation - The Federal Government's share of a State's expenditures under the Medicaid program.

76) **FinOps:** A cloud financial management practice that combines finance, operations, and engineering to optimize cloud cost efficiency and accountability.

77) **GenAI:** Generative AI - The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

78) **GitHub:** A cloud-based platform for source control and collaboration, using Git to track and manage code changes.

79) **GitHub Actions:** A CI/CD automation feature in GitHub that builds, tests, and deploys code based on defined workflows.

80) **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).

81) **GraphQL:** An API query language that lets clients request exactly the data they need from multiple resources in a single call.

82) **HEDIS**: Healthcare Effectiveness Data and Information Set developed and maintained by the NCQA. HEDIS reporting is a requirement of health plans by NCQA and the Centers for Medicare and Medicaid Services (CMS) for use in health plan accreditation, Star Ratings, and regulatory compliance.

83) **HIPAA**: Health Insurance Portability and Accountability Act of 1996, as amended and its promulgating regulations.

84) **HITECH:** Health Information Technology for Economic and Clinical Health Act.

85) **HL7:** Health Level Seven - A standard for exchanging healthcare data between systems such as Electronic Health Records, labs, and payers.

86) **HL7 FHIR: Fast** Healthcare Interoperability Resources - A modern health data exchange standard by HL7 that uses RESTful APIs and JSON/XML formats to enable seamless, secure interoperability between healthcare systems.

87) **IaC:** Infrastructure as code - A practice in IT operations where infrastructure (such as servers, networks, and configurations) is provisioned and managed using machine-readable code, enabling automation, consistency, and version control.

88) **IAM:** Identity and Access Management - A framework of policies, technologies, and processes that ensures the right individuals have appropriate access to technology resources, managing user identities and controlling access to systems and data securely.

89) **IAST:** Interactive Application Security Testing - Combines elements of both SAST and DAST by analyzing applications from within during runtime.

90) **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.

91) **Implementation Schedule:** Comprehensive list of milestones, deliverables, and tasks along with the associated due dates, durations and resources required for implementation.

92) **IMS:** Integrated Master Schedule

93) **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.

94) **Infrastructure Drift:** When the actual state of cloud or system infrastructure deviates from its defined configuration in code (IaC) due to manual changes or untracked updates.

95) **Integration pattern:** A reusable design approach that defines how different systems or components communicate and exchange data within an IT environment to help standardize and streamline system interactions.

96) **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.

97) **ISDM:** Information Systems Development Methodology - A structured framework of procedures, techniques, tools, and documentation that guides teams through planning, designing, building, testing, and maintaining information systems.

98) **ITD:** Information Technology Division of the NC Department of Health and Human Services

99) **ITSM:** Information Technology Service Management - The processes used to manage IT services within an organization.

100) **JSON:** JavaScript Object Notation - A lightweight, human-readable data format for storing and exchanging structured or semi-structured data.

101) **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.

102) **LLM:** Large Language Model - An AI model trained on massive text datasets that can understand, generate, and reason with human language.

103) **LME/MCO**: Local Management Entity/Managed Care Organization - A local management entity that is under contract with the Department to operate the combined Medicaid Waiver program authorized under Section 1915(b) and NC General Statutes - Chapter 122C 8 Section 1915(c) of the Social Security Act or to operate a capitated PHP contract under Article 4 of Chapter 108D of the General Statutes.

104) **Low-Latency Ingestion:** The ability to capture, process, and make data available for analysis almost immediately after it is generated—typically within milliseconds to a few seconds.

105) **Managed Compute:** Cloud-provided, automatically scaled compute resources (e.g., virtual warehouses, clusters) that handle processing without requiring users to manage infrastructure or scaling manually.

106) **MCOs:** Managed Care Organizations - Federal regulation 42 CFR 438.2 defines MCO as an entity that has, or is seeking to qualify for, a comprehensive risk contract under this part, and that is:

(1) A Federally qualified HMO that meets the advance directives requirements of subpart I of part 489 of this chapter; or

(2) Any public or private entity that meets the advance directives requirements and is determined by the Secretary to also meet the following conditions:

(i) Makes the services it provides to its Medicaid enrollees as accessible (in terms of timeliness, amount, duration, and scope) as those services are to other Medicaid beneficiaries within the area served by the entity.

(ii) Meets the solvency standards of § 438.116.

107) **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.

108) **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.

109) **MES PMO**: Technology Program Management Organization comprised of the engineers, architects, specialists, analysts, project managers, program managers, and the Program Director for the MES project.

110) **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.

111) **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.

112) **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.

113) **ML Pipeline:** An automated workflow that handles the stages of machine learning—data preparation, training, validation, deployment, and monitoring—within a reproducible, scalable framework.

114) **ML/AI:** Machine Learning. Artificial Intelligence.

115) **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.

116) **N.C.G.S.:** North Carolina General Statutes

117) **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 .

118) **NCAC**: North Carolina Administrative Code

119) **NCDIT or DIT**: The NC Department of Information Technology, formerly Office of Information Technology Services.

120) **NCID**: 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.

121) **NCQA:** National Committee for Quality Assurance - An organization that accredits and measures healthcare quality, including HEDIS performance.

122) **NIST:** National Institute of Standards and Technology.

123) **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.

124) **OBA:** Outcomes Based Assessment (OBA) - A data quality evaluation framework used by CMS to assess the timeliness, completeness, and accuracy of Medicaid data submitted through T-MSIS.

125) **ODS:** Operational Data Store - A centralized, integrated database that stores near–real-time operational data from multiple systems to support reporting and short-term analytics.

126) **ORC:** Optimized Row Columnar – A columnar file format used in Hadoop and Spark for efficient storage and high-performance read operations.

127) **ORR:** Operational Readiness Review - A formal assessment ensuring IT systems are fully prepared, compliant, and capable of stable production operations before launch, involving independent auditors, detailed documentation, and testing against standards for security, privacy, and consumer communication.

128) **ORH:** Office of Rural Health – The division in the Department that assists underserved communities by providing support to improve health care access, quality, and cost-effectiveness.

129) **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.

130) **OWASP TOP 10:** A widely recognized standard that ranks the ten most critical web application security risks, published by the Open Web Application Security Project (OWASP). It serves as a baseline checklist for identifying, preventing, and remediating common vulnerabilities in modern applications.

131) **Parquet:** A columnar storage format optimized for efficient querying and compression in big data systems.

132) **PCDU:** PHP Contractual Data Utility: State system designed to receive and manage contractual deliverables and reports from state vendors. Reports received and flagged for data quality reviews and report ingestion are ingested within the Data Analytics Platform. The PCDU is built on an AWS Platform leveraging S3 for file storage.

133) **PHI:** Protected Health Information, as defined in HIPAA.

134) **PHP:** Prepaid Health Plan as defined in Session Law 2015-245, as amended.

135) **PII:** Personally Identifiable Information - Information that can identify an individual, such as name, address, SSN, or email.

136) **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.

137) **Proposal:** The response to the RFP solicitation submitted to NCDHHS by the Vendor. This is also referred to as the Response or Offer.

138) **Provider:** The general term used to refer to individual practitioners and facilities, entities, organizations, and atypical organizations or institutions.

139) **PySpark:** The Python API for Apache Spark, enabling large-scale distributed data processing and analytics.

140) **Quality Management Plan**: Describes how quality will be managed throughout the lifecycle of the project.

141) **RAG:** Retrieval-Augmented Generation - Technique for building AI applications that provide accurate, context-aware responses based on specific or proprietary data. Used to enhance AI accuracy and prevent hallucinations.

142) **RASP**: Runtime Application Self-Protection – A security technology that is integrated into an application or its runtime environment. It continuously monitors the application's behavior and context during execution and can detect and block attacks in real time.

143) **RBAC:** Role-Based Access Control - Restricts network access based on a user's role within an organization.

144) **RCA**: Root Cause Analysis.

145) **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.

146) **Reasonable, Necessary, or Proper**: as used herein shall be interpreted solely by the State of North Carolina.

147) **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.

148) **Release Management Plan**: Managing, planning, scheduling and controlling a software build through different stages and environments; including testing and deploying software releases.

149) **REST API:** Representational State Transfer API - A standard web interface that allows systems to communicate using HTTP methods (GET, POST, PUT, DELETE).

150) **REST/JSON:** A common web API architecture (REST) that exchanges data in lightweight, human-readable JSON format, enabling fast, scalable system integrations.

151) **RFP:** Request for Proposal - A formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. This document contains requirements and specifications of the RFP, instructions to Offerors and the standard IT Terms and Conditions for Goods and Related Services. This document is used as the foundation for the contract to be awarded.

152) **RPO**: Recovery Point Objective – The maximum acceptable amount of data loss the Department can tolerate after a disruptive event, measured in time.

153) **RTM**: Requirements Traceability Matrix - Document that contains a matrix which shows bi-directional traceability with applicable testable and non-testable contractual requirements and their realization throughout all project phases.

154) **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.

155) **SaaS**: Software as a Service. A software delivery and licensing model, in which software is accessed online via a subscription, rather than bought and installed on individual servers and computers.

156) **SAS Analytics**: Statistical Analytics System – Comprehensive software suite for data management, advanced analytics, business intelligence, and AI.

157) **SAST**: Static Application Security Testing - A white-box security testing method that analyzes source code, bytecode, or binary code for vulnerabilities without executing the program.

158) **Scoped API tokens:** Access credentials that grant only limited, predefined permissions to specific data or actions, enforcing the principle of least privilege.

159) **SDK:** Software Development Kit - A set of tools, libraries, and documentation developers use to build applications for a specific platform or service.

160) **SDLC:** System Development Life Cycle. A project management model that outlines the phases required to build an IT system.

161) **Semi-structured data:** Data with some organizational structure (e.g., JSON, XML, log files) but not strictly tabular, allowing flexible schema and metadata tagging.

162) **Seven Standards and Conditions:** Centers for Medicare & Medicaid Services issued standards and conditions that must be met by the States if they have to be eligible for Medicaid technology investments, if they are to be eligible for the enhanced match funding. These standards and conditions have been issued under sections 1903(a) (3) (A) (i) and 1903(a) (3) (B) of the Social Security Act. Sections include modularity, MITA, industry standards, leverage, business results, reporting, and interoperability.

163) **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

164) **SIEM:** Security Information and Event Management

165) **Signed URLs:** Time-limited, cryptographically signed links that grant controlled access to specific cloud resources (e.g., files, datasets) without exposing permanent credentials.

166) **(Significant) Security Incident (N.C.G.S. 143B-1320(16a)):** 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 have a high or medium functional impact to the mission of an agency.

167) **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.

168) **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.

169) **SMC**: Streamlined Modular Certification is CMS's methodology of Medicaid Enterprise System certification based on the combination of developing outcomes statements and evaluation criteria, identifying test cases for system demonstrations, and collecting and assessing operational data.

170) **SOC 2:** A compliance framework that ensures a service provider securely manages customer data based on five trust principles — security, availability, processing integrity, confidentiality, and privacy.

171) **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.

172) **SPOC**: Single Point of Contact. A person serving as a coordinator or the focal point of information.

173) **Storage zone:** A logical area in a data lake or platform (e.g., raw, curated, semantic) used to organize data by processing stage or purpose.

174) **Structured data:** Data organized in fixed fields and formats (e.g., tables, databases) that can be easily queried using SQL or similar tools.

175) **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.

176) **SURS:** Surveillance and Utilization Review System - A federally mandated Medicaid program component used to detect, monitor, and investigate potential fraud, waste, and abuse in provider and member activities by analyzing claims and utilization data.

177) **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.

178) **Tableau**: Visual analytics platform that assists users and organizations visualize, understand, and use data to solve problems, primarily by transforming complex data into interactive and easy-to-understand charts, graphs, maps, and dashboards.

179) **Tech Ops**: NCDHHS Technical Operations team.

180) **Time travel:** A feature (e.g., in Delta Lake) that allows querying or restoring data as it existed at a specific point in time.

181) **T-MSIS:** Transformed Medicaid Statistical Information System - A federal CMS data platform that collects and standardizes detailed Medicaid and CHIP program data from all states to support oversight, policy analysis, and program integrity.

182) **Training Plan**: Identifies the training that Vendor is expected to complete over a stated period of time.

183) **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.

184) **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.

185) **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.

186) **Unit Testing**: The lowest testing level, which is used by developers to verify that the implemented code functions as expected.

187) **Unstructured data:** Data that lacks a predefined format or model (e.g., documents, images, emails, videos), requiring specialized tools for processing and analysis.

188) **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.

189) **VRAR:** Vendor Readiness Assessment, 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.

190) **WCAG:** Web Content Accessibility Guidelines - International technical standards from the World Wide Web Consortium that provide a unified framework for making digital content (websites, apps) accessible to people with disabilities.

191) **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.

192) **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.

193) **X12:** ANSI X12 - A data exchange standard widely used in healthcare and insurance for electronic data interchange (EDI) transactions such as claims, eligibility, and payments.

194) **XML:** Extensible Markup Language - A hierarchical text format used for storing and transporting structured data across systems.

195) **YAML:** A human-readable configuration format commonly used for defining pipelines, workflows, and deployment settings.

196) **Zero Copy Data Sharing:** A method of sharing live data between platforms or accounts without physically copying or moving it. Instead, access is granted at the storage or metadata layer, enabling real-time, secure sharing while maintaining a single source of truth and reducing storage and latency costs.

197) **ZCC:** Zero Count Check – A validation step that verifies whether any records (rows) have been ingested from a source file, table, or data stream. If the count of ingested records is zero, the check triggers an alert or error, indicating a potential problem with the data pipeline, source system, or upstream process.

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 meetings rescheduled by the Department, 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, 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, (not withstanding 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) <u>WARRANTY TERMS</u>: 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) <u>RESTRICTIONS</u>: 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) <u>SUPPORT OR MAINTENANCE SERVICES</u>: 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) <u>STATE PROPERTY AND INTANGIBLES RIGHTS:</u> 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 (Only Applies to Proposed SaaS Solutions)

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:

c) 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.

d) 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) PEFORMANCE 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 that 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) <u>ACCEPTANCE CRITERIA:</u> See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 9: Acceptance Process

17) <u>CONFIDENTIALITY:</u> See Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 18: Confidentiality

18) <u>SECURITY OF STATE DATA</u>:

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. § 75-60*ff*) 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: NCDHHS 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, 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 Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph 18, TERMINATION. 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 AGEEMENT 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 Z: 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 NCDHHS 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 NCDHHS 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 NCDHHS Inspector General determine that there is a reasonable possibility of fraud or similar risk, the State, CMS or the NCDHHS 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 in Attachment E: Cost Form 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: NCDHHS 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 polices 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)
- NCDHHS Privacy and Security Policies (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/departmental/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), 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).

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). 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=).

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)
- 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) 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) 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 1st 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. The Vendor must provide its total all inclusive, turnkey costs associated with the solution and services outlined in this RFP, including all direct and indirect costs. The total proposed price is made up of data from the following worksheets in the Cost Proposal Workbook: worksheet 2. DDI Milestone Costs, worksheet 3. DDI Run Rate Costs, worksheet 4. O&M Deliverable Costs, worksheet 5. O&M Run Rate Costs, worksheet 6. Software Related Costs, and worksheet 7. Variable Use Costs. Vendors must also supply supporting information in worksheet 8. Software Cost Details, worksheet 9. Key Personnel Labor Rates, worksheet 10. Consulting Labor Rates, and worksheet 11. Basis of Estimates, 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.

All variable and fixed costs for Design, Development, and Implementation (DDI) and Operations & Maintenance (O&M) must be entered only once in the respective worksheets of the Cost Proposal Workbook. Do not duplicate or allocate the same costs across multiple worksheets, as this will result in double counting. Each cost element should appear in its designated worksheet to ensure accuracy and compliance with the pricing structure.

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

Summary of eleven (11) worksheets included in the Cost Proposal Workbook.

0. Instructions - provides a description of the worksheets and general instructions.
1. Cost Summary – provides a summary of all costs inclusive of Implementation (DDI) and Operations and Maintenance (O&M).
2. DDI Milestone Costs – provides the costs associated with developing deliverables and attaining milestones during the DDI stage of the project. These costs must not include the DDI Run Rate costs provided in worksheet *3. DDI Run Rate Costs*. The Vendor must provide the costs associated with producing deliverables and achieving each project milestones in the contract year that the milestone is anticipated to be achieved.
3. DDI Run Rate Costs – provides the costs associated with run rate costs during the DDI stage. These costs must not include the costs associated with labor and resources used to attain the milestones in worksheet *2. DDI Milestone Costs* or the software related costs incurred during the DDI stage.
4. O&M Deliverable Costs – provides the costs associated with developing Deliverables during O&M. These costs must not include the O&M Run Rate costs provided in worksheet *5. O&M Run Rate Costs.*
5. O&M Run Rate Costs – provides the costs associated with run rate costs during O&M. These costs do not include the costs associated with labor and resources used to attain the deliverables in worksheet *4. O&M Deliverable Costs* or the software related costs incurred during the O&M stage of the project.
6. Software Related Costs – provides the annual software costs for the ongoing maintenance, services, support, and cloud hosting necessary to provide the Solution and services outlined in the RFP.
7. Estimated Variable Use Costs – provides the total estimated not-to-exceed variable use costs inclusive of such costs as usage-based charges for data storage growth, backups, geo-redundancy, compute consumption, scaling costs, and outbound data transfers.
8. Software Costs Details – provides cost details for each Software line item listed in worksheet *6. Software Related Costs*. This worksheet includes such costs as software licensing, maintenance, and hosting fees at a software application level.

9. Key Personnel Labor Rates – provides fully burdened off-site hourly labor rates for all key personnel and the percentage allocation to the project for all Key Personnel.
10. Consulting Labor Rates – provides fully burdened off-site hourly labor rates for all labor categories of consulting services that may be used during O&M. The consulting labor rates contained in this worksheet apply only to the Consulting Services as defined in *Sections 3.1.8 Consulting Services and 7.14.11 Consulting Services Pool.*
11. Basis of Estimates – provides any basis of estimates and assumptions how costs were developed that enables the State to have a full understanding of the Vendor's pricing methodology.

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 *11. 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 (including Software Related costs and Variable Use 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.

No payments will be made for items not quoted in the Vendor’s Cost Proposal Workbook. 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.

Note: The screen images in the following pages are captured from the worksheets contained in the Cost Proposal Workbook and are provided as a visual reference only; some worksheets are not shown in their entirety. The Cost Proposal Workbook must be completed and submitted in Excel format.

Notes	
The Vendor 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. DDI Milestone Costs, 3. DDI Run Rate Costs, 4. O&M Deliverable Costs, 5. O&M Run Rate Costs, 6. Software Related Costs, and 7. Estimated Variable Use Costs. Vendors must also supply supporting information in Sheet 8. Software Cost Details, Sheet 9. Key Personnel Labor Rates, Sheet 10. Consulting Labor Rates, and Sheet 11. Basis of Estimates, 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. In addition to the items below, the State expects Vendor to review the Cost Proposal Workbook Instructions in the **Attachment E: Cost Form in the RFP.** The Vendor must not modify formulas in this workbook. It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.	
Data Analytics Platform	
0. Instructions	
Vendor Name:	*<Vendor Name>*
Worksheet Title	**Instructions**
1. Cost Summary	The Cost Summary tab will automatically calculate the Vendor's Total Proposed Price using prices entered by the Vendor in Worksheets 2. DDI Milestone Costs, 3. DDI Run Rate Costs, 4. O&M Deliverable Costs, 5. O&M Run Rate Costs, 6. Software Related Costs, and 7. Variable Use Costs.
2. DDI Milestone Costs	The Vendor must provide the costs associated with developing Deliverables and attaining milestones during the DDI stage of the project. These costs must not include the DDI Run Rate costs provided in worksheet 3. DDI Run Rate Costs.
3. DDI Run Rates Costs	The Vendor must provide the costs associated with run rate costs during the DDI stage of the project. These costs must not include the costs associated with labor and resources used to attain the milestones in the worksheet 2. DDI Milestone Costs or the software related costs incurred during the DDI stage of the project.
4. O&M Deliverable Costs	The Vendor must provide the costs associated with developing Deliverables during the O&M stage of the project. These costs must not include the O&M Run Rate costs provided in the worksheet 5.O&M Run Rate Costs.
5. O&M Run Rate Costs	The Vendor must provide the costs associated with run rate costs during the O&M stage of the project. These costs must not include the costs associated with labor and resources used to attain the deliverables in the worksheet 4. O&M Deliverable Costs or the software related costs incurred during the O&M stage of the project.
6. Software Related Costs	The Vendor must provide the annual software costs for the ongoing maintenance, services, support, and cloud hosting necessary to provide the Solution and services outlined in the RFP. The Vendor may provide any additional third party software applications that support the Solution and are not included in the Software list in this worksheet. Any software costs provided in this worksheet must not be included in any costs, in this Cost Proposal Workbook, that are associated with the costs for DDI Milestones, DDI Run Rates, O&M Deliverables, O&M Run Rate, or Variable Use costs.
7. Estimated Variable Use Costs	The Vendor must provide the total estimated variable not-to-exceed use costs inclusive of such costs as usage-based charges for obect storage, backups, geo-redundancy, compute consumption, scaling costs, and data transfers. Any variable costs provided in this worksheet must not be included in any costs, in this Cost Proposal Workbook, that are associated with the fixed costs provided for DDI Milestones, DDI Run Rates, O&M Deliverables, O&M Run Rate, or Software Related costs.
8. Software Cost Details	The Vendor must provide cost details for each Software line item listed in the worksheet 6. Software Related Costs. This worksheet includes such costs as software licensing, maintenance, and hosting fees at a software application level. The information provided in this worksheet is for information purposes and is not included in the worksheet 1. Cost Summary.
9. Key Personnel Labor Rates	The Vendor must provide fully burdened hourly labor rates for all key personnel and the percentage allocation to the project for all Key Personnel. The information provided in this worksheet is for information purposes and is not included in the worksheet 1. Cost Summary.
10. Consulting Labor Rates	The Vendor must provided fully burdened hourly labor rates for all labor categories of consulting services that may be used in the O&M stage of the project. The information provided in this worksheet is for information purposes and is not included in the worksheet 1. Cost Summary.
11. Basis of Estimates	The Vendor must provide any basis of estimates and assumptions how costs were developed that enables the State to have a full understanding of the Vendor's pricing methodology.

0. Instructions

Notes
The Total Proposed Costs on this worksheet will be automatically calculated using the totals of costs entered in worksheets 2. DDI Milestone Costs, 3. DDI Run Rate Costs, 4. O&M Deliverable Costs, 5. O&M Run Rate Costs, 6. Software Related Costs, and 7. Estimated Variable Use Costs. The Necessary System Change (NSC) Costs provided in the table below are predetermined by the Department and are a specific not-to-exceed cost per year to allow flexibility for implementing necessary system changes. Do not modify these NSC Cost entries. See Section 7.14.7 for more information on NSC Costs. The Consulting Labor Costs provided in the table below are predetermined by the Department and are a specific not-to-exceed cost per year. Do not modify these Consulting Labor Costs entries. See Section 7.14.11 for more information on the Consulting Services Pool. It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.

Data Analytics Platform

1. Cost Summary

Vendor Name: *<Vendor 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 - Milestone Costs	$0.00	$0.00	$0.00					**$0.00**
Implementation - Run Rate Costs	$0.00	$0.00	$0.00					**$0.00**
Implementation - Software Related Costs	$0.00	$0.00	$0.00					**$0.00**
Implementation - Estimated Variable Use Costs	$0.00	$0.00	$0.00					**$0.00**
Operations and Maintenance - Deliverables Costs			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Operations and Maintenance - Run Rate Costs			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Operations and Maintenance - Software Related Costs			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Operations and Maintenance - Estimated Variable Use Costs			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Operations and Maintenance - NSC Costs			$800,000.00	$800,000.00	$800,000.00	$800,000.00	$800,000.00	**$4,000,000.00**
Operations and Maintenance - Consulting Labor Costs			$500,000.00	$500,000.00	$500,000.00	$500,000.00	$500,000.00	**$2,500,000.00**
Total Costs:	**$0.00**	**$0.00**	**$1,300,000.00**	**$1,300,000.00**	**$1,300,000.00**	**$1,300,000.00**	**$1,300,000.00**	**$6,500,000.00**

1. Cost Summary

Notes
The costs provided in this worksheet will be automatically updated in the 1. Cost Summary worksheet. For each milestone listed in this worksheet, the milestone's scope, acceptance criteria, deliverables and prior deliverables are provided in Attachment N: Deliverables and Milestones. Please enter the costs associated with producing deliverables and achieving each project milestones in the Contract Year that the milestone is anticipated to be achieved. These milestone costs occur only during the DDI phase of the project. **Any costs associated with Key Personnel and support staff utilized to produce deliverables and achieve the project milestones entered in this sheet must not be included in the run rate costs as provided in the worksheet 3. DDI Run Rate Costs.** It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.

Data Analytics Platform

2. DDI Milestone Costs

Vendor Name: *<Vendor Name>*

ID	Milestone	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2
1	Planning & Discovery Complete	$0.00	$0.00	$0.00				
2	Infrastructure - Design and Approvals Complete	$0.00	$0.00	$0.00				
3	Infrastructure - Capabilities Enablement - Foundational Capabilities (Data warehouse, Audit, security, data management, integration, ingestion and consumption, tools, advanced analytics) Set up	$0.00	$0.00	$0.00				
4	Infrastructure - Capabilities Enablement - Disaster Recovery Set up	$0.00	$0.00	$0.00				
5	Infrastructure - Capabilities Enablement - DevOps Set up	$0.00	$0.00	$0.00				
6	Migration - Data Model Design Complete	$0.00	$0.00	$0.00				
7	Migration - New Data Products Design Complete	$0.00	$0.00	$0.00				
8	Testing - Security and Penetration Testing Complete	$0.00	$0.00	$0.00				
9	Infrastructure - Capabilities Enablement - DAP ready for Data	$0.00	$0.00	$0.00				
10	Infrastructure - Capabilities Enablement - Data Observability Set up	$0.00	$0.00	$0.00				
11	Infrastructure - Capabilities Enablement - Data Governance Tool Set up	$0.00	$0.00	$0.00				
12	Infrastructure - Capabilities Enablement - Infrastructure as Code Set up	$0.00	$0.00	$0.00				
13	Infrastructure - Capabilities Enablement - Automated Testing Set Up	$0.00	$0.00	$0.00				
14	Infrastructure - Capabilities Enablement - ODS Set Up	$0.00	$0.00	$0.00				
15	Infrastructure - Capabilities Enablement - Complete	$0.00	$0.00	$0.00				
16	Migration - Data Integration from Source to Bronze Layer Complete	$0.00	$0.00	$0.00				
17	Migration - Data Pipelines from Bronze to Silver Layer Complete	$0.00	$0.00	$0.00				
18	Migration - Existing Data Products Migration and New Data Products Development Complete into Gold Layer	$0.00	$0.00	$0.00				

2. DDI Milestone Costs

Notes
The costs provided in this worksheet will be automatically updated in the 1. Cost Summary worksheet. DDI Run Rate costs refer to the ongoing expenses for support and services provided during the Design, Development, and Implementation (DDI) phase that are not directly associated with the creation of deliverables or the attainment of project milestones. These costs typically include activities such as: Operational Support, Administrative Services, Technical Assistance, Knowledge Transfer, Governance and Oversight. **Any costs provided in this worksheet must not be included in any costs associated with a) the development of deliverables and attainment of milestones as provided in the worksheet 2. DDI Milestone Costs or b) the Software related costs as provided in the worksheet 6. Software Related Costs.** It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.

Data Analytics Platform

3. DDI Run Rate Costs

Vendor Name: *<Vendor 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
Non-Milestone Related Services and Support	$0.00	$0.00	$0.00					$0.00
	$0.00	$0.00	$0.00					$0.00
	$0.00	$0.00	$0.00					$0.00
Total DDI Run Rate Costs:	**$0.00**	**$0.00**	**$0.00**					**$0.00**

3. DDI Run Rate Costs

Notes
The costs provided in this worksheet will be automatically updated in the 1. Cost Summary worksheet. For each deliverable listed in this worksheet, the deliverable description and frequency is provided in Attachment N: Deliverables and Milestones. Please enter the costs associated with producing the deliverables for each Contract Year that the deliverable is to be provided. **Any costs associated with Key Personnel and support staff utilized to produce the deliverables entered in this sheet must not be included in the run rate costs as provided in the worksheet 5. O&M Run Rate Costs.** It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.

Data Analytics Platform

4. O&M Deliverable Costs

Vendor Name: *<Vendor Name>*

Deliverable ID	Deliverable Name	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	Total Costs
DAP-DEL-DMD-001	Data Pipelines Documentation	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
DAP-DEL-MMM-001	Monthly Observability Summary	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-AI-02	GenAI Disclosure and Fact Sheet	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-001	Data Architecture	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-002	Data Architecture Document - Conceptual Data Model (CDM)	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-003	Data Architecture Document - Data Dictionary (Electronic)	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-004	Data Architecture Document - Logical Data Model (LDM)	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-006	Configuration/Customization Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-010	System Design Document (SDD)	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-ARCH-012	Section 508 Compliance Test Report	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-CERT-002	CMS Operational Report Workbook	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-OM-001	Operations, Maintenance, and Configuration Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-OM-002	Capacity Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-OM-004	Operations Procedure Manual	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-OM-006	Turnover Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-001	System Security Plan (SSP)	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-002	Privacy & Security Incident Management Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-003	Business Continuity Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-004	Disaster Recovery Plan	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-005	Privacy Impact Analysis	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-006	3rd Party Privacy Security Assessment	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-007	Disaster Recovery/Business Continuity Test Report	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
MES-DEL-SEC-008	Penetration Test Report	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**

4. O&M Deliverable Costs

Notes
The costs provided in this worksheet will be automatically updated in the 1. Cost Summary worksheet. O&M Run Rate costs refer to the ongoing fixed expenses for support and services provided during the Operations and Maintenance (O&M) phase that are not directly associated with the creation of deliverables. These fixed costs typically include activities such as: Operational Support, System Monitoring, Routine Maintenance, Help Desk and End-User Support, Operational Oversight, Knowledge Transfer and Training. **Any costs provided in this worksheet must not be included in any costs associated with a) the development of deliverables as provided in the worksheet 4. O&M Deliverable Costs or b) the Software related costs as provided in the worksheet 6. Software Related Costs.** It is the responsibility of the Vendor to ensure spreadsheet calculations are correct.

Data Analytics Platform

5. O&M Run Rate Costs

Vendor Name: *<Vendor Name>*

Description	Contract Year 1	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Option Year 1	Option Year 2	Total Costs
Non-Deliverable Related Services and Support			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
			$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
Total O&M Run Rate Costs:			**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**

5. O&M Run Rate Costs

Notes

The costs on this worksheet will be automatically updated in the 1. Cost Summary sheet. Enter the total annual software costs and fees inclusive of such costs as Licensing Fees, Maintenance Fees, Hosting Fees, and any other fees for the software. The Vendor may enter additional software applications not listed in the Software column and provide annual software costs. The software cost details will be provided in the 8. Software Cost Details worksheet in this workbook.

Any software costs provided in this worksheet must not be included in any costs, in this Cost Proposal Workbook, that are associated with the costs for DDI Milestones, DDI Run Rates, O&M Deliverables, O&M Run Rate, or Variable Use costs.

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

Data Analytics Platform

6. Software Related Costs

Vendor Name: *<Vendor Name>*

ID	Software	Contract Year 1 - DDI	Contract Year 2 - DDI	Contract Year 3 - DDI	Contract Year 3 - O&M	Contract Year 4 - O&M	Contract Year 5 - O&M	Option Year 1 - O&M	Option Year 2 - O&M	Total Costs
1	Cloud Hosting	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
2	Data Platform	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
3	Power BI	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
4	SURS Application	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
5	SAS Enterprise Guide	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
6	Other Third Party Software Application 1	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
7	Other Third Party Software Application 2	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
8	Other Third Party Software Application 3	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
9	Other Third Party Software Application n	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
10		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
11		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
12		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
	Total Software Related Costs	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**

6. Software Related Costs

Notes

The estimated, not-to-exceed costs on this worksheet will be automatically updated in the 1. Cost Summary sheet. Enter the estimated, not-to-exceed variable use costs inclusive of such costs as usage-based charges for data storage growth, backups, geo-redundancy, compute consumption, scaling costs, and outbound data transfers. The Vendor may enter other use costs not listed in the Category column and provide the annual use costs.

Any estimated variable costs provided in this worksheet must not be included in any costs, in this Cost Proposal Workbook, that are associated with the fixed costs for DDI Milestones, DDI Run Rates, O&M Deliverables, O&M Run Rate, or Software Related costs.

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

Data Analytics Platform

6. Software Related Costs

Vendor Name: *<Vendor Name>*

ID	Category	Contract Year 1 - DDI	Contract Year 2 - DDI	Contract Year 3 - DDI	Contract Year 3 - O&M	Contract Year 4 - O&M	Contract Year 5 - O&M	Option Year 1 - O&M	Option Year 2 - O&M	Total Costs
1	Data Storage	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
2	Compute / Infrastructure Services	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
3	Data Egress	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
4		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
5		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
6		$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.00**
	Total Variable Use Related Costs	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**

7. Estimate Variable Use Costs

Notes

The information in this worksheet provides the detailed cost breakdown of the software applications listed in the worksheet 6. Software Related Costs in this workbook. Any applicable fees must be included for each contract year. Please provide a reference to the Software ID and Software information provided in the worksheet 6. Software Related Costs in the Software ID and Software columns in this worksheet. A software ID may be referenced more than once if multiple applications, services, or tools comprise the referenced software.

The information in this worksheet is for informational purposes only and will not be updated in either the worksheet 1.Cost Summary worksheet or the worksheet 6. Software Related Costs.

Data Analytics Platform

7. Software Cost Details

Vendor Name: *<Vendor Name>*

Application Detail							Contract Year 1 - DDI				
Software ID	Software	Software Application Name	Description of Functionality Provided	# of Licenses Provided	Perpetual or Subscription?	Comments	Total License Fees	Total Maintenance Fees	Total Hosting Fees	Other Fees	Total
1	Cloud Hosting					example - please update	$0.00	$0.00	$0.00	$0.00	$0.00
1	Cloud Hosting					example - please update	$0.00	$0.00	$0.00	$0.00	$0.00
1	Cloud Hosting					example - please update	$0.00	$0.00	$0.00	$0.00	$0.00
2	Data Platform					example - please update	$0.00	$0.00	$0.00	$0.00	$0.00
2	Data Platform					example - please update	$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00
							$0.00	$0.00	$0.00	$0.00	$0.00

8. Software Cost Details

Notes
The costs on this worksheet provide the Vendor's **fully burdened off-site hourly labor rates** for the various job titles in Attachment K: Vendor Key Personnel. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Vendor's staff training, project facility, and any other expenses must be included in the Vendor's fixed hourly rates. Provide an estimate of the anticipated percentage of time to be allocated to the Department for each Key Personnel. The information in this worksheet is for reference purposes only and will not be updated in the worksheet 1.Cost Summary.

Data Analytics Platform

8. Key Personnel Labor Rates

Vendor Name: *<Vendor Name>*

Job Title	Contract Year 1		Contract Year 2		Contract Year 3		Contract Year 4		Contract Year 5		Option Year 1		Option Year 2	
	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage	Hourly Rate	Allocation Percentage
Delivery Lead / Account Executive	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Program / Project Manager	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Cloud Platform Architect	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Data Architect	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Data Governance Lead	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Security Architect / Compliance Specialist	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Data Engineering Lead	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Cloud Infrastructure / DevOps Engineer/ Platform Admin	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
BI / Reporting Lead	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Data Quality & Testing Lead	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Operations & Maintenance (O&M) Manager	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%
Data Operations Coach					$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%	$0.00	0%

9. Key Personnel Labor Rates

Notes
The costs on this worksheet provide the Vendor's **fully burdened off-site hourly labor rates** for the Labor Categories provided in this sheet. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Vendor's staff training, project facility, and any other expenses must be included in the Vendor's fixed hourly rates. The consulting labor rates contained in this worksheet apply only to services pertaining to the Consulting Services as defined in Sections 3.1.8 Consulting Services and 7.14.11 Consulting Services Pool. The information in this worksheet is for reference purposes only and will not be updated in the worksheet 1. Cost Summary.

Data Analytics Platform

9. Consulting Labor Rates

Vendor Name: *<Vendor Name>*

Labor Category	Labor Category Description	Minimum years of experience required	Contract Year 1 Hourly Rate	Contract Year 2 Hourly Rate	Contract Year 3 Hourly Rate	Contract Year 4 Hourly Rate	Contract Year 5 Hourly Rate	Option Year 1 Hourly Rate	Option Year 2 Hourly Rate
Cloud Developer	Performs application development from concept to design to implementation via programming languages or scripts based off architectural designs and business requirements. Oversees development, debugging, deployment and maintenance of host based, serverless and containerized applications in cloud based environments. Have ability to write cloud native API to support software, automation scripts and solutions for the customer base. Possess understanding of development in Agile methodology utilizing DevSecOps concepts and principles.	7+ years total industry experience, including 5+ years relevant cloud/ Data Platform development experience			$0.00	$0.00	$0.00	$0.00	$0.00
Cloud Big Data Specialist	Develop, test and maintain big data solutions for environments that requires collecting, storing, process and analyzing huge sets of data. Select and integrate big data tools both native to Cloud Service Providers and agnostic vendors and solutions. Implement ETL process, monitor for performance and cost and provide consulting advice on necessary improvements. Define retention policies as well as DR plan based on business continuity scenarios.	10+ years total industry experience, including 6+ years relevant big data/cloud data experience			$0.00	$0.00	$0.00	$0.00	$0.00
Cloud Migration Specialist	Possess subject matter expertise on moving from on-premise/private cloud workloads to public cloud. Plan and implement migration strategies to ensure data and workloads are moved to cloud with minimal downtime and impact. Possess strong understanding of migration tools/vendors and ensure right tool is used for the right job.	10+ years total industry experience, including 7+ years relevant cloud migration experience			$0.00	$0.00	$0.00	$0.00	$0.00
Cloud AI/ML Specialist	Develop operating software that can be used for artificial intelligence applications. Work closely with software engineers or big data specialists produce solutions that utilize artificial intelligence, machine learning and deep learning capability to serve the business need. Showcase the potential for AI via early stage use cases to demonstrate the art of the possible in order to provide consulting and thought leadership towards adoption of AI and ML capabilities.	10+ years total industry experience, including atleast 3-5 years relevant AI/ML experience in cloud environments			$0.00	$0.00	$0.00	$0.00	$0.00

10. Consulting Labor Rates

Notes
The Vendor must provide any basis of estimates and assumptions how the costs in this workbook were developed that enables the State to have a full understanding of the Vendor's pricing methodology. Please enter the Worksheet name and the Cost area or elements within the worksheet and provide the assumptions and basis of estimates information in the table below. The Vendor may add additional rows to the table as necessary.

Data Analytics Platform

10. Basis of Estimates

Vendor Name:	*<Vendor Name>*		
Item #	**Worksheet Name**	**Cost Area or Element**	**Assumptions / Basis of Estimates**
1			
2			
3			
4			
5			
6			
7			

11. 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 Attachment G 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 documents in 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: 30-2025-008-DHB
Data Analytics Platform Solution

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 PROGAM 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 MES Decision Support System (DSS) / Data Warehouse (DW) (DSS/DW) Module 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 MES Decision Support System (DSS) / Data Warehouse (DW) (DSS/DW) Module to a State Medicaid program.						
SUPPORTING INFORMATION:	**E**	**V**	**S**	**M**	**U**	**N/A**

TE4: Contractor provided an effective solution for the MES Decision Support System (DSS) / Data Warehouse (DW) (DSS/DW) Module.						
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**

TE6: Contractor effectively handled change management, knowledge transfer, and training of end users to enable MES Decision Sup System (DSS) / Data Warehouse (DW) (DSS/DW) Module adoption.						
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 copyof 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) and is aligned with the business capabilities and processes described within the Medicaid Information Technology Architecture (MITA) framework. It is, however, understood that the MITA framework is a high-level depiction of a Medicaid program and that additional capabilities and processes will be required to fully describe and document the North Carolina Medicaid Enterprise Systems.

The MES Enterprise Architecture standards require the use of industry standard conventions such as UML2, BPMN and ArchiMate to consistently describe all applications and all other architecture components within the MES environment. 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.

The Department leverages Orbus Infinity (Orbus Software) as a central repository for all MES EA information and artifacts. All MES vendors will be given access to the Orbus Infinity environment and will be required to enter architectural details into this system. The Orbus Infinity application is accessed through remote desktop services that are provided by the Department and maintains vendor information in separate, secured instances of the application. Vendors cannot view information provided by other vendors.

Information is entered into Orbus Infinity using online forms and templates while additional information is provided through attached documents or diagrams. The Department has standardized on 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, Security, Quality, Dictionary), Data Exchanges, Data Integrations, Data Interfaces, Data Architecture Designs, Conceptual Data Models, 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, Disaster Recovery and Business Continuity, Application Security, Data Security, Infrastructure Security, Security Monitoring.

All MES 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.

Any change to requirements, measures or metrics must be updated within Orbus Infinity so that a full impact assessment can be performed by the Department.

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.

b) The 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 *Table K-1 Vendor Key Personnel.* Vendor must indicate the name of the proposed individual who will perform each role. If a substitution is needed and the appropriate personnel is not immediately available, the Contractor must notify the Department of the interim personnel as they work to obtain the Department's approval for the formal substitution request.

c) If the Vendor needs to 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 suggested role

   v. Requested effective date

   The Contractor shall provide an updated organizational chart within five (5) business days of the Department's approval of the substitution.

d) The Vendor must provide a detailed staffing contingency plan for handling sudden and unexpected increases in the volume of transactions or the number of users with a description of how the plan will be implemented and coordinated with the Department.

Role Title	Phase	Description of Role Responsibilities and Duties	Minimum Qualifications
Delivery Lead / Account Executive	DDI/O&M	Acts as the single point of contact for matters concerning the Contractor's performance under the Contract. This person shall have the authority to make decisions that are binding to the Contract, shall be responsible for timely completion of the project, and shall be responsible for meeting all contractual obligations. This role holds accountability for the whole project and would be the escalation contact for the state team.	- Minimum 10 years in technical delivery and contract management experience managing related services with similar budgets, preferably in Medicaid or the healthcare industry and for a project similar in size and scope to this project.
Program / Project Manager	DDI	Tracks milestones (e.g., environment setup, ingestion, migration, go-live), manages risks, ensures alignment with NCDHHS MES PMO and change-control processes.	8+ years of IT project management with at least 3 years of data platform/cloud programs; proven delivery using Agile or hybrid methodology; strong stakeholder management; PMP or equivalent experience preferred.
Cloud Platform Architect	DDI	Cloud networking, integration patterns, security zones, scaling model, metadata and lineage integration, DevOps integration design, environment design, disaster recovery planning	7+ years of experience in cloud solution design, including 3+ years working with modern cloud data platforms; experience with Data Lake and Lakehouse architectures; cloud architect–level certification or equivalent experience preferred.

Role Title	Phase	Description of Role Responsibilities and Duties	Minimum Qualifications
Data Architect	DDI	Defines and governs a high performance and cost-efficient enterprise data model across conceptual, logical, and physical layers, including design of data products	6+ years of experience in data architecture on cloud platforms; proven experience designing data models for cloud-based data warehouses, preferably in Medicaid or healthcare domains; ability to collaborate effectively with architects and data governance leads.
Data Governance Lead	DDI	Metadata management, glossary, CDEs, data quality framework, catalog integration, stewardship workflows, policy enforcement	3+ years in data governance or metadata management; hands-on experience with the Solution recommended data governance tool; understanding of data lineage, data quality, and policy frameworks; strong communication and facilitation skills.
Security Architect / Compliance Specialist	DDI	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.
Data Engineering Lead	DDI/O&M	Designs ETL/ELT pipelines (ADF, Snowpipe, etc.), manages reusable ingestion frameworks, performance tuning, CDC, and orchestration, leads data migration during DDI, including converting legacy SAS code base for new data model and platform, and responsible for data pipeline maintenance during O&M	7+ years of experience in data engineering, including 3+ years working with modern cloud-based data platforms; strong proficiency in SQL and PySpark; experience with data integration, CI/CD pipelines, and data modeling; experience with SAS preferred; proven experience leading engineering teams.
Cloud Infrastructure / DevOps Engineer/ Platform Admin	DDI/O&M	Infra-as-Code, containerization, deployment automation, cost monitoring, environment isolation, backup/recovery, DevOps setup.	5+ years of experience in cloud infrastructure; hands-on experience with infrastructure-as-code (IaC) tools and CI/CD pipelines; experience managing multi-environment data platforms; cloud administrator or DevOps engineer certification preferred.
BI / Reporting Lead	DDI	Power BI workspace setup, dataset optimization, semantic models, alignment with new data model, user training and adoption, leads report/dashboard migrations	5+ years in BI/reporting; 3+ years with Power BI and cloud data sources; experience with semantic layer design; Power BI Data Analyst Associate certification or equivalent preferred, proven experience leading BI developer teams.
Data Quality & Testing Lead	DDI/O&M	Automated data validation, reconciliation scripts, pipeline testing, regression testing post-release, specifically around SIT, and Parallel Run	5+ years in Cloud based data testing and quality assurance; hands-on with SQL and PySpark, automation frameworks, and reconciliation scripting; experience validating data migrations and transformations in Data warehouse/lake house or similar.
Operations & Maintenance (O&M) Manager	O&M	Monitoring jobs, incident triage, cost-performance tuning, backlog management, release scheduling, and knowledge transfer to internal staff, monthly invoicing and budgeting	6+ years of experience managing production operations for data platforms; hands-on experience with platform monitoring, cost management, and performance optimization

Role Title	Phase	Description of Role Responsibilities and Duties	Minimum Qualifications
			tools; experience managing SLAs and coordinating with vendors.
Data Operations Coach	O&M	- Mentor analysts/business users in developing code for jobs/reports on new Solution/technology stack and troubleshooting issues in the new Solution. - Guide the team in adopting best practices for code development, including code versioning, peer reviews, and performance optimization. - Provide day-to-day support and knowledge transfer to build self-sufficiency within the State team. - Responsible for development of onboarding materials, conducts workshops, builds SOPs for future operations, ensures business users understand governance processes. - Perform standard Data Engineering tasks as part of the daily operations when there are no coaching needs	7+ years of experience in data engineering, including at least 3+ years working with modern cloud-based data platforms; strong proficiency in SQL and PySpark; experience with data integration, CI/CD, and data modeling; 3+ years of experience in organizational change management or training; experience supporting self-service reporting, advanced analytics, and adoption of cloud and new data platforms; strong communication and documentation skills.

Table K-1 Vendor Key Personnel

ATTACHMENT L: SERVICE LEVEL AGREEMENTS

1.0 Service Level Agreements (Implementation, O&M & Transition)

The State has identified the Service Level Agreements (SLAs) provided in *Table L-1 Service Level Agreements* 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 Table L-1 Service Level Agreements. 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.

Table L-1 Service Level Agreements information includes:

- SLA ID: Unique identifier of the SLA
- Description: A description of the SLA.
- Liquidated Damages: The State and Vendor agree that failure to meet certain performance standards will result in liquidated damages.
- Phase / Stage: The phase of the project when the SLA will be enforced and measured.
- Frequency / Updates: Indicates how often the SLA will be measured.
- Category: Categorization and grouping of SLA.

Note: The SLA ID assigned to each SLA in *Table L-1 Service Level Agreements* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
DAP-SLA-MS-001	Vendor shall adhere to the following service request resolution time frames ninety-five (95%) of the time based on complexity levels: Level A: Basic Support, except password resets, such as product issues, etc., are resolved within two (2) business days.	Level A, C: 5% of retainage for missing SLA within those categories in the month Level B: 2.5% of retainage for missing SLA in the month	O&M	Monthly	Operations

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
	Level B: Complex Support, such as in-depth data analysis, aggregate methodologies, issues related to the health care domain, etc. are resolved within six (6) business days. Level C: New User Provisioning is completed within one (1) business day of the request. Changes to existing User Provisioning is completed within one (1) business day of the request.				
DAP-SLA-MS-002	This SLA applies to all datasets and data assets according to their pre-defined processing frequency (daily, weekly, or other scheduled intervals). Data will be considered compliant if, by 8:00 AM ET on the scheduled processing day, 100% of datasets are: - fully refreshed (all expected records or partitions loaded in accordance with the Data Asset Inventory), - validated (all pre-defined data quality checks executed and passed), and - available (accessible and able to be queried by authorized State users within the production environment).	If the SLA is not met on any scheduled processing business day, liquidated damages apply on a per-day basis as follows: • If less than 100% of datasets are fully refreshed, validated, and available by 8:00 AM ET on a given day, liquidated damages of $1,500 apply for that day. Liquidated damages will be assessed only for the days on which the applicable SLA thresholds are not achieved.	O&M	Monthly	Operations
MES-SLA-INT-001	Solution shall ensure data received from real-time interfaces will be accessible in the Solution within thirty minutes; excluding batch interface updates.	Department will assess as specified below, per hour for each hour, or portion thereof, if any of Solution interface jobs fails to complete within 30 minutes of expected execution. • $100/hour - 0 to 24 hours beyond the Performance Standard • $200/hour - 24 to 48 hours beyond the Performance Standard • $300/hour > 48 hours beyond the Performance Standard	O&M	Monthly	Integration
MES-SLA-OM-001	Production Solution must have Availability 99.9% of the time, 24 hours a day, seven days a week, excluding Department approved planned Downtime. Availability is calculated as follows: Availability percentage = unplanned Downtime (Total Downtime-approved Downtime) divided by Total time (24X7). The module is considered unavailable when any of the capabilities	Department will assess as specified below, per hour for each hour, or portion thereof, if any of the Solution fails to meet the 99.9% Availability Performance Standard. • $1,000/hour - 0 to 24 hours beyond the Performance Standard	O&M	Monthly	Operations

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
	do not function as described in this RFP and subsequent documentation.	• $2,000/hour - 24 to 48 hours beyond the Performance Standard • $3,000/hour > 48 hours beyond the Performance Standard			
MES-SLA-OM-002	Reporting timelines for production issues. • Critical priority Issues: Must be reported within one (1) hour of identification. • High, medium, and low priority Issues: Must be reported within four (4) business hours of identification, or by 7 AM the next business day if discovered outside of business hours.	In the event of noncompliance with any service level, the State may assess liquidated damages according to the following schedule unless otherwise stated: Department will assess as specified below, per hour for each hour, or portion thereof, if issues are not reported within the reporting performance standard. Critical Priority Issues: • $500/hour - 0 to 24 hours beyond the Performance Standard • $1000/hour - 24 to 48 hours beyond the Performance Standard • $2000/hour > 48 hours beyond the Performance Standard High, Medium and Low Priority Issues: • $100/hour - 0 to 24 hours beyond the Performance Standard • $200/hour - 24 to 48 hours beyond the Performance Standard • $300/hour > 48 hours beyond the Performance Standard	O&M	Monthly	Operations
MES-SLA-OM-003	Resolution timelines for production issues. • Critical priority Issues: Must be resolved within two (2) hours of reporting. Status updates are required every thirty (30) minutes, or at an alternative interval if mutually agreed upon. Note: Environment down/availability will require 24/7 response and resolution effort until the issue is resolved. • High priority Issues: Must be resolved within forty-eight (48) hours from the time the incident is reported. • Medium priority Issues: Must be resolved within four (4) business days from the time the incident is reported.	Department will assess as specified below, per hour for each hour or business day per business day where noted, or portion thereof, if issues are not resolved within the resolution performance standard. Critical Priority Issues: • $1000/hour – for any delay beyond the Performance Standard High Priority Issues: • $250/hour – for any delay beyond the Performance Standard Medium Priority Issues:	O&M	Monthly	Operations

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
	• Low priority Issues: Must be resolved within ten (10) business days from the time the incident is reported.	• $1000/business day – for any delay beyond the Performance Standard Low Priority Issues: • $100/business day - for any delay beyond the Performance Standard			
MES-SLA-PM-001	The Vendor must meet the due date for submission and subsequent resubmissions for each deliverable as defined in the Department approved project schedule.	1% of retainage per Business Day from the Deliverable Submission Due Date in the Work Plan.	DDI / O&M	Monthly	Project Management
MES-SLA-PM-002	Vendor shall ensure there are no more than two submissions of any Deliverable to gain Acceptance by the Department using the process defined in Attachment N: Deliverables and Milestones Schedule.	$1000.00 per submission per Deliverable requiring more than two submissions.	DDI / O&M	Monthly	Project Management
MES-SLA-PM-003	Vendor must have an acceptable documented risk mitigation plan submitted to the Department within 5 business days of risk identification for high or critical project risk. The Department, after consulting with Vendor, will determine the level of criticality of each project risk.	Severity of SLA Breach, Impact Description, Monthly Liquidated Damages (% of Monthly Retainage) High, Significant impact on business operations, 5% per business day beyond 5 business days Critical, Severe impact 10% per business day beyond 5 business days.	DDI	Monthly	Project Management
MES-SLA-PM-004	The Vendor must provide accurate responses to all Department Change Requests for Enhancements including proposed solution and hours/cost within 15 business days for low complexity projects, 25 business days for medium complexity projects or 35 business days for high complexity projects, from submission of a Department Change Request for an Enhancement. The Vendor will determine the level of complexity in consultation with the Department.	$200 will be assessed for each business day that the Vendor fails to provide an acceptable proposed solution for a Change Request for Enhancements within the specified performance standard. "acceptable" means that the Change Request for Enhancement from the Vendor includes Vendor's proposed solution and associated hours/costs to comply with request made by the Department.	DDI / O&M	Monthly	Project Management
MES-SLA-PM-005	Vendor must ensure all reports listed in Attachment AA: Reports are available online for review by the Department pursuant to the following schedule: A. Daily or Weekly Reports – by the end of the calendar day following the end of the reporting period.	• $50 per day per report beyond the Performance Standard for Daily and Weekly reports. • $500.00 per day per report beyond the Performance Standard for Monthly, Quarterly and Annually.	O&M	Monthly	Project Management

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
	B. Monthly Reports – by the third calendar day following the end of the reporting period C. Quarterly or Annual reports – by the fifth calendar day following the end of the reporting period.				
MES-SLA-SEC-001	Vendor must setup the alternate processing site with a Recovery Time Objective (RTO) of 5 min and a Recovery Point Objective (RPO) of 1 hour from the time a disaster is declared. The Vendor must 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.	5% of monthly retainage for each occurrence.	O&M	Monthly	Disaster Recovery
MES-SLA-SEC-002	Vendor must conduct and pass comprehensive annual technical and operational testing of the Disaster Recovery Plan and Business Continuity Plan with any test failures documented and resolved within 30 calendar days of testing completion.	$500.00 per day beyond the Performance Standard (e.g. if remediation takes more than 30 days, for each day after) until the detailed Disaster Recovery Plan test results are delivered to the Department.	O&M	Annually	Disaster Recovery
MES-SLA-SEC-003	If the Vendor is out of compliance with the Federal, State, and/or NCDHHS privacy & security policies, a mitigation plan to regain compliance is due to the to the Department Contract Administrator and the NCDHHS Privacy & Security Office (PSO) within ten (10) business days.	5% of monthly retainage for each occurrence of a mitigation plan that is delayed beyond 10 business days.	DDI / O&M	Monthly	Security
MES-SLA-SEC-004	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 Department Contract Administrator and the NCDHHS Privacy & Security Office (PSO) within ten (10) Business Days from the day the reports are submitted to the Vendor.	5% of monthly retainage for each occurrence of a CAP or PO&AM plan delayed beyond 10 business days..	DDI / O&M	Monthly	Security
MES-SLA-SEC-005	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 NCDHHS Privacy and Security Office within twenty-four (24) hours after the incident is first discovered.	10% of monthly retainage for each failure to meet the notification periods identified in the SLA.	DDI / O&M	Monthly	Security

SLA ID	Description	Liquidated Damages	Phase / Stage	Frequency	Category
	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.				
MES-SLA-SEC-006	Vendor must report any confirmed security breaches to the Department Contract Administrator and NCDHHS Privacy and Security Office within one (1) hour. Vendor must work with the Department to gather, analyze and report findings to the Office for Civil Rights (OCR). Sufficient technical evaluation will be completed by the Vendor to verify the number of members potentially affected. The Vendor must share, coordinate, and assist in workarounds (as required) with any impacted modules.	• All costs of mitigation (all Vendor and Department costs) for any HIPAA incident that results from actions attributed to Vendor's performance of the Contract. • In addition, Vendor will receive sanctions, if any, determined by the OCR and be responsible for mitigation costs and other associated costs such as call center costs, credit reporting, publications, and media centers.	DDI / O&M	Monthly	Security
MES-SLA-SEC-007	Vendor must perform patching and corrections to mitigate • critical security vulnerabilities within seven business days, • high vulnerabilities within thirty business days, • medium vulnerabilities within sixty business days, • low vulnerabilities within ninety business days. The Vendor must determine the level of criticality in consultation with the Department and in accordance with Section 3.3.3 Vulnerability Risk Ratings and Remediation.	• $5,000.00 per occurrence per day for Critical. • $2,500.00 per occurrence per day for High. • $5,000 per occurrence per week for all other criticality levels if the patch or correction is not Implemented within the Performance Standard timeframe.	DDI / O&M	Monthly	Security
MES-SLA-TST-001	The Vendor must resolve defects identified during all applicable test phases in accordance with the approved Master Test Plan. Consistent failure to meet the defined thresholds will trigger SLA enforcement if any of the following thresholds are exceeded during a sprint or test cycle: • More than 15 open defects remain unresolved assigned to the Vendor or; • The average aging of critical and high-priority defects assigned to the Vendor exceeds 8 business days.	If any of the SLA thresholds are reached within a testing cycle: $500 per business day until the threshold level is resolved.	DDI / O&M	Per Testing Cycle	Testing

Table L-1 Service Level Agreements

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	Brandon Newpher
Address	1915 Health Services Way, Raleigh NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh NC 27699-2501
Telephone Number	919-527-7238
Email Address	brandon.newpher@dhhs.nc.gov

Contract Administrator for all day-to-day matters:

Name and Title	Sri Kandukuri
Address	1915 Health Services Way, Raleigh NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh NC 27699-2501
Telephone Number	919-909-1983
Email Address	sri.kandukuri@dhhs.nc.gov

State Privacy and Security Point of Contact:

Name and Title	Ramana Posam
Address	1915 Health Services Way, Raleigh NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh NC 27699-2501
Telephone Number	919-855-3090
Email Address	posam.ramana@dhhs.nc.gov

State Technical Point of Contact:

Name and Title	Naga Narne
Address	1915 Health Services Way, Raleigh NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh NC 27699-2501
Telephone Number	919-820-0712
Email Address	naga.narne@dhhs.nc.gov

Invoices Electronic Submission Contact:

Name and Title	Sri Kandukuri
Address	1915 Health Services Way, Raleigh NC 27607
Mail Service Center Address	2501 Mail Service Center, Raleigh NC 27699-2501
Telephone Number	919-909-1983
Email Address	sri.kandukuri@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

1.0 DELIVERABLES

Table N-1 Deliverables lists the deliverables to be provided by the Vendor for this project. The information for each deliverable includes:

- Deliverable ID: Unique identifier of the deliverable.
- Title: Name of the deliverable.
- Description: A summary of the elements to be included in the deliverable.
- Phase / Stage: The phase of the project when the deliverable is expected to be delivered. The timing of the deliverable with the phase is in alignment with the milestone schedule provided in *Table N-2 Milestones*
- Frequency / Updates: Indicates how often the deliverable is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the deliverable. The meaning of the values is as follows:
    1. None – No preferred template exists. The Vendor is free to provide the deliverable in its own format and content.
    2. State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Deliverable ID.
    3. DED Required: A Design Expectation Document (DED) must be submitted by the Vendor and approved by the State prior to the actual deliverable being submitted.

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 *Attachment B: Department of Information Technology Terms and Conditions, Section 1, Paragraph Acceptance Process.* The Vendor must ensure that, for each deliverable, no more than two review iterations are used to gain acceptance by the State 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.

Note: The Deliverable ID assigned to each deliverable in *Table N-1 Deliverables* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
DAP-DEL-DMD-001	Data Pipelines Documentation	Documentation for all pipelines (source-to-target mappings, dependencies, schedules, owners).	DDI / O&M	As Needed	None
DAP-DEL-MIGR-001	Solution Migration Design	Document detailing the migration technical design (e.g. encryption, data model mapping, entity relationships, security controls), migration processes, assumptions, and mappings for auditability and future reference. The design needs to cover report migration and code migration.	DDI	As Needed	None
DAP-DEL-MMM-001	Monthly Observability Summary	An observability summary shall be provided monthly to the State, based on real-time observability dashboards and monitoring tools, to track query performance, system latency, and cost trends.	O&M	Monthly	None
MES-DEL-AI-001	GenAI Disclosure and Fact Sheet	The Vendor must submit and maintain the GenAI Disclosure and Factsheet using the template provided in Attachment AC.	DDI / O&M	As Needed	None
MES-DEL-ARCH-001	Data Architecture	Document that describes the Vendor's solution's data, how it is used, stored, and transmitted. The document should also include, at minimum, the following information: • Data Governance: Define the authority and control over the management of data assets as well as how the Vendor will act as a Data Governance partner with Business and Technology Owners to decide how data can be used and how this usage must be controlled. Data Governance will influence all levels of Data Management and other architectural areas. • Data Management: Define processes that will be used to support Data Development, Data Operations, Data Security and Data Quality while supporting the functional and non-functional requirements and adhering to the Data Governance processes. • Data Development Management: Describe the process for designing, implementing and maintaining the solutions to meet the data needs of an organization. • Data Operations Management: Describe the process for planning, monitoring, controlling and supporting of structured and unstructured data assets across the data assets lifecycle. • Data Security Management: Describe the process for planning, development, and execution of data security policies and procedures to provide proper authentication, authorization, access and auditing of data and information. Must include processes for data privacy and	DDI / O&M	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		security analysis along with requirements for encryption during processing, transmission and storage. • Data Quality Management: Describe the process for planning, implementation, and control activities that apply data quality management techniques to measure, assess, improve, and ensure the fitness of data for use.			
MES-DEL-ARCH-002	Data Architecture Document - Conceptual Data Model (CDM)	Conceptual Data Model (CDM) identifies the data elements required for an end-to-end business process execution including the identification of data standards that will reduce future rework to achieve successful data sharing across the enterprise and for intrastate/interstate exchanges. The CDM is required to be used as a reference to provide high-level overview of the data and relationships used by the enterprise and to provide a tool for ensuring the completeness of the business model.	DDI / O&M	As Needed	None
MES-DEL-ARCH-003	Data Architecture Document - Data Dictionary (Electronic)	Electronic data dictionary using industry best practices to be approved by the Department. At a minimum, the data dictionary shall contain for each field: field name in human readable format, field business description, technical description, database field name, database table, field type and length, valid values and their corresponding descriptions, source, and authorization for access for each data element in the files and databases, flag for Critical Data Elements (CDEs), data lineage, ownership, and applicable data quality rules for use in the data governance tool.	DDI / O&M	As Needed	None
MES-DEL-ARCH-004	Data Architecture Document - Logical Data Model (LDM)	Logical Data Model that describes and diagrams the module's data elements and relationships. This should include a description of all table structures, including column names, column data types, column constraints, primary keys, foreign keys, and relationships (a Physical Data Model).	DDI / O&M	As Needed	None
MES-DEL-ARCH-005	MES Architecture Documentation	Document that contains data and information regarding the total solution to include each DAP component. It will address Enterprise Architecture as well as Application/Solution Architecture, Infrastructure Architecture, Performance Architecture and Integration Architecture as defined within the Federal Enterprise Architecture Framework. The Application Architecture will describe the application functions, process flows, communication flows, services used, user communities, use cases, software used, etc. The Application Architecture will demonstrate how the functional and non-functional requirements are being met or expanded upon. The Solution Architecture Document includes a technical explanation of all aspects of the solution including detailed architectural diagrams, data	DDI	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		flows, component specifications, SaaS, COTS products and hosting environment details. The document will include architectural tradeoffs using the Architecture Tradeoff Analysis Method (ATAM) method or other suitable method for evaluating the proposed platform architecture relative to the enterprise goals to identify risks that would inhibit the achievement of Agency's business goals. The Infrastructure Architectures describe the hardware, platforms or infrastructure services used by the Contractor's solution. It will also describe in sufficient detail the physical characteristics of the hardware, system software, and network components to build and integrate the architectural solution. The Performance Architecture describes how the application will scale and what metrics are measured to ensure the components are meeting the performance levels set by the State. Describe the tools used to measure the metrics and how they are used in capacity planning. The Interface Architecture should describe the interface(s) between the system being developed and other systems (e.g., batch transfers, real time APIs, queries, etc.), indicating the location of the interfacing system. Include the interface architecture(s) being implemented and the interfacing mechanisms (e.g., MQ, Gentran, etc.) and how they incorporate the State's Medicaid Integration Services capabilities. If remote connectivity is required, identify the method of access. Provide a diagram depicting the communications path(s) between this system and each of the other systems. The graphical representation should depict the connectivity between systems, showing the direction of data flow.			
MES-DEL-ARCH-006	Configuration/Customization Plan	Document that describes the Vendor's responsibility to identify, control, and track versions of hardware, software, documentation, processes, procedures, and all other components of the environment under the control of change management. Processes are provided to ensure that only authorized components, referred to as configuration items (CIs), are used in the environment and that all changes to configuration items are recorded and tracked through the component life cycle. This plan will outline the Vendor's: • Approach to conducting design sessions or walkthroughs. • Configuration management. • Approach to system enhancements	DDI / O&M	As Needed	DED Required

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Programming and coding standards • Approach to moving and promoting code between lower and production environments • Approach to applying the latest patches to software, hardware, and environments. The Vendor will perform and manage the configuration/customization process and keep the State apprised of its progress. The initial configuration/customization plan is part of the implementation cost and not eligible for Change Order or Change Request spending. The Configuration Management Approach specifies: • How the solution will store configurations, including naming conventions and data management (repository design, creation, loading, updating, backup, and recovery). • Baseline • Baseline documents list • Configuration items list • Configuration items compatibility list (version)			
MES-DEL-ARCH-010	System Design Document (SDD)	Documentation that describes how the functional and nonfunctional requirements recorded in the Requirements Response Matrix transform into more technical system design details from which the system is configured and built. The SDD documents the high-level system design and the low-level design details. The SDD describes design goals and considerations, provides a high-level overview of the system architecture, and describes the data design associated with the system, as well as the human-machine interface and operational scenarios. The high-level system design is further decomposed into low-level design details for each system component, including infrastructure, integration patterns, data flows, internal communications, software, system integrity controls, external interfaces, monitoring & observability, and migration technical design (e.g. encryption, data model mapping, entity relationships, security control). The SDD documents and tracks the necessary information required to effectively define architecture and system design in order to give the development team guidance on the architecture of the system to be developed. Design documents are incrementally and iteratively updated	DDI / O&M	As Needed	State Provided

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		during the system development life cycle and include proprietary contractor material. Its intended audience is the project manager, project team, and development team. The Contractor shall provide and maintain system design documentation that includes at a minimum: • A description of each component, their purpose, including basic functions and the business areas supported • User stories/use cases • User interface design • A module system diagram, including all components, identifying all business process diagrams, data flows, systems functions, and their associated data storage • Configurations • Job streams within each module, identifying programs, inputs and outputs, control, job stream flow, operating procedures, and error and recovery procedures. • Listing of the edits and audits applied to each input item and the corresponding error messages. • Narrative descriptions of each of the reports and an explanation of their use must be presented. • Definition of all fields in reports, including a detailed explanation of all report item calculations.			
MES-DEL-ARCH-012	Section 508 Compliance Test Report	The Vendor must provide a completed Vendor Product Accessibility Template (VPAT) in accordance with Section 508 of the Rehabilitation Act, using the most current VPAT available at the time of submission, whenever there are changes to the user interface. Third-party attested VPATs do not require separate accessibility testing documentation. Self-reported VPATs must include documented test results demonstrating conformance with WCAG Level AA, as adopted under Section 508 and in effect at the time of completion.	DDI / O&M	As Needed	None
MES-DEL-CERT-001	Certification Plan	Document which defines the Vendor's approach to CMS certification. It must include supporting the State with the following: • The processes and procedures that will be used to manage certification requirements throughout the project lifecycle • Intake Form • Complete certification phase deliverables • Solution functionality validation against Conditions for Enhanced Funding	DDI	Once	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• CMS-required and State-specific outcomes • Deliverables traceability to Appendix B - Required Artifacts List found in the CMS Streamlined Modular Certification (SMC) Guidance document at https://cmsgov.github.io/CMCS-DSG-DSS-Certification/SMC%20Guidance.pdf • Operational Reporting Workbook • The process the vendor will use to support CMS Certification Life Cycle The Certification Plan must comply with the most current SMC process to ensure the system will meet all certification requirements.			
MES-DEL-CERT-002	CMS Operational Report Workbook	Vendor must submit monthly operational reports and data to the Department that support the module in CMS certification and utilize the most updated CMS templates. These reports must demonstrate the continuous achievement of the module's required and desired outcomes through the delivery of the new module and include data and metrics. The Department may also use these reports to support funding requests as needed and to provide CMS with early and ongoing insight into program evaluation and opportunities for improvement.	O&M	Monthly	None
MES-DEL-CERT-003	Operational Readiness Review Checklist	Checklist with areas that examine the actual solution characteristics and the procedures of the product's operation to ensure that all testing, hardware, software, resources, procedures, and user documentation accurately reflect the deployed state of the system.	DDI	Once	DED Required
MES-DEL-COMM-001	DDI Communication Plan	Document to provide a plan for communications that will occur on the project and how it will be managed. This includes details about various types and means of communication, communication channels, communication flow within the organizational structure, escalation, guidelines for meetings, dissemination of knowledge, and communication effectiveness. The plan must include, but is not limited to: • A defined approach and actions to engage stakeholders throughout the life of the project • Information communications • Information communication requirements/needs • How, where, and when communications will occur • Who will provide/receive the communication • The purpose of the communications	DDI	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• The title of communications • Meeting protocol procedures–noting when minutes are taken, etc. • Stakeholder communications approach—to include interactions among the State and other Stakeholders Updates/modifications to the DDI Communication Plan, as mutually agreed, will occur as needed.			
MES-DEL-COMM-002	Operations Communications Plan	This document will define the methodology for engaging users and stakeholders during the Operations Phase to promote adoption of the new system. It will describe the processes to ensure timely and effective communication, training, and support to facilitate user interaction with the system. The plan must include: • User communication strategies • Identification of user needs and requirements for system interaction • How, where, and when user engagement and training will occur (including hands on training sessions) • Roles and responsibilities for providing and receiving user-related communications • Meeting protocols to address user feedback and system updates–including documentation of key decisions • Interactions among the State, the Vendor, and other stakeholders to support user adoption • The Vendor's approach to raising awareness of system features and benefits following Contract award; and the facilitation of ongoing user engagement and system adoption efforts • Reporting and escalation of user-related issues—to include reporting of system usability concerns and adoption challenges	DDI	Once	None
MES-DEL-DATA-001	Data Management, Conversion and Migration Plan	Document that describes how the Vendor will convert and migrate all required data from existing systems into the Solution and includes the following: • A data management strategy that will support integration, optimization, quality, stewardship, standards, and align with the Department's Data Governance processes. • Description of appropriate skill sets, processes, technologies/tools, and any naming conventions followed. • Approach to conversion, cleansing and migration.	DDI	As Needed	DED Required

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Approach to risk management and security for data conversion effort. • Approach for testing migration or converted data. • Approach to reporting the number of records successfully converted vs. errors or exceptions. • Approach for cleansing and validating data to prepare it for loading to the proposed solution that is refined as necessary. • Approach to resolving data conversion errors and issues. • Approach for supporting the Department validation of converted data. • Tasks, timelines, and responsible parties for all conversion and migration tasks. • Entrance and exit criteria for each phase of the effort.			
MES-DEL-DATA-002	Data Conversion Test Results	Document containing test results for each test run during migration of historical data from the current solution to new Solution. The test results include: • Executed test cases • Mapping of executed test cases to the associated requirement • Mapping of executed test cases to their artifacts and results • Executing tester for test case • Date of execution • Pass/fail status • Balancing reports that account for all input data being transformed to output data and identify anomalies for resolution • Exception reports that identify data which fails the conversion process Data Conversion will not be considered complete until the Department validates successful data conversion through these reports.	DDI	As Needed	DED Required
MES-DEL-INT-001	System Interface Design Strategy	Document that describes: • how interface requirements are gathered • how top-level designs are defined and responsibilities assigned • how detailed designs are determined and created • how interface tests are identified, created and executed • how defects or data exchange failures are escalated for quick resolution • how interface creation is managed and executed • how interfaces are maintained and monitored • any other key features of the Vendor's Interface Design Strategy.	DDI	Once	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		The document must also include the template the Vendor will use and populate during the interface design sessions. That template must minimally gather: • data exchanges and contact points between the MIS and the Vendor • interface frequency • method of data exchanges • interface requirements Additionally, the Vendor must work with the Medicaid Integration Services (MIS) on how the Vendor will coordinate with the MIS to achieve all product requirements.			
MES-DEL-INT-002	Interface Control Document	Document which details all interfaces and will include data layout documentation, data mapping crosswalk, inbound/outbound capability, business rules, and frequency of all interfaces. This document will be used to request State approval of the integration or interface prior to the start of this development work. Source to target mappings should be provided in Excel format as Addendums to the Interface Control Document.	DDI	As Needed	State Provided
MES-DEL-OM-001	Operations, Maintenance, and Configuration Plan	Document that describes post-implementation processes for areas such as: • Architecture/hosting operations • Monitoring daily operations performance • Performing routine maintenance • Maintaining user documentation • Online help approach and documentation, as appropriate • Approach to enhancements and other new requirements • Maintaining system documentation • Archiving requirements. • Process improvement • Performance metrics (which ones will be measured, how the measurements will be collected and reported on, and what happens if something exceeds an acceptable threshold, document performance optimization techniques used) • Risk and issue management plan • Resource management • Software testing and system engineering, O&M defect management	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		The above areas will be included in the plan, either by incorporating the topic in the document or referring to other stand-alone documents. Roles and responsibilities of the State and Vendor will be clearly delineated.			
MES-DEL-OM-002	Capacity Plan	Document that describes, at a minimum, the number of concurrent users supported, number of transactions, storage capacity, throughput volume, scaling, availability and how it will be continuously monitored during operations and maintenance.	DDI / O&M	As Needed	None
MES-DEL-OM-004	Operations Procedure Manual	Document that provides guidelines for the operation and use of the module and/or module component(s). At minimum the Operations Procedure Manual shall contain policies, processes and workflows for the module and/or module component(s).	DDI / O&M	As Needed	None
MES-DEL-OM-005	Release Management Plan	Document that describes the approach to work with the Department or impacted Department Contractors, and the MES PMO with the objective of a 60-day lead time for releases. The document should also contain details on the Vendor's approach to managing, planning, scheduling, and controlling a DAP component build through different stages and environments; including testing and deploying DAP releases.	DDI	As Needed	DED Required
MES-DEL-OM-006	Turnover Plan	A Turnover Plan document must be submitted to the Department at least nine (9) months before the end of the final Contract year (including option years that have been exercised) or within a timeframe specified by the Department in the event of early contract termination. The plan document will include: • Proposed approach to turnover, including established roles and responsibilities between contractor and state team. • Tasks and subtasks for turnover. • Schedule for turnover and contingency plans. • Updated operational tasks and procedures during turnover. • Description of vendor coordination activities that will occur during the turnover task and implementation of the activities to ensure continued system and services as deemed necessary by the Department. • List of incomplete tasks, such as system defects, modifications or enhancements, reference updates, and configuration requests. • A detailed description of the services that would be required by another Contractor to fully take over system, technical, and business functions outlined in the Contract. The description shall also include an estimate	DDI / O&M	Once	DED Required

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		of the number and type of personnel required to support the technical platform and supporting services. • The data and documentation shall be organized in a format required by the State (e.g., by provider unique ID and provider name). • The conversion and migration of all pertinent information and work in progress, leases, etc.			
MES-DEL-PM-001	Project Management Plan	Document to provide a comprehensive baseline of what needs to be achieved by the project, how it is to be achieved, who will be involved, how it will be reported and measured and how information will be communicated with the project. It will serve as a reference for decision and clarifications as well as define how all project activities will be executed, monitored, and controlled. This document describes the processes for ensuring adherence to State, NCDHHS, and federal policies, standards, guidelines, and procedures. The document will also include: • Project charter • Project budget and adherence thereto • List of all known assumptions, risks and risk mitigation strategies, and target resolution dates	DDI	As Needed	None
MES-DEL-PM-002	Quality Management Plan	Document that identifies what defines quality, the quality standards for the project, how those quality standards are measured, and how the quality of all submissions to the Department will be ensured and maintained. It includes the process steps and quality tools that will be used (i.e., templates, standards, and checklists).	DDI	As Needed	None
MES-DEL-PM-003	Risk and Issue Management Plan	Document that describes how risks and issues will be monitored, maintained and acted upon throughout the project in accordance with Section 7.11.1 Risk and Issue Management of the RFP. The document must contain the following: • Proactive identification and analysis of risks before they become issues. • Roles and responsibilities. • Development of risk avoidance, transfer, mitigation or management strategies. • Approach to monitoring, communicating, reporting of risk and issue status including procedures for documenting, resolving, and reporting issues and risks identified by the Vendor, the Department or other project contractors. • Approach to impact analysis.	DDI	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Approach to root cause analysis. • The appropriate methods, tools, and techniques for active and ongoing identification and assessment of project risks. • Describe how risks will be quantified and qualified. • Describe the plan for timely notification to the Department of any changes in risk or trigger-of-risk events.			
MES-DEL-PM-004	Change Management Plan and CR Approval Process	Document that describes how changes will be initiated, submitted, assessed for impacts, reviewed, approved, or rejected throughout the life of the project. Applicable changes include alterations to project's budget, requirements, scope, and schedule. The plan must align with the Department's formal process and include the following: • Approach to coordinating with any other Department Contractor that may be impacted by or have a dependency on the change • A process flow that clearly outlines the life cycle of a CR • Roles and responsibilities • Approach to monitoring change requests through their lifespan to ensure timely resolution • Approach to communicating changes to internal and external stakeholders • Approach to status tracking and escalation for at-risk CRs	DDI	As Needed	None
MES-DEL-PM-005	Requirements Traceability Matrix (RTM)	Document that contains a matrix which shows bi-directional traceability with applicable testable and non-testable contractual requirements and their realization throughout all project phases (e.g., requirements, design, testing, and Streamlined Modular Certification (SMC) checklist items). This should include how the requirement is realized (e.g., configuration, custom development, base functionality). All revisions must be reviewed and approved by the State. The matrix will contain the following at a minimum: • Requirement number and description. • Definition of how the requirement will be satisfied. • Physical mapping of the requirement to the specific artifact.	DDI / O&M	As Needed	State Provided
MES-DEL-PM-006	Project Work Plan	Document which details a comprehensive work plan, with Gantt Chart, aligned with the project scope and Department requirements The document must include: • Identify planned completion dates for all deliverables and milestones.	DDI	Quarterly	State Provided

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Include key elements for the Department's Integrated Master Schedule (IMS), such as major phase dates, milestones, vendor integration points, and dependencies (including cross-modules). • Be regularly updated and refined throughout the project, with baseline schedules maintained for comparative reporting. • Reflect any approved changes through the Change Request Management Process and be re-baselined as needed.			
MES-DEL-PM-007	Agile Approach	Document that describes the Vendor's overall agile methodology and approach to program increment (PI) planning and sprint planning that includes, at minimum: • Defined roles and responsibilities • Number of agile ceremonies (sprints, feature refinement, design sessions) • Program increment planning – provide a PI Schedule and describe what the Vendor does within a PI • Description of tools used during program increments and sprints • Backlog management prioritization process – how product backlogs are refined, prioritized and maintained • Definition of "Done"- how to ensure consistent quality and completion criteria across features, stories and releases • Integration and testing approach – how continuous integration, test automation and quality gates are embedded in sprints	DDI	As Needed	None
MES-DEL-PM-010	Project Performance Measures	Document that provides performance measures related to ongoing project progress. It describes how the performance measures and success criteria will be monitored and reported on throughout the project lifecycle. At a minimum, these measures shall relate to scope, schedule, and budget performance areas. Additionally, the document contains project performance measures that will be used to determine if the stated project objectives have been met by the close of the project. These measures should be specific, measurable, and attainable within the project scope, time, and budget.	DDI	Once	None
MES-DEL-PM-011	Implementation Cutover Plan	Document which provides a more detailed view of the high-level tasks, pre-launch cutover tasks captured in the project schedule and must be kept in sync with that document. The Plan will contain the following information: • The rollout approach • Overall integration approach	DDI	Once	DED Required

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Approach to continuous integration of other modules or data from other data providing entities. • The proposed Implementation Schedule. • The rollback strategy. • Communication and Vendor support procedures. • Contractor and State roles and responsibilities. • Operational Readiness Checklist(s) that defines, in advance, the go/no-go decision, and all aspects of Vendor, solution, and State readiness. • All critical tasks that are required for cutover. • Post cutover monitoring. • The onsite (upon approval by state team) and offsite user support provided by the Vendor and State during the initial solution implementation. • Solution acceptance procedures. • Tools and processes to ensure overall quality. • Describe post implementation production deployment process and activities. • Post-implementation evaluation (includes metrics for measurement of successful implementation)			
MES-DEL-SEC-001	System Security Plan (SSP)	Document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems. The document will use industry-standard templates, such as FedRAMP or NIST, to ensure alignment with compliance requirements.	DDI / O&M	Annually	None
MES-DEL-SEC-002	Privacy & Security Incident Management Plan	Document that contains a plan to manage privacy and security incidents 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.	DDI / O&M	Annually	None
MES-DEL-SEC-003	Business Continuity Plan	Document providing details for a business continuity plan that must include the following:	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Identification of the core business processes involved in the production solution. For each core business process include: - Identification of potential failures for the process. - Risk analysis - Impact analysis and Definition of minimum acceptable levels of service/output. - Definition of triggers for activating contingency plans. • Definition of triggers for activating contingency plans. • Procedures for activating any special teams for business continuity. • A plan for recovery of business functions, units, processes, human resources, and technology infrastructure. • Communication protocols and process for restoring operations in a timely manner.			
MES-DEL-SEC-004	Disaster Recovery Plan	Document providing details for a disaster recovery plan that must include the following: • Retention and storage of backup files and software. • Hardware backup for critical solution components. • Facility backup. • Backup for any telecommunications links and networks. • Backup procedures and support to accommodate the loss of any online communications. • A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility. • The off-site storage facility must provide security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations. • An enumeration of the prioritized order of restoration for Contractor's proposed solution. • Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	DDI / O&M	As Needed	None
MES-DEL-SEC-005	Privacy Impact Analysis	Document that details the privacy impact of each module or module component that includes the following information: • Use of personally identifiable information (PII) or personal health information (PHI) and a description of the types of data that will be collected	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Sources of PII/PHI, populations, and transfer and disclosure mechanisms • Legal environment (legal authorities and state privacy laws) • Details about the entities with which the collected information will be shared • Privacy and security standards for its business partners and other third parties and the agreements that bind these entities • Incident handling procedures • Privacy and/or security awareness programs and materials for its workforce			
MES-DEL-SEC-006	3rd Party Privacy Security Assessment	The Vendor must provide access to the infrastructure and systems for the State-hired third-party vendor to perform the privacy & security assessments in compliance with the latest NIST 800-53 requirements overlaid with the HIPAA privacy & security requirements and the penetration testing results. If the Vendor has obtained a HITRUST CSF for their solution (not the cloud service provider HITRUST CSF), the State may accept the HITRUST CSF as an equivalent for 3rd Party Privacy Security Assessment. The Vendor needs to provide detailed HITRUSTCSF assessment reports, not just a certification letter.	DDI / O&M	Bi-Annually	None
MES-DEL-SEC-007	Disaster Recovery/Business Continuity Test Report	Report which contains the test results of an annual test of the Disaster Recovery Plan and Business Continuity Plan. The report includes the After-Action report, test results, outcomes, corrective action plan, and revisions, if any, to the Department.	DDI / O&M	Annually	None
MES-DEL-SEC-008	Penetration Test Report	Report from an independent third party which has performed penetration testing within 90 Days prior to implementation. Penetration testing must also be performed by an independent third party on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists. Penetration Test Report results must be supplied to the Department and any critical or high vulnerabilities mitigated.	DDI / O&M	Annually	None
MES-DEL-SEC-009	IT System Risk Assessment	Document which contains results and outputs from an internal risk assessment conducted by the Vendor. The assessment will be in compliance with the latest NIST 800-53 and HIPAA privacy & security controls. The assessment will be performed on an annual basis and when additions or changes to system functionality impact the security framework, architecture or when a new vulnerability exists. The results and outputs of the assessment will be documented and submitted to the State.	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
MES-DEL-SEC-010	Service Organization Control (SOC) 2 Type II Report	The Vendor must provide a completed Security Audit Report with results 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 or current NIST 800-53 assessment at a "moderate" system risk control level.	O&M	Annually	None
MES-DEL-SEC-011	CMS Information Security Program Plan of Action and Milestones (POA&M)	The Vendor must respond to all risks identified through the periodic security risk assessments with a CMS Information Security Program 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. Vendor should use the FedRamp template.	O&M	As Needed	None
MES-DEL-STAF-001	Staffing Plan	Document containing a staffing plan that must include: • Identify the roles and responsibilities by resource type throughout all phases of the contract, including identifying key and non-key personnel as well as FTE allocation for all personnel. Clearly differentiate between Contractor staff and subcontractor staff. • Provide estimated staffing levels by resource type for each project phase • Detail how the staffing levels shall achieve consistent, dependable service regardless of changes that may influence work volume. • Identify total hours to be expended, per phase or effort, and for the entire project, by Proposer staff and by State project staff. • Tools and processes used to screen available staff and fill positions. • Expectations regarding onsite time for contractor resources. • Process for temporarily and permanently replacing vacancies in key personnel and other manager/lead positions. • Detail how the staffing levels shall achieve consistent, dependable service for handling sudden and unexpected increases in volume of transactions or the number of users.	DDI	Once	None
MES-DEL-TRN-001	Training Plan and Schedule	Document that describes the Vendor's cohesive and responsive training to ensure that all users can be efficient and effective while using the system, including 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	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		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. 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. The plan must also include the following: • User Data: The Contractor must develop a User Training Plan that explains the data available to each user type and how to sign on and access that data. • Summary of training approach that focuses on the train-the-trainer methodology, objectives, and desired outcomes. • Training needs analysis, including an assessment of the target audience and their knowledge and skills. • Recommendations on type and delivery approach based on training needs analysis. • Summary of proposed training materials and documentation in addition to hands-on training. • Approach to maintaining training documentation and accompanying materials. • Approach to providing training necessary to support new functionality and/or major software releases that materially change the user interaction. • Approach to processing for incorporating feedback to improve train the trainer effectiveness over the course of the Contract. • Approach to conducting dry runs for training sessions.			
MES-DEL-TRN-002	Training Guides and Materials	Documents providing training guides and materials that includes: • Computer-based training (CBT) courses • Instructor-led training courses in a location in accordance with program requirements	DDI / O&M	Annually	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Secure, browser-based, Web-enabled tutorials in the content, frequency, format, and all media as directed by the State The Vendor must produce initial and ongoing updates to training materials and assess the training needs of end users prior to implementation by meeting with subject matter experts for the different functions to be performed and will design training methods that will meet the established goals as identified in the training requirements.			
MES-DEL-TRN-003	Functional Design Documentation	The Vendor must provide User Documentation during the DDI phase of the project for use during UAT and maintained throughout the project for final review and submission prior to Go Live. The State requires User Documentation for use by a novice business user to understand the automated system or application from a business function perspective. The Vendor must provide comprehensive, well-organized user documentation. The Vendor's User Documentation must include at a minimum: • User documentation must be written and organized so that novice users can learn from reading the documentation how to access the on-line windows/screens, read reports, and perform all other user functions. Should be written in a procedural step-by-step format. (Instructions for sequential functions must follow the flow of actual activity). • Manuals that help users understand the purpose and operation of the module/module component(s) for each business process/major program/functional area. Should cover system navigation, online help, and policies and procedures. • Acronyms and abbreviations used in user instructions must be identified and must be consistent with windows, screens, reports, and the data element dictionary. • The documentation must be available on-line and provide an on-line search capability with context-sensitive help. • Provide the ability to produce a PDF version upon request • Use version control to retain historical versions of documentation and revisions must be clearly identified. • User manuals must contain a table of contents and an index. • Definitions of codes used in various sections of a user manual must be consistent.	DDI	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Descriptions of error messages for all fields incurring edits must be presented and the necessary steps to correct such errors must be provided. • Each user manual must contain a section describing all reports generated within the subsystem, which includes the following: - A narrative description of each report. - The purpose of the report. - Definition of all fields in the report, including detailed explanations of calculations used to create all data and explanations of all subtotals and totals. • Definitions of all user-defined, report-specific code descriptions; and a copy of representative; and pages of each report. Instructions for requesting reports or other outputs must be presented with examples of input documents and/or screens. • Instructions for making on-line updates must clearly depict which data and files are being changed.			
MES-DEL-TST-001	Master Test Plan	Document that describes the Vendor's plan for all testing activities, processes, types, and levels. Testing must be as automated and self-documenting as possible (e.g., continuous unit testing). This plan must be aligned with CMS's Testing Guidance Framework. At a minimum, the Master Test Plan must address the following: • Overall testing strategy for the testing types defined in Section 7.17 Testing of the RFP • Approach to planning and preparing the necessary environments as described in Section 7.17 Testing of the RFP. • Approach for testing nonfunctional requirements. • Approach to test documentation • Approach to quality control/quality assurance. • Tools, techniques, and methods. • Reporting mechanisms, traceability, and metrics. • Defect management including: - Approach and tools utilized to collect, assign, identify, prioritize, track, manage, resolve, and test system defects reported by the Department, other Department Contractors, or other personnel authorized by the Department. - Approach to defect severity categorization. - Approach to reporting and documenting defects. Defect reports should include at a minimum the current defect list (with frequency	DDI	As Needed	None

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		and severity), associated implementation timelines, and information on operational impact. - Describe aging information to track how long defects are taking to resolve. - Describe the defect management processes related to all test types and levels in Section 7.17 Testing of the RFP (e.g., the relationship between defect resolution and the coordinated test case execution). - Describe the defect management processes after implementation. • Entrance and exit criteria for each test level • Configuration management for each test level • Testing roles and responsibilities for vendor and Department • Acceptance Criteria • Test Coverage • Walkthroughs, Inspections, and Demos • Test Data Considerations • Inputs to and outputs of System Testing • Pass/Fail Criteria • Suspension Criteria and Resumption requirements • Meetings and Communication • Applications or systems that are part of the testing • Integrations that are part of the testing • Test environment build and maintenance • Test scenario, case, and result traceability to contract requirements • Test schedule • Approach to working collaboratively with other State healthcare programs enterprise Contractors • Constraints and assumptions and all associated dependencies • Approach to testing compliance with Section 508 accessibility requirements • Testing scope, including what is out of scope			
MES-DEL-TST-002	Performance Test Results	Document providing test results demonstrating that the solution meets all Service Level Agreements for system performance	DDI	As Needed	None
MES-DEL-TST-003	Testing Results	Document providing testing results for each applicable test phase listed in Section 7.17 Testing that include: • Executed test cases • Mapping of executed test cases to the associated contract requirement	DDI	As Needed	DED Required

Deliverable ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Mapping of executed test cases to their artifacts and results • Executing tester for each test case • Date of execution • Pass/fail status • Registry of open, closed, and deferred defects • Screenprints, test results, and artifacts No test phase will be considered complete until the Department reviews and approves of the testing results. Depending on the testing methodology, these results may be submitted in phases.			

Table N-1 Deliverables

2.0 MILESTONES AND ACCEPTANCE CRITERIA

The milestone information shown in *Table N-2 Milestones* includes defined milestones ("events") representing meaningful progress points during the execution of the DDI phase of the DAP Solution project. The Vendor must provide the duration associated with each milestone in *Table N-2 Milestones* to support the reasonableness of the proposed schedule. The Vendor must also provide the proposed cost for each milestone in *Sheet 2. DDI Milestone Costs* included in the Cost Proposal Workbook referenced in *Attachment E: Cost Form*.

Each milestone includes:

- ID: Identifier of the milestone.
- Milestone: Name of the milestone.
- Scope: Scope of the of the activities to be completed during the milestone.
- Acceptance criteria: Criteria required to be met before milestone considered complete.
- Deliverables: Deliverables that must be submitted and approved in PCDU.
- Prior Milestones: The milestone(s) that are required to be completed before the current milestone can be approved.
- Duration: Number of weeks to perform the milestone activities and meet the acceptance criteria for the milestone.

These milestones will form the basis for a significant portion of the project's Implementation payment schedule. Milestone payments will be made only upon the Department's approval the milestone has been fully achieved in accordance with acceptance criteria provided. The Vendor is encouraged to submit a milestone's deliverables as they are completed rather than waiting and submitting all the deliverables associated within a milestone at one time. For specific deliverables referenced in multiple milestones where the acceptance criteria indicate only relevant sections of the specific deliverable

will be reviewed, the relevant sections of the deliverable to be reviewed will be identified and mutually agreed upon by the Vendor and the Department prior to deliverable submission.

Following the award of the contract, the State will work with the Vendor to finalize the timeline and milestones. Any changes to the milestone schedule, acceptance criteria, or associated payments will require a formal contract amendment approved by the State.

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
1	Planning & Discovery Complete	Define project scope, timelines, resources, and governance. Assess current state, gather requirements, identify gaps.	Relevant deliverables approved by stakeholders. Roles and responsibilities assigned. Current State Discovery document finalized and signed off. Requirements documented.	• (MES-DEL-PM-001) Project Management Plan • (MES-DEL-PM-006) Project Work Plan • (MES-DEL-PM-007) Agile Approach • (MES-DEL-STAF-001) Staffing Plan • (MES-DEL-PM-002) Quality Management Plan • (MES-DEL-COMM-001) DDI Communication Plan • (MES-DEL-PM-003) Risk and Issue Management Plan • (MES-DEL-PM-010) Project Performance Measures • (MES-DEL-PM-004) Change Management Plan and CR Approval Process • (MES-DEL-PM-005) Requirements Traceability Matrix (RTM) • (MES-DEL-INT-001) System Interface Design Strategy • (MES-DEL-AI-001) GenAI Disclosure and Fact Sheet	None	
2	Infrastructure - Design and Approvals Complete	Design target infrastructure architecture and get necessary approvals.	Relevant deliverables approved.	• (MES-DEL-ARCH-005) MES Architecture Documentation (Initial) • (MES-DEL-ARCH-010) System Design Document (Initial) • (MES-DEL-INT-002) Interface Control Document • (MES-DEL-OM-002) Capacity Plan • (MES-DEL-SEC-001) System Security Plan (SSP) • (MES-DEL-SEC-002) Privacy & Security Incident Management Plan • (MES-DEL-SEC-005) Privacy Impact Analysis	None	

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
3	Infrastructure - Capabilities Enablement - Foundational Capabilities (Data warehouse, Audit, security, data management, integration, ingestion and consumption, tools, advanced analytics) Set up	Provision core infrastructure (networking, compute, storage).	Foundational components deployed, validated, demo completed and approved. Relevant deliverables approved.	• (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2	
4	Infrastructure - Capabilities Enablement - Disaster Recovery Set up	Implement DR strategy and configure backup/recovery.	DR environment configured, tested successfully, demoed and approved. Relevant deliverables approved.	• (MES-DEL-SEC-004) Disaster Recovery Plan • (MES-DEL-SEC-007) Disaster Recovery/Business Continuity Test Report • (MES-DEL-SEC-003) Business Continuity Plan • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3	
5	Infrastructure - Capabilities Enablement - DevOps Set up	Set up CI/CD pipelines, version control, and automation tools.	DevOps pipelines operational and integrated with source control, demo completed and approved. Relevant deliverables approved.	• (MES-DEL-OM-005) Release Management Plan • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3	
6	Migration - Data Model Design Complete	Design target data models for new platform.	Data model documentation approved.	• (MES-DEL-ARCH-001) Data Architecture (Relevant Sections) • (MES-DEL-ARCH-001) Data Architecture Document - Logical Data Model (LDM) Document • (MES-DEL-ARCH-001) Data Architecture Document - Conceptual Model Data (CDM)	1, 2	
7	Migration - New Data Products Design Complete	Define new data products and their specifications.	Design documents for new data products approved.	• (DAP-DEL-DMD-001) Data Pipelines Documentation (Relevant Sections) • (MES-DEL-ARCH-001) Data Architecture (Relevant Sections)	1, 2, 6	

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
8	Testing - Security and Penetration Testing Complete	Conduct security assessments and penetration tests.	No critical vulnerabilities found; reports approved.	• (MES-DEL-SEC-008) Penetration Test Report • (MES-DEL-SEC-009) IT System Risk Assessment • (MES-DEL-SEC-006) 3rd Party Privacy Security Assessment	1, 2, 3, 4	
9	Infrastructure - Capabilities Enablement - DAP ready for Data	Prepare Data Analytics Platform (DAP) for ingesting data.	DAP environment provisioned and validated for data ingestion. Demo completed and approved by Business. Relevant deliverables approved.	• (DAP-DEL-MIGR-001) Solution Migration Design • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized) • (MES-DEL-TST-001) Master Test Plan (Relevant Sections)	1, 2, 3, 4, 5, 6, 7, 8	
10	Infrastructure - Capabilities Enablement - Data Observability Set up	Implement monitoring for data pipelines and infrastructure.	Observability tools configured with alerts and dashboards. Data dry runs and demo completed on live data and approved by Business. Relevant deliverables approved.	• (DAP-DEL-MMM-001) Monthly Observability Summary • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3	
11	Infrastructure - Capabilities Enablement - Data Governance Tool Set up	Deploy tools for data cataloging, lineage, and policy enforcement.	Governance tools operational and integrated with data sources. Demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Relevant Sections) • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3	
12	Infrastructure - Capabilities Enablement - Infrastructure as Code Set up	Implement IaC for repeatable infrastructure provisioning.	IaC scripts deployed and tested in at least one environment. Demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3, 5	
13	Infrastructure - Capabilities Enablement - Automated Testing Set Up	Set up automated testing for data quality and pipelines.	Automated tests implemented and passing in CI/CD. Demo completed and approved by Business.	• (MES-DEL-TST-001) Master Test Plan (Relevant Sections) • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized)	1, 2, 3, 5	

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
			Relevant deliverables approved.	• (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized) • (MES-DEL-PM-005) Requirements Traceability Matrix (RTM)		
14	Infrastructure - Capabilities Enablement - ODS Set Up	Deploy Operational Data Store for real-time/near-real-time data.	ODS deployed and integrated with source systems. Demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-ARCH-001) Data Architecture (Relevant Sections) • (MES-DEL-ARCH-005) MES Architecture Documentation (Relevant Sections finalized) • (MES-DEL-ARCH-010) System Design Document (Relevant Sections finalized)	1, 2, 3, 9	
15	Infrastructure - Capabilities Enablement - Complete	All infrastructure capabilities fully deployed and validated.	All infrastructure milestones completed and signed off. Demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-CERT-003) Operational Readiness Review Checklist • (MES-DEL-ARCH-006) Configuration/Customization Plan • (MES-DEL-ARCH-005) MES Architecture Documentation (All Parts finalized) • (MES-DEL-ARCH-010) System Design Document (All Parts finalized)	1, 2, 3, 4, 5, 8, 9, 10, 11, 12, 13, 14	
16	Migration - Data Integration from Source to Bronze Layer Complete	Ingest raw data from source systems into Bronze layer.	Data pipelines from source to Bronze operational, demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Relevant Sections) • (DAP-DEL-DMD-001) Data Pipelines Documentation (Relevant Sections)	6, 9	
17	Migration - Data Pipelines from Bronze to Silver Layer Complete	Transform raw data into cleansed, structured Silver layer.	Silver layer pipelines deployed and data quality validated, demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Relevant Sections) • (DAP-DEL-DMD-001) Data Pipelines Documentation (Relevant Sections)	6, 9, 16	
18	Migration - Existing Data Products Migration and New Data Products Development Complete into Gold Layer	Rebuild or migrate existing data products to new platform.	All legacy data products migrated, demo completed and approved by Business.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Relevant Sections)	6, 7, 9, 17	

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
			Relevant deliverables approved.	• (DAP-DEL-DMD-001) Data Pipelines Documentation (Relevant Sections)		
19	Migration - Migration and Conversion of Reports and Dashboards Complete	Recreate or migrate BI reports and dashboards.	Reports and dashboards validated against legacy outputs, demo completed and approved by Business.	No associated deliverables	18	
20	Migration - Data Catalog and Business Glossary for Migrated Assets Complete	Document and catalog all migrated data assets.	Data catalog and glossary updated and published, demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (Relevant Sections) • (MES-DEL-ARCH-001) Data Architecture Document - Data Dictionary (Electronic)	11, 16, 17, 18, 19	
21	Migration - Data Migration Complete	Migrate historical and current data to target platform.	Data migration completed with reconciliation and validation, demo completed and approved by Business. Relevant deliverables approved.	• (MES-DEL-DATA-001) Data Management, Conversion and Migration Plan (All Sections) • (MES-DEL-DATA-002) Data Conversion Test Results (Initial)	1 through 20	
22	Testing - Infrastructure SIT Complete	System Integration Testing of infrastructure components.	SIT test cases executed and passed.	• (MES-DEL-TST-003) Testing Results (Relevant Sections)	1, 2, 3, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15	
23	Testing - Data Pipelines SIT Complete	SIT for data pipelines from source to Silver layer.	SIT test cases executed and passed.	• (MES-DEL-TST-003) Testing Results (Relevant Sections)	9, 16, 17, 18, 22	
24	Testing - Reports and Dashboards SIT Complete	SIT for BI layer reports and dashboards.	SIT test cases executed and passed.	• (MES-DEL-TST-003) Testing Results (Relevant Sections)	9, 19, 22, 23	
25	Testing - Infrastructure UAT Complete	User Acceptance Testing of infrastructure readiness.	UAT sign-off from infrastructure stakeholders.	No associated deliverables	22	
26	Testing - Data Pipelines Output UAT Complete	UAT for the data loaded in the tables created by the data pipelines.	UAT sign-off from pipelines stakeholders	No associated deliverables	23	
27	Testing - Reports and Dashboards UAT Complete	UAT for business reports and dashboards.	UAT sign-off from reports and dashboards stakeholders	No associated deliverables	24	

ID	Milestone	Scope	Acceptance Criteria	Deliverables	Prior Milestones	Duration
28	Testing - Performance Testing Complete	Validate system performance under load.	Performance benchmarks met or exceeded.	• (MES-DEL-TST-002) Performance Test Results	22, 23, 24	
29	Testing - End to End Testing Complete	Full workflow testing from ingestion to reporting.	End-to-end testing executed successfully.	• (MES-DEL-TST-003) Testing Results (Relevant Sections)	25, 26, 27	
30	Testing - Parallel Run	Run legacy and new systems in parallel for comparison.	Results match across systems; discrepancies resolved.	• (MES-DEL-TST-003) Testing Results (All Sections)	29	
31	Cutover - Final Data Migration and Testing Complete	Final sync of data and validation before go-live.	Final data load completed and validated. Relevant deliverables approved.	• (MES-DEL-PM-011) Implementation Cutover Plan • (MES-DEL-DATA-002) Data Conversion Test Results (Final) • (MES-DEL-PM-005) Requirements Traceability Matrix (RTM)	30	
32	Cutover - Change Management Planning Complete	Prepare users and stakeholders for transition.	Change management plan approved and communicated.	• (MES-DEL-TRN-001) Training Plan and Schedule • (MES-DEL-TRN-002) Training Guides and Materials • (MES-DEL-TRN-003) Functional Design Documentation	25, 26, 27	
33	Cutover - Pre-Go Live User Training Complete	Train end users on new tools and processes.	Training sessions completed; materials distributed.	No associated deliverables	25, 26, 27, 32	
34	Cutover - Go Live Successfully Completed	Transition to production environment.	System live with monitoring in place and no critical issues. Relevant deliverables approved.	• (MES-DEL-CERT-001) Certification Plan • (MES-DEL-CERT-002) CMS Operational Report Workbook • (MES-DEL-OM-001) Operations, Maintenance and Configuration Plan • (MES-DEL-OM-004) Operations Procedure Manual • (MES-DEL-COMM-002) Operations Communications Plan • (MES-DEL-ARCH-012) Section 508 Compliance Test Report	1 through 33	

Table N-2 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. Serer 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. 143-59.1and -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

The undersigned states that:

1. **He or she is the duly authorized representative of the Vendor named below;**
2. **He or she is authorized to make, and does hereby make, the following certifications on behalf of the Vendor, 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 Vendor **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 Vendor **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. Describe how the Vendor can require its subcontractors, if any, to make the same certifications and disclosure.

_____

Signature Title

_____

Vendor Name **Date**

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

I. Certification Regarding Nondiscrimination

The Vendor 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 Vendor 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 Vendor'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 Vendor'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 thirty (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

_____
City, State, Zip Code

_____
Street

_____
City, State, Zip Code

3. Vendor 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 Vendor certifies that it will comply with the requirements of the Act. The Vendor 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 Vendor.]

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, 45 CFR Part 76. 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 Non-Procurement 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 Vendor 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 sub-awardee 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 sub-awardee, e.g., the first sub-awardee 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 "Sub-awardee", 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)

1.Type of Federal Action: a. Contract b. Grant c. Cooperative agreement d. Loan e. Loan guarantee f. Felon 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_____ Quarter_____ Date of Last Report:_____

4.Name and Address of Reporting Entity: Prime Sub-awardee Tier (if known) _____ Congressional District (if known) _____	5.If Reporting Entity in No. 4 is Sub-awardee, Enter Name and Address of Prime: Congressional District (if known) _____
6.Federal Department/Agency:	7.Federal Program Name/Description: CFDA Number (if applicable)
8.Federal Action Number (if known)	9.Award Amount (if known) $
10.a.Name and Address of Lobbying Entity (*if individual, last name, first name, MI*): (*attach Continuation Sheet(s) SF-LLL-A, if necessary*)	10.b. Individuals Performing Services (*including address if different from No. 10a.*) (*last name, first name, and MI*): (*attach Continuation Sheet(s) SF-LLL-A, if necessary*)
11.Amount of Payment (*check all that apply*): $ _____ □ actual □ planned	13.Type of Payment (*check all that apply*): a. Retainer b. One-time fee

	c. Commission d. Contingent fee e. Deferred f. Other; specify:
12.Form of Payment (*check all that apply*): a. Cash b. In-kind; specify: Nature_____ Value _____	
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*):	
15.Continuation Sheet(s) SF-LLL-A attached: Yes or 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: ___ Title: _____ Telephone No: _____ 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 [Enter Name of Contractor] ("Business Associate") (collectively the "Parties").

1. BACKGROUND

a. Covered Entity and Business Associate are parties to an agreement entitled **30-2025-008-DHB Data Analytics Platform**, 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 Date
Title

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

_____ _____

Melanie Bush Date
Deputy Secretary
NC Medicaid

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 Requirements*. 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 or the Solution 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	Scope of Work: Solution Overview	10
Section 3.1.2	Scope of Work: Solution Development Activities	30
Section 3.1.3	Scope of Work: Platform Enablement	20
Section 3.1.4	Scope of Work: Assets Migration and Validation	10
Section 3.1.5	Scope of Work: Data Management and Governance	5
Section 3.1.6	Scope of Work: Data Products	5
Section 3.1.7	Scope of Work: Ongoing Support and Operations	5
Section 3.1.8	Scope of Work: Consulting Services	2
Section 3.1.9	Scope of Work: Staffing	2
Section 3.2.5	Enterprise Licensing	5
Section 3.4.2	Architecture Diagrams	n/a
Section 7.1	Vendor Utilization of Workers Outside the US	2
Section 7.4	Vendor's License or Support Agreements	n/a
Section 7.11	Project Management	5

Vendor to provide a response for all Specifications in the tables provided in *Section 3.6.1 Specifications*. 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 Specifications* in this RFP are ranked in descending order of importance.

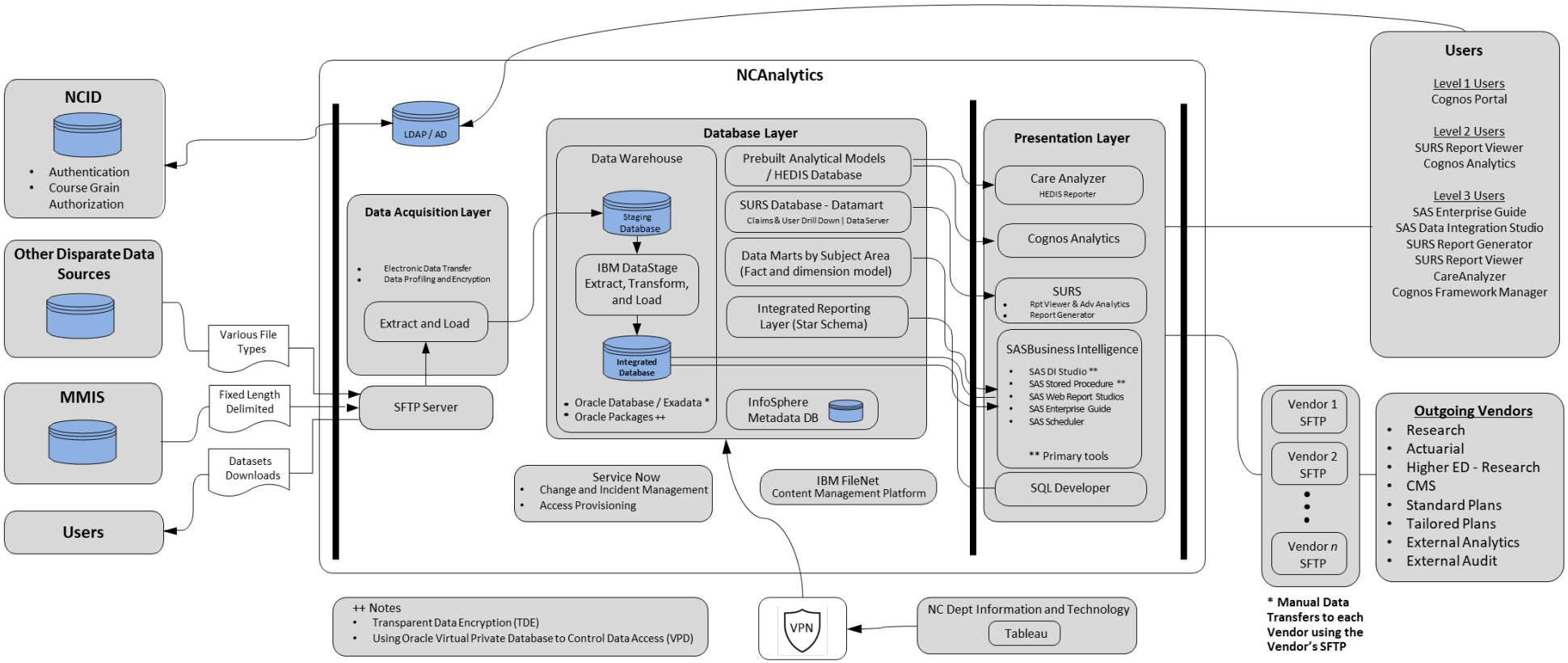
RFP Section	Area	Page Limitation
Section 3.6.1: Table S1	Platform Architecture	n/a
Section 3.6.1: Table S2	Data Flow Architecture	n/a
Section 3.6.1: Table S3	Migration	n/a
Section 3.6.1: Table S4	Workflow Management and Performance	n/a
Section 3.6.1: Table S5	Data Governance and Management	n/a

RFP Section	Area	Page Limitation
Section 3.6.1: Table S6	Operations	n/a
Section 3.6.1: Table S7	Project Management	n/a
Section 3.6.1: Table S8	Testing	n/a
Section 3.6.1: Table S9	Security and Compliance	n/a
Section 3.6.1: Table S10	Cost & Resource Management	n/a
Section 3.6.1: Table S11	Training & User Adoption	n/a
Section 3.6.1: Table S12	Program Integrity	n/a
Section 3.6.1: Table S13	Advanced Analytics & AI	n/a
Section 3.6.1: Table S14	Transition	n/a
Section 3.6.1: Table S15	Certification	n/a

ATTACHMENT U: CONCEPTUAL ARCHITECTURAL DIAGRAMS

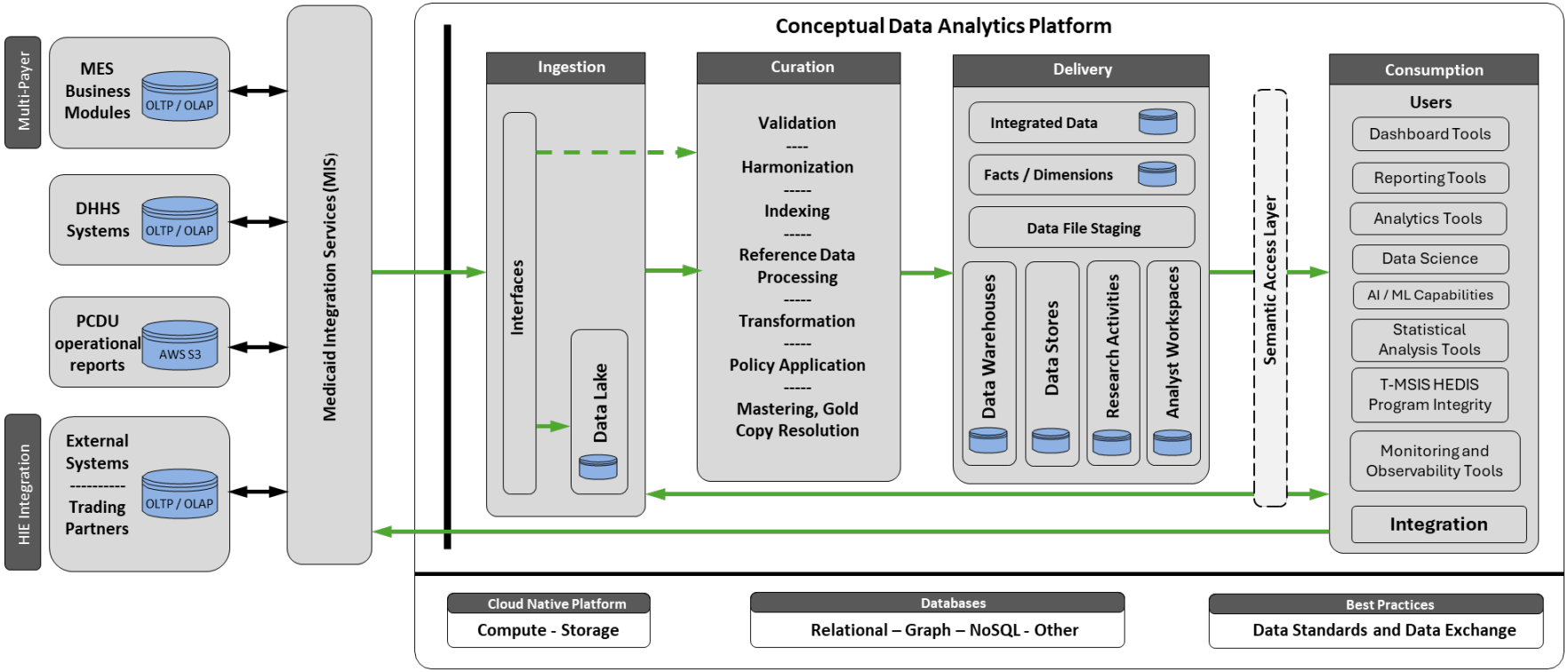
The following architectural diagram provides the high-level current state for the module.

.



The following architectural diagram provides the intended future state of the Data Analytics Platform

The future state diagram included in this RFP is intended as a high-level conceptual view for understanding purposes only. Vendors are encouraged to propose alternative architecture diagrams or approaches that meet the stated requirements and align with best practices, provided they support the overall requirements of the solution.



MES Business Modules

- Claims
- Encounters
- Pharmacy
- Provider Enrollment
- Member Eligibility and Enrollment
- Prior Authorization
- Electronic Visit Verification
- Health Plan Operational Data
- Appeals and Grievances
- Care Management
- Third Party Liability
- Finance
- Reference Data

Data Management

- Data Governance
- Data Architecture
- Data Modeling and Design
- Data Storage
- Data Operations
- Data Security
- Data Quality Monitoring
- Data Integration and Interoperability
- Documents and Content
- Reference Data
- Metadata
- Data Quality
- Audit Trails

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 a Medicaid Integration Services platform (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 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 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 traffic management	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 Act as a consumer for the other module vendor APIs

S No.	Type of API	Description	MIS API Gateway	MIS API Management Portal	Module Vendor Interaction
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 access end point. 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 platform **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:

i. Secure FTP (SFTP (SSH File Transfer Protocol, FTPS, and Secure Copy Protocol (SCP)) for protected file transfer;
ii. 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.

The architectural diagram showing the design for NCID coarse-grained authorization and SAML flow for single-sign-on is provided in Figure V1 below.

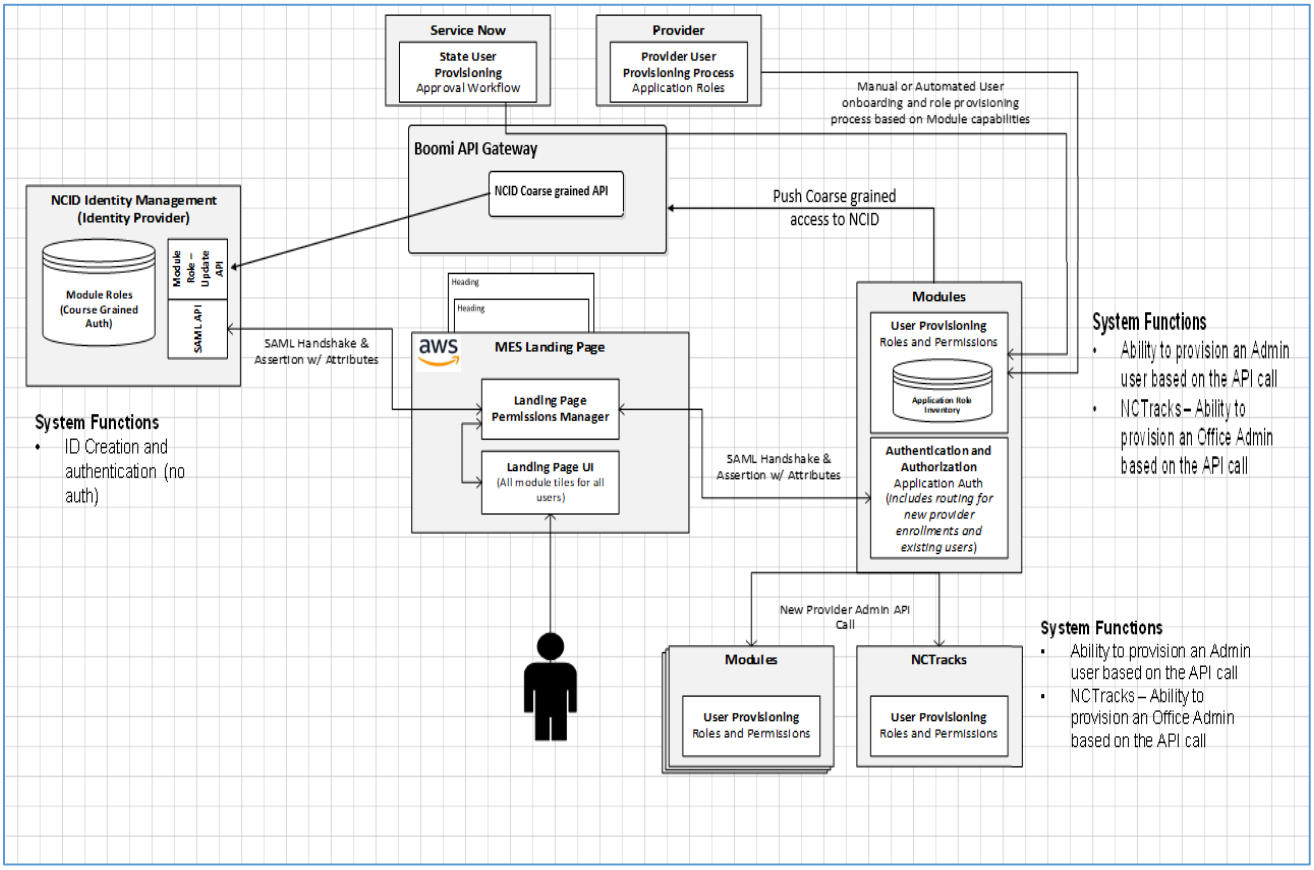


Figure V1 – Architectural Diagram showing NCID and SAML

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 NCDHHS 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

1.0 WORK PRODUCTS

Work products are incidental artifacts created during the performance of the contract. 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.*

Table W-1 Work Products lists the work products to be provided by the Vendor for this project. The information for each work product includes:

- Work Product ID: Unique identifier of the work product.
- Title: Name of the work product.
- Description: A summary of the elements to be included in the work product.
- Phase / Stage: The phase of the project when the work product is expected to be delivered.
- Frequency / Updates: Indicates how often the work product is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the work product. The meaning of the values is as follows:
    1. None – No preferred template exists. The Vendor is free to provide the deliverable in its own format and content.
    2. State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Work Product ID.

Note: The Work Product ID assigned to each work product in *Table W-1 Work Products* may not always be sequentially numbered. Any apparent gaps in the numbering sequence are intentional.

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
MES-WP-CERT-001	Certification Crosswalk Report	Document that describes how the Vendor's deliverables and other documentation align with federal certification requirements and milestone reviews. The Vendor must produce reports on this crosswalk at the direction of the Department.	O&M	As Needed	None
MES-WP-OM-001	Major | Minor Release Notes	Electronic notifications including detailed release notes for Major and Minor version, patches, updates and fixes deployed to the production environment.	DDI	As Needed	None
MES-WP-OM-002	Release Milestones and Updates	Document containing the schedule of system releases, updates, maintenance, and milestones for the next 45 days. This will be submitted to the Department weekly on Fridays.	DDI	Weekly	None

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
MES-WP-OM-003	Root Cause Analysis (RCA)	Document that adheres to the format defined by the Department. The RCA must detail the causes, impacts, downtime, and remediations required to resolve any issue. The Vendor must ensure the RCA includes mitigations and corrective actions to prevent future interruptions. The RCA must be submitted within seventy-two hours following the resolution of the failure.	DDI / O&M	As Needed	State Provided
MES-WP-PM-001	Vendor Kickoff Presentation	A presentation jointly developed by the Vendor and the Department which will be presented by the Vendor to the Department. The presentation will provide a clear overview of the project implementation plan, and module overview which marks the formal kickoff of the project with the business.	DDI	Once	None
MES-WP-PM-002	Meeting Agendas, Minutes, and Documentation	Document which contains information containing the capture and dissemination of agendas, meeting minutes and documentation necessary for successful execution of the project.	DDI	As Needed	None
MES-WP-PM-003	Lessons Learned (with Evaluation) Report	Document that records all lessons learned throughout the project. The lessons learned will be ongoing and will be used to enhance build strategies on subsequent builds to gain greater efficiency and effectiveness into process. Lessons learned will be shared among the DDI team in partnership with the Department. Lessons learned will be incorporated into the Vendor's overall quality management process. Lessons learned will also be a key element of our approach to configuration/change management and process improvement. The Vendor must also hold a walk-through meeting of the results and provide an evaluation report for all engagements.	DDI	As Needed	None
MES-WP-PM-004	Program Increment (PI) Release Plan	Release Plan submitted within five business days of completing each PI Planning Session. This Release Plan must include, at minimum: • Number of expected sprints • Estimated sprint duration • Targeted features for each sprint • Planned completion dates for features / Milestones and Key deliverables major checkpoints, reviews • Dependencies across features • Scope changes or variance • Capacity allocation – expected team velocity, allocation by team/role and how capacity is planned across sprints • Risk and Mitigation Plan – anticipated risks technology, dependency, resourcing etc. and mitigation strategies	DDI	Quarterly	None

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Integration and Deployment Plan – how increments will be integrated and tested and deployed • Metrics and Tracking – PI level indicator – predictability, scope stability, velocity, defect leakage • Change Management and Communication Plan – how changes to scope or timeline are communicated • Release readiness Criteria – what must be achieved before release or PI. Work product submission schedule will be determined in collaboration between the Vendor and the Department. Most organizations conduct PI planning events every 8-12 weeks.			
MES-WP-PM-005	Sprint Retrospective	Document compiled at the conclusion of every sprint. It captures the collective insights, performance metrics, and improvement actions identified during retrospective sessions across Agile teams. This work product supports continuous improvement by consolidating lessons learned and providing visibility into team dynamics, delivery challenges, and process enhancements. The document must include: • Sprint Overview: A brief summary of each sprint, including goals, key accomplishments, and any deviations from planned outcomes. • Progress Metrics - Mechanisms for tracking sprint progress to assess performance (Velocity trends, defect rates, test coverage, and automation percentages) to be reported on within the weekly project status. • Risks and Issues - Summary of any risks/issues encountered during the sprint, including their mitigation plan. • Retrospective Summary - Key takeaways from the sprint retrospective, including: • What Went Well: Highlights of successful practices, team collaboration, and delivery achievements. • What Didn't Go Well: Challenges encountered, including blockers, inefficiencies, or misalignments. • What To Improve: Actionable recommendations for process, tooling, or communication improvements. • Velocity tracking - story points completed vs. committed, with historical comparison to prior sprints. • Change log - updates on any new scope added, descoped, or deferred during the sprint. • Commitment status - updates on specific features, integrations, or milestones tied to the sprint.	DDI	As Needed	None

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Stakeholder engagement - feedback captured in Sprint Reviews or mid-sprint demos.			
MES-WP-PM-006	Program Increment (PI) Inspect and Adapt	Document submitted in coordination with the Inspect and Adapt session conducted at the conclusion of the Agile Program Increment. It serves as a formal retrospective and continuous improvement artifact documenting key insights, performance metrics, and actionable recommendations. The report should include: • Program Performance Review: A summary of objectives met, features delivered, and metrics tracked during the PI, including velocity, quality, and predictability indicators. • Problem-Solving Workshop Outcomes: Documentation of systemic issues identified during the PI, root cause analysis, and proposed corrective actions. This section highlights cross-team collaboration and resolution strategies. • Lessons Learned: A detailed account of successes and areas for improvement gathered from Agile teams, Product Management, and stakeholders. Topics include team dynamics, planning accuracy, dependency management, tooling effectiveness, and stakeholder engagement. • Improvement Backlog: A prioritized list of improvement items to be addressed in future PIs, including process enhancements, tooling upgrades, and training needs. • Business value achieved - comparison of planned PI Objectives vs. actual business value delivered • Trend analysis - comparison with prior PIs to show improvement or recurring challenges (e.g., predictability, scope stability). • Team health check - qualitative assessment of team morale, collaboration, and alignment with program values. • User feedback - insights gathered from demos, reviews, or user satisfaction surveys if any conducted during the PI. This report is intended to inform leadership, guide future PI planning, and reinforce a culture of transparency and continuous learning.	DDI	As Needed	None
MES-WP-TEST-001	Test Summary Result Report	For each test phase listed in Section 7.17 Testing of the RFP, the Vendor must submit a Test Summary Result Report and obtain Department approval to close the current test phase. This is comprehensive report that includes the following: • Overview of testing activities/Test Phase/Test Dates/Test Environment (configuration)	DDI	As Needed	None

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Total Number of Test Cases Executed • Test Case Final Execution Status (Passed/Failed/NA/Deferred/Date/Evidence of completion) • Total Number of defects Logged • Defect Final Execution Status (Passed/Failed/NA/Deferred/Date/Evidence of completion) • List of requirements covered during the test phase			
MES-WP-TEST-002	SIT/Parallel Test Scenarios and Cases	Document that details test scenarios and test cases for SIT / Parallel Tests. The document must include: • Positive and negative scenarios (which must include error handling and stressing the system with bad and invalid data) • Step-by-step instructions • Expected results • Actual results	DDI	As Needed	None
MES-WP-STAF-001	Organization Staffing Charts	Organization charts showing the number and type of staff resources to be assigned to a) the transition to Solution and b) subsequent operations, and maintenance. The former chart will focus on the requirements gathering and design phase of the project, while the latter will address steady-state operations. Each staffing chart must include: • Roles and qualifications of each proposed team member. • Include and identify any subcontractors and their proposed function. • Identify the geographic location of each proposed team member. • Identify any known changes throughout the term of the Contract (i.e. changes between implementation and steady-state operations). • Identify aggregate full-time equivalent projections and the assumptions used to generate those projections. • Include the named individual, the role they are filling and the time frame or project phases during which each individual/role will be required.	DDI / O&M	As Needed	None
DAP-WP-CUR-001	Data Flows	Document that details all ETL/ELT and data flows, including source to target mappings with transformation logic	DDI / O&M	As Needed	None
DAP-WP-PM-001	Current State Discovery	Document summarizing the existing data, capabilities, and infrastructure landscape and serves as a comprehensive reference capturing the current environment prior to the design and implementation of the new platform. It must include: • An inventory of existing data sources, systems, integrations, and data flows.	DDI	Once	None

Work Product ID	Title	Description	Phase / Stage	Frequency / Updates	Template
		• Documentation of current data models, storage structures, and reporting tools. • A summary of data governance, quality, and security practices currently in place. • Identification of dependencies, key stakeholders, and system ownership. • Current-state architecture diagrams illustrating major components and interfaces. • Known gaps, limitations, and improvement opportunities relevant to the future-state solution. The Current State Discovery Document must be delivered in a structured, reviewable format (e.g., Word with supporting diagrams). The document will serve as a baseline reference for future-state design, migration planning, and validation.			
DAP-WP-MIGR-001	Functional Equivalence Mapping	Document showing how legacy features map to new Solution features.	DDI	Once	None
DAP-WP-STAF-001	Key Personnel Resume	Resume for proposed key personnel replacement that demonstrates the minimum qualifications for the role are met. Replacements are subject to Department approval prior to any assignment.	DDI / O&M	As Needed	None
DAP-WP-DPR-001	Data Product Design Template	Template that enables data product teams to develop documents which provides details of the design of a Data Product which will serve as the basis for the data product teams to do the development work, the Data Product Owner to confirm acceptance of the design and for the Data Governance team to properly catalogue the Data Product with its metadata.	DDI	Once	None
DAP-WP-CONS-001	Self-Service Capabilities Documentation	Documentation describing the self-service capabilities pertaining to data products for enabling end users—such as data analysts, business users, and data stewards covering the following topics: • Overview of available data products: What they are, what problems they solve. • Schema and metadata: Field definitions, data types, update frequency. • Access instructions: How to connect, query, or subscribe to data. • Governance and usage policies: Data sensitivity, compliance, and sharing rules. • Examples and use cases: Sample queries, dashboards, or workflows.	DDI	As Needed	None

Table W-1 Work Products

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

As provided in *Section 1.3.3 Proposed Modifications to Terms and Conditions*, 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 X.

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	**Redline of Proposed Modification**
	(i.e., section & page number)	(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 Y 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 Minimum Requirement 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* 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 is 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.

☐ **Offeror Confirms** ☐ **Offeror Does Not Confirm**

4. **Experience Requirements**

The Offeror has a minimum of five (5) years combined experience providing services and solutions 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 specified in this section must have occurred within the five (5) years immediately preceding the date the RFP is issued by the Department as outlined in the following table. Where Offeror indicates areas of experience that are for services *similar* to those described in this RFP, Offeror must reference the specific RFP requirements and RFP section(s) relating to the similar services and describe, in detail, how the services are similar to be considered. It is the responsibility of the Offeror to clearly demonstrate in detail how services are similar and should be considered in the column titled *Description of Services Provided* below.

Name and Type Entity	Description of Services Provided	Size of population served by program(s)	Period of Experience (Start Date and End Date)

By completing and signing this *Attachment Y: Minimum Qualifications*, the Offeror affirms adherence to the required Minimums 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 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 this 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: REPORTS

1.0 REPORTS

Table AA-1 Reports List provides a list of the reports to be provided by the Vendor. The information for each report includes:

- Report ID: Unique identifier of the report.
- Title: Name of the report.
- Description: A summary of the elements to be included in the report.
- Frequency: Indicates how often the report is expected to be provided to the State.
- Template: Indicates if a preferred template is available to use to develop the report. The meaning of the values is as follows:
    1. None – No preferred template exists. The Vendor is free to provide the report in its own format and content.
    2. State Provided – A preferred template is provided by the State and can be found in the Bidder's Library which is included as part of the Ariba Sourcing Event in the NC eProcurement system. The name of the State provided template in the Bidder's Library contains the Report ID.

Reports submitted by Vendor should follow industry standards, best practices, and include data elements provided in the report description. *NOTE: Administrative Reports are NOT separately priced. The efforts and time required to develop and provide reports in the frequency shown must be factored into the overall cost and timeframe of project implementation and operations.*

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

a. Provide accurate and comprehensive content.
b. Follow industry standards and best practices.
c. Appropriately define and reference information.

The reporting deadline by frequency follows:

a. Daily or Weekly Reports – by the end of the Business Day following the end of the reporting period.
b. Monthly Reports – by the third Business Day following the end of the reporting period.
c. Quarterly or Annual reports – by the fifth Business Day following the end of the reporting period.
d. Annual reports – by the fifth Business Day following the end of the reporting period.

Informal reviews and walkthroughs of draft and final reports are encouraged. The State will provide final approval of the content and layout of all reports listed in *Table AA-1 Reports List*.

Report ID	Title	Description	Frequency	Template
DAP-REP-01	Data Quality (DQ) Scoring Report/Dashboard	Report that contains a comprehensive view of data quality across technical data assets (e.g., schemas, files, tables, and database objects) and cover completeness, accuracy, consistency, and validity of the data, catering to different personas from executive to data engineers seeking in depth information, to be developed jointly with the State during DDI. The report must include visualizations such as donut/pie charts to represent the current DQ status across datasets, and time-series bar charts that display DQ run metrics aggregated by month. These visualizations must enable trend analysis and monitoring of data quality over time, particularly for data sources where variability is expected.	Monthly	None
DAP-REP-02	Monitoring Tool Availability report	Report for the monitoring tool availability attestation from the Vendor contains a validation of what percentage of the time the monitoring tool was available in the period.	Monthly	None
DAP-REP-03	Subcontractor Usage Report	Report that contains the usage of subcontractors and certifies that all subcontractors are in compliance with the employment practices mandated by federal and State statutes and regulations. The Subcontractor Usage Report must include the total subcontractor FTE's, total subcontractor hours and responsibilities assigned on the project.	Annually	None
DAP-REP-04	Data Pipelines Operations Daily Report	Report will contain: • List of successful ingestions of the interface files, including number sent from source system and actual number processed by DAP • List of failed ingestions of the interface files, including number sent from source system and actual number processed by DAP • List of successful API ingestions • List of failed API ingestions • List of successful jobs across all data layers • List of failed jobs across all data layers • Confirmation that failed jobs / interfaces re-ran successfully • Failures over consecutive attempts • Remediation efforts report for those that have multiple failures over the last day • Remediation efforts report for those that have failed multiple consecutive attempts	Daily	None
DAP-REP-05	Data Pipelines Operations Monthly Report	Report will contain: • List of successful ingestions of the interface files, including number sent from source system and actual number processed by DAP • List of failed ingestions of the interface files, including number sent from source system and actual number processed by DAP • List of successful API ingestions • List of failed API ingestions • List of successful jobs across all data layers • List of failed jobs across all data layers • Confirmation that failed jobs / interfaces re-ran successfully	Monthly	None

Report ID	Title	Description	Frequency	Template
		Failures over consecutive attempts		
DAP-REP-06	System Monitoring Report	The report will contain, in both graphic and tabular/text format, the cloud platform and data warehouse performance and include: • Performance trends • Responses • Query time metrics Recent or recurring performance issues	Monthly	None
DAP-REP-07	Capacity Planning Report	The report will contain: • Utilization trends for servers, storage, network, backup hardware, and security devices • Thresholds where capacity would be increased • The interval that each of these is measured • Trend of utilization over the previous six months	Monthly	None
DAP-REP-08	Cost & Usage Report	Report that contains spend analysis, consumption trends, and ongoing cost optimization recommendations.	Monthly	None
DAP-REP-09	Infrastructure Optimizations Report	Report that contains all infrastructure optimizations to meet performance requirements or as requested by the Department.	Annually	None
DAP-REP-10	User Access Control Report	Report will contain: • The list of users who have access, what components of DAP they have access to, and what level of access to the system they have • Ensure that only legitimate users have access to the system Privileged access that must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know basis.	Quarterly	None
DAP-REP-11	System Enhancement Pool report	Report contains details on tickets invoiced for consulting services and must include dollars used and dollars remaining for the Department's approval.	Monthly	None
DAP-REP-12	Training Evaluation Report	Report to be completed after each training session provided and contains the results, findings, interpretations, conclusions, and recommendations derived from the training evaluation. This report will include an analysis of the training and its intended outcome to ensure that the training was delivered effectively and efficiently to all users, including the Contractor staff, State staff, and external users. The Vendor will collect feedback from the users to assess whether the training achieved its intended outcome, and if the training materials and resources used aligned with or met the training objectives and needs of the users. Also, the Vendor will document any training gaps, lessons learned, and opportunities for improvement in the evaluation report	As Needed	None
MES-DEL-OM-003	Decommission Recommendations Report	Report that identifies any unneeded subscriptions, software, and licenses, The Vendor must present the report recommendations to the Department for review and ensure that any unneeded subscriptions, software, and licenses have been decommissioned upon approval from the Department.	Monthly	None

Report ID	Title	Description	Frequency	Template
MES-DEL-PM-008	SLA Assessment Report	Report detailing SLA assessments must include: • 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 • Log and Aging Report for all Resolution Efforts	Monthly	None
MES-REP-03	Vulnerability Management Report	A report that contains: • All servers and systems patched proactively/timely to mitigate the vulnerabilities. • Application components security scanning reports for identifying OWASP TOP 10 vulnerabilities • SAST, DAST, IAST, and RASP testing reports • Cloud Security Posture Management Reports	Monthly	None
MES-REP-05	Turnover Activities Report	Report will document that all Contractor 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.	Monthly	None
MES-REP-06	Failed Patching Attempts Report	Report must include: • Servers that failed during the week • Number of times each server failed • For those servers that fail two (2) or more consecutive attempts, the number of consecutive attempts • Remediation plan for each server that failed.	Monthly	None
MES-REP-08	Weekly Status Report	The vendor must submit a weekly status report during DDI and O&M that contains the information defined in the Department's template and guidance document.	Weekly	State Provided

Table AA-1 Reports List

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