STATE OF NORTH CAROLINA **Department of Health and Human Services** **Information and Technology Division**	**REQUEST FOR PROPOSAL NO. 30-22174**
	Offers will be opened: 06/02/2023
	Issue Date: 04/12/2023
Refer ALL inquiries regarding this RFP to: Kevin Barlage – Contract Specialist kevin.barlage@dhhs.nc.gov Medicaid.Procurement@dhhs.nc.gov	Commodity Number: 811620
	Description: Interoperability – Patient Access
	Purchasing Agency: DHHS, Division of Health Benefits
	Requisition No.: N/A

OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR:			
STREET ADDRESS:		P.O. BOX:	ZIP:
CITY, STATE & ZIP:		TELEPHONE NUMBER:	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING:		FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:	

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: 180 days.

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of Purchasing Agency shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR PURCHASING AGENCY USE ONLY

Offer accepted and Contract awarded this date , as indicated on attached certification,

by (Authorized representative of Purchasing Agency).

Table of Contents

1.0 ANTICIPATED PROCUREMENT SCHEDULE

The Agency Procurement Agent will make every effort to adhere to the following schedule:

Action	Responsibility	Date	Time (EST)
RFP Issued	Agency	04/12/23	
Written Questions Deadline	Potential Vendors	04/24/23	2:00 pm
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	05/09/23	
Proposals Due	Vendor(s)	06/02/23	2:00 pm
Evaluation Begins	Agency	06/05/23	
Estimated Contract Award	Agency	11/05/23	
Protest Deadline	Responding Vendors	15 days after award	

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

To improve health information access to patients, Providers and Payers, the Centers for Medicare & Medicaid Services (CMS), and the Office of the National Coordinator of Health IT (ONC), released the Interoperability and Patient Access Final Rule CMS-9115-F (1) (Rule). This created regulations including policies which require or encourage Payers to implement Application Programming Interfaces (APIs) to improve the electronic exchange of healthcare data – sharing information with patients or exchanging information between a Payer and Provider or between two Payers. APIs can connect to mobile apps on handheld devices or to a Provider Electronic Health Record (EHR) or practice management system to enable a more seamless method of exchanging information. The regulations also include policies that may reduce burdens of the prior authorization process by increasing automation and encouraging improvements in policies and procedures to streamline decision making and communications.

The Department of Health and Human Services (HHS) finalized technical as well as content and vocabulary standards in the Office of the National Coordinator for Health Information Technology's (ONC) 21st Century Cures Act Final Rule (45 CFR 170 and 171) ("Cures Act"), which CMS adopted to support these API policies. Other Health Level 7 (HL7) implementation guides (IGs) are available for Provider, Payer and prior authorization APIs, which are not yet mandatory. In addition, CMS continues to work with HL7 and other industry partners to ensure IGs and additional resources are freely available to Payers to use if they choose to use them.

Links to CMS Interoperability and Patient Access Final Rule and additional information on policies and technical resources:

CMS Interoperability and Patient Access Final Rule: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index#CMS-Interoperability-and-Patient-Access-Final-Rule

Cures Act:. https://www.healthit.gov/topic/oncs-cures-act-final-rule

The Purpose of this Request for Proposal (RFP) is the for the North Carolina Department of Health and Human Services, Division of Health Benefits (NCDHHS or "Department"), to solicit offers for the acquisition of a solution to ensure that NCDHHS, complies with CMS Interoperability and Patient Access Final Rule CMS-9115-F (1). Through this RFP, NCDHHS is seeking to establish a contract with a vendor that can provide a solution that meets the requirements of the CMS Interoperability Final Rule, as well as provide professional services for implementation.

Effective July 1, 2021, nearly 1.7 million Medicaid beneficiaries in North Carolina began receiving their Medicaid services through NC Medicaid Managed Care Prepaid Health Plans (PHPs). Approximately 1.1 million beneficiaries are not enrolled with a PHP and remain in NC Medicaid Direct (Fee-For-Service). These 1.1 million beneficiaries are the user group for the Patient Access API as described in the Rule.

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. 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."

2.2.1 EFFECTIVE DATE

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

2.3 CONTRACT TYPE

Definite Quantity Contract - This request is for a 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.

2.4 AGENCY BACKGROUND

The North Carolina Department of Health and Human Services (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 (Division of Health Benefits) is dedicated to providing access to physical and behavioral health care and services to improve the health and well-being of over 2.8 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) 3.0 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 Interoperability and Patient Access Project is being planned and executed within the Department's Medicaid Enterprise System (MES) Modernization Program. The purpose of this project is to comply with the federal regulations identified above for the NC Medicaid Direct (fee-for-service) population only, with the following goals:

- Provide data needed by Patients and Providers to make informed decisions about their healthcare in an easily accessed format available on devices such as hand-held or personal computers.
- Ensure compliance with the CMS Interoperability and Patient Access Final Rule (CMS-9115F) and the Office of the National Coordinator (ONC) for Health Information Technology 21st CURES Act (2).

- Improve beneficiaries' ability to view or transfer their health information between Provider agencies, by making it accessible via third-party apps through an API.
- Improve beneficiaries' ability to find care by providing a current Medicaid Provider Directory via an API.

Because the Agency is in the process of modernizing the legacy MMIS with a modular Medicaid Enterprise System spanning a multi-year transformation, the Vendor should design the Interoperability Solution in a way so that it can integrate, with minimal effort and time, with the new MES as part of the modernization effort. The Agency's anticipated goal is to implement the Interoperability Solution on or before July 1, 2024.

3.1.1 IMPLENTATION OF PATIENT ACCESS API

The Vendor will develop and implement the Patient Access API that meets the Patient API portion of the Rule including Claims, Clinical, and Pharmacy Data (Drug Formulary). The secure, standards-based API will allow patients, or their personal representatives, to easily access their claims and encounter information. This includes providing access to cost information, as well as a defined sub-set of their clinical information and formulary data through a third-party application of their choice. The solution must use the required standards, profiles, and protocol described on the CMS website to meet the Rule.

3.1.2 IMPLEMENTATION OF PROVIDER DIRECTORY API – OPTION

If exercised by the State, the Vendor will develop and implement the Provider Directory Fast Healthcare Interoperability Resources (FHIR) API that meets the Provider Directory API portion of the Rule that allows for a set of Provider information to be made publicly available through a public facing digital endpoint on the Payer's website. The solution must use the required standards, profiles, and protocol described on the CMS website to meet the Rule.

3.1.3 IMPLEMENTATION OF PAYER-TO-PAYER DATA EXCHANGE API

The Vendor will develop and implement the Payer-to-Payer Data Exchange API. The solution must use the proposed standards, profiles and protocols described on the CMS website to meet the Payer-to-Payer Data Exchange part of the Rule.

3.1.4 SYSTEM INTEGRATION PLATFORM INTEGRATION

The Department has acquired a System Integration Platform (SIP) that resides on Amazon Web Services (AWS), provides centralized data exchange capabilities, and provides a single hub for all integrations and interfaces for the Medicaid program. The SIP provides for a common infrastructure to communicate and integrate using a consistent standards-based approach. The Vendor will integrate the IO Solution with the SIP to access Claims, Clinical, Pharmacy, and related data from the various MES modules.

3.1.5 IDENTITY MANAGEMENT

The Vendor solution must integrate with the State provided Identity Management solution, which is a multifactor authentication solution, based on the OpenID Connect (OIDC) standard for access credentialling and authorization.

3.1.6 CONSENT MANAGEMENT SOLUTION

The Vendor must implement a consent management solution to obtain consent from the beneficiaries or their personal representatives before gaining access to their health information.

3.1.7 EXTRACTION, TRANSLATION, AND LOAD SERVICES

The Extraction, Translation and Load process will use comma-separated values (CSV) and fixed length file extracts provided by the MMIS to generate FHIR formatted data. This FHIR formatted data will then be used to load (and keep current) data served in the APIs required in the Rule.

3.1.8 MIGRATION ACTIVITIES

According to the Rule, the Interoperability Solution should store five (5) years of patient data so that beneficiaries and Payers can access it when needed. The data from the current Medicaid system must be transferred into the Interoperability Solution via the State's System Integration Platform (SIP). NC Medicaid wants its current Medicaid data, including Provider and claim information, to be converted to a FHIR standard. The Vendor must create FHIR JavaScript Object Notation (JSON) documents that conform to the Rule's specifications.

The State is looking for a solution that will move and transform data from the legacy Medicaid system to the Interoperability system with data transfers that can take place with one or more of the formats listed below.

- FHIR JSON / FHIR Newline Delimited (ND-JSON)
- Fixed-length extract data and templates
- Electronic Data Interchange (EDI)/X12
- HL7v2
- Text
- CSV
- JSON
- Extensible Markup Language (XML)
- Hypertext Markup Language (HTML), including index files
- Proprietary files

3.1.9 ONGOING OPERATIONS AND MAINTENANCE

The Vendor must assist the State with day-to-day operations and maintenance of the Interoperability Solution. Any defects discovered during daily operations must be triaged according to the defect management processes, and code must be updated, tested, and approved by the Business representative before being deployed into production according to the release management process.

The vendor must adhere to all SLAs and KPIs set forth in this document.

3.2 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.2.1 REQUIREMENTS

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

3.2.2 SPECIFICATIONS

A specification documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, will mean that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or

Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.2.3 SITE AND SYSTEM PREPARATION

Vendors shall provide the Purchasing State Agency 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 *Interoperability and Patient Access Solution* 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.

3.4 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 DEFINED

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/architectural-artifacts.

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 the future state.

3.4.3 VIRTUALIZATION: RESERVIED

3.4.4 IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT (ICAM)

The State is implementing a centralized identity, credential, and access management (ICAM) solution as part of the Medicaid Enterprise System Integration Platform (SIP).

a. The proposed solution must externalize identity management and must integrate with the MES ICAM solution. The MES ICAM solution utilizes the North Carolina Identity Service (NCID) for the identity management and authentication related functions performed by this application. NCID is the State's enterprise Identity management (IDM) service. It is operated by the North Carolina Department of Information Technology (DIT). Additional information regarding this service can be found in the DIT Service Catalog at: http://it.nc.gov/it-services (see Identity Management - NC Identity Management under the main menu item Application Services) and the NCID website here: https://it.nc.gov/ncid/.

b. Changes or upgrades made to the NCID service constitute a change to all applications or services that utilize NCID. As with any change to an application or service, an NCID change will require appropriate testing and may require system changes to accommodate the NCID change.

3.4.5 CLOUD SERVICE PROVIDERS

a. The Vendor shall describe how the proposed solution will support the agency's information system security compliance requirements as described in the Statewide Information Security Manual, specifically relating to, and without limitation, the sections relating to cloud services: http://it.nc.gov/statewide-resources/policies.

b. The Vendor will be required to receive and securely manage HIPAA, PHI, PII and other confidential data.

c. To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using the latest 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.

d. The Vendor will be required to provide assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, ISO 27001, and HITRUST. For offered solutions that already meet these requirements, the Vendor shall include these reports as part of their submission.

3.5 BUSINESS AND TECHNICAL REQUIREMENTS

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

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

3.5.1 REQUIREMENTS

Table 1. Interoperability

Requirement #	Requirement Description
BUS-00006	The Vendor solution generated FHIR resources must support consistent IDs.

Requirement #	Requirement Description
BUS-00007	The Vendor solution must support the FHIR resource data structure validation for ingestion.
BUS-00008	The Vendor solution must support the FHIR resource and coding terminology enrichments and mapping for aggregated data generation as well as ingestion.
BUS-00009	The Vendor solution must support automatic FHIR version histories that are stored and can be queried.
BUS-00010	The Vendor solution must support FHIR resource provenance tracking.
BUS-00011	The Vendor solution must support the ingestion of data through integrations with legacy formats including HL7, CCDA, CSV, HIPAA X12 EDI and as agreed upon by the State.
BUS-00012	The Vendor must provide an Application vetting process capability (that comprises four sub-processes: app intake, app testing, app approval/rejection, and results submission processes) and security reviews to onboard all the third-party applications that are used by the beneficiaries to access their health record.
BUS-00013	The Vendor solution implementing the APIs must use publicly available CMS approved implementation guides as recommended by CMS-9115-F.
BUS-00014	The Vendor solution must use a FHIR 4 server.
BUS-00015	The Vendor solution must consist of a “sandbox” separate from the production server and test server to allow developer testing and development outside the production and test environments. The sandbox must mimic the production environment and must have a mechanism for registration / onboarding before given access to test their apps with the Vendor solution.
BUS-00016	The Vendor must work with the State to determine which users will have access to confidential, PHI, or PII data.
BUS-00017	The Vendor solution must provide a developer Portal to: obtain API related information such as keys, to manage applications, and to manage the development sandbox.
BUS-00018	The Vendor solution must support bi-directional data exchange, to get data from app developers, or external parties into the Interoperability Solution.
BUS-00019	The Vendor solution must support large binary resources, in excess of 100Mb, to accommodate a Member’s complete healthcare record.
BUS-00020	The Vendor solution must support a proxy or delegate to authorize access to a dependent’s data.
BUS-00021	The Vendor solution must support scale to support over 1,000,000 Members.

Table 2. Patient Access API

Requirement #	Requirement Description
BUS-00001	The Vendor solution must provide a Patient Access API necessary to meet or exceed the required and recommended standards, profiles, and protocols as set forth in the CMS Interoperability and Patient Access Rule (CMS-9115-F). See https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index for more information.
BUS-00002	The Vendor solution must ensure that a minimum of five (5) years of clinical and claims data are available on demand through FHIR compliant APIs.

Table 3. Payer-to-Payer API

Requirement #	Requirement Description
BUS-00034	The Vendor Solution must provide for Payers to maintain a process to coordinate care between Payers by exchanging the US Core Data for Interoperability (USCDI), at the enrollee’s request. When a Payer receives this information, they are to incorporate into the recipient Payer’s data system.

Requirement #	Requirement Description
BUS-00035	The Vendor solution must be able to receive the USCDI data set from another Payer that had covered the enrollee within the previous five (5) years.
BUS-00036	The Vendor solution must be able to send the USCDI data set at any time during an enrollee’s enrollment and up to five (5) years later to another Payer that currently covers the enrollee.
BUS-00037	The Vendor solution must be able to send the USCDI data set at any time during enrollment or up to five (5) years after enrollment has ended to a Payer identified by the enrollee.
BUS-00038	The Vendor solution must share, at enrollment for Payers with specific annual open enrollment, or during the first calendar quarter of each year for those Payers that do not have a specific annual enrollment, USCDI clinical, claims, and encounter data (not including cost data), as well as pending and active prior authorization decisions.

Table 4. Consent Management

Requirement #	Requirement Description
BUS-00044	The Vendor Solution must provide the functionality to require the member's consent before sharing their data with Payers, Providers, or other representatives.
BUS-00045	The Vendor solution must provide the ability for members to revoke access to third-party applications.
BUS-00046	The Vendor solution must support white-labeled (health plan branded) member consent applications.
BUS-00047	The Vendor solution must store and manage Consent Information.
BUS-00048	The Vendor solution must collect the consent information from the members for every application that the individual is choosing to access healthcare data.
BUS-00049	The Vendor solution must collect the Member's consent when the Member decides to disenroll from the Vendor solution.

Table 5. Identity Management

Requirement #	Requirement Description
SEC-00038	The Vendor solution must integrate with the State provided Identity Management solution, which is a multifactor authentication solution, based on the OpenID Connect (OIDC) standard for access credentialling and authorization.
SEC-00039	The Vendor solution must integrate with the centralized ICAM service for the purposes of authentication and authorization of State users and administrators.

Table 6. Interface

Requirement #	Requirement Description
ARCH-00001	The Vendor must provide the capability to accept, process, and store the Claims, Provider, Prior Authorization and Member information received in an Industry standard format through the State's system integrator as per the schedules agreed by the State.
ARCH-00002	The Vendor must provide the capability to accept, process, and store the Encounter information received in an Industry standard format through the State's system integrator as per the schedules agreed by the State.
ARCH-00003	The Vendor must provide the capability to accept, process and store the Claims, Medication, Drug formulary, Tier & Co-pay data information received in an Industry standard format through the State's system integrator as per the schedules agreed by the State.

Requirement #	Requirement Description
ARCH-00004	The Vendor must provide the capability to accept, process, and store the clinical, ADT, Registries, laboratory and medication information received in an Industry standard format through the State's system integrator as per the schedules agreed by the State.
ARCH-00005	The Vendor solution must support the conversion of standard transactions into FHIR equivalent based transactions in accordance with the latest version of HL7.
ARCH-00006	The Vendor solution must support ingesting CCDA documents into the FHIR data server and share the documents as FHIR transactions with the authorized users.
ARCH-00007	The Vendor solution must support the conversion of proprietary flat file format transactions into FHIR equivalent based transactions in accordance with the latest version of HL7.
ARCH-00008	The Vendor solution must utilize the Department's System Integration Platform (SIP) to integrate with cloud hosted and on-prem data sources.

Table 7. Operations and Maintenance

Requirement #	Requirement Description
OPS-00001	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.
OPS-00002	The Vendor must be responsible for resolving all service defects and service disruptions at no additional cost to the State. Defects are not considered resolved until approved by the Department.
OPS-00003	The Vendor must follow agreed-upon Release Management processes to submit and schedule all releases.
OPS-00004	The Vendor must make Technical Support personnel available with system expertise via a toll-free number during normal State business hours.
OPS-00005	The Vendor must obtain approval by the Department prior to scheduling non-emergency system downtime/maintenance.
OPS-00006	The Vendor must perform all reporting, vulnerability scans, privileged user access reports and all other reporting that is described within the State security policies (includes all monthly, quarterly, annual reports, etc.). References: https://it.nc.gov/documents/statewide-policies/statewide-information-security-manual/open https://it.nc.gov/resources/cybersecurity-risk-management/initiatives/information-security-policies
OPS-00007	The Vendor must provide a report for all Sev1 and Sev2 incidents on a monthly basis for the previous month and must provide a Root Cause Analysis for each of the Sev1 and Sev2 incidents.
OPS-00008	The Vendor must provide an Impact Analysis of any problems that are escalated to the Vendor and must provide resulting information to the Department.
OPS-00009	The Vendor must provide system maintenance which will include, at a minimum: service changes, system upgrades, correction of deficiencies, performance enhancements, script changes, system parameters, configuration changes, patching, and other activities required to meet the solution requirements.
OPS-00010	The Vendor must utilize the IT Service Management tool that is designated by the Department to track all Incidents, Problems and Changes (including Service Requests).
OPS-00011	The Vendor must work with the Department system integrator (SI) contractor to track defects and align Severity Levels and other categorizations with the Department definitions.
OPS-00012	The Vendor will be solely responsible for obtaining and maintaining all permits, approvals, licenses, certifications, and similar authorizations required by any local, State, or Federal entities for the project and maintaining them throughout the duration of the Contract.

Table 8. Security and Risk Management

Requirement #	Requirement Description
SEC-00004	The Vendor must conduct annual independent third-party penetration testing and submit the test results and reports to the Department.
SEC-00005	The Vendor must provide the Department with an annual report, conducted by an external auditor that is accredited by the Association of International Certified Public Accountants (AICPA), on effectiveness of internal controls that is compliant with the current AICPA standard, Reporting on Controls at a Service Organization (SOC 2 – Type 2) includes all five trusted service criteria (i.e., security, availability, confidentiality, process integrity and privacy..
SEC-00006	The Vendor must provide Corrective Action Plans (CAPs) to remediate any deficiencies found in any audit or assessment findings from the Security Assessment Report such as the SOC 2 – Type 2 audit, HITRUST CSF assessments within 30 days of receiving the report, and must remediate the findings as per the guidelines described in the State Security Policies, and must adapt to evolving controls as standards change.
SEC-00007	The Vendor must provide weekly status updates for each CAP until the CAP is complete and the finding is remediated in accordance with the State IT Security Policies.
SEC-00008	The Vendor and its subcontractors 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 DHHS Internal Audit, or any other authorized auditors as determined by Department.
SEC-00009	The Vendor must incorporate SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing) in their SDLC and share the security testing results with the Department before implementing any major changes to the system into the production.
SEC-00010	The Vendor must implement the risk management framework in compliance with the NIST Risk Management Framework or equivalent.
SEC-00011	The Vendor must perform internal risk assessment annually and share the assessment findings and corresponding POA&M / CAPs with the Department.
SEC-00012	The Vendor must incorporate other security testing IAST (Interactive application security testing) and RASP (Runtime Application Self Protection) techniques to improve the security posture of the application.
SEC-00013	The Vendor must implement the Web Application Firewall (WAF) to mitigate the application security vulnerabilities such as OWASP TOP 10.
SEC-00014	The Vendor must implement encryption for data in transit and data at rest using FIPS 140-2 or FIPS 140-3 compliant crypto material.
SEC-00015	The Vendor must run weekly vulnerability scans on all Vendor and subcontractor networks and systems that will access State data and information.
SEC-00016	The Vendor must provide all vulnerability reports to the Department along with weekly and quarterly reports to track critical and high vulnerabilities.
SEC-00017	The Vendor must review privileged access accounts with the Department and provide the summary report on a quarterly basis.
SEC-00018	The Vendor must provide the list of users and their access to the system in a report that Department authorized users can access when needed.
SEC-00020	The Vendor must provide at least two Department individuals with administrative accounts to provide continuity of operations.
SEC-00021	The Vendor must implement the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks.
SEC-00022	The Vendor solution must support element-level access permissions.

Table 9. Disaster Recovery Plan

Requirement #	Requirement Description
SEC-00024	The Vendor must conduct Business Impact Analysis (BIA) to identify hierarchy of critical services and infrastructure to determine the order that services will be restored for developing the detailed Business Continuity and Contingency Plan (BCP) and Disaster Recovery Plan (DRP) in accordance with guidance provided by NIST 800-34 revision 1.
SEC-00025	The DRP must include detailed procedures to address the following potential events: natural disasters (e.g., earthquake, fire, flood, storms), terrorist acts, power disruptions, or power failure, computer software or hardware failures, computer shutdown due to cyberattacks (e.g., hacking, malware, and ransomware).
SEC-00026	The DRP must adhere to Federal, State and Department laws, rules, regulations, and guidelines pertaining to business continuity / disaster recovery from agencies such as CMS, FEMA, NC DIT, and NCDHHS.
SEC-00027	The disaster recovery site must be geographically separated from the primary site by at least 100 miles and not reliant on the same power or network utilities.
SEC-00028	The Vendor must maintain or otherwise arrange for a disaster recovery site for its system operations in the event of a disaster that renders the production site inoperable.
SEC-00029	The Vendor must provide back-up processing capability at a DR site such that normal processing can continue in the event of a disaster or major hardware problem at the primary site. All operations at the remote back-up (DR) site must meet established contractual performance and SLA requirements.
SEC-00030	If the production site becomes unavailable due to a disaster, the Vendor must move operations to the disaster recovery site and remain operational at the disaster recovery site until the Department approves a return to normal operations.
SEC-00031	The disaster recovery environment must fully support production-level availability, capacity, and capabilities while maintaining adherence to all contract SLAs.
SEC-00032	The Vendor must determine when the primary production site is inoperable due to a disaster and execute the Disaster Recovery Plan.
SEC-00033	The Vendor must conduct annual disaster recovery testing to validate the DRP meets the DR SLA requirements. The Vendor will include recovery of any new functionality or integrations implemented during the previous year.
SEC-00034	The vendor must submit an After Action Report that includes the DR testing results and issues experienced during DR testing.
SEC-00035	As part of Go-Live/ORR, 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 DRP and in support of all SLAs.
SEC-00036	The Vendor must perform DR 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.
SEC-00037	The Vendor must coordinate disaster recovery activities with the Department, MES contractors, application business owner, system owner and division BCP Coordinator.

Table 10. Audit

Requirement #	Requirement Description
AUDIT- 00001	The Vendor must produce and maintain for ten (10) years, (3 years in excess of the contract including option 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.

Requirement #	Requirement Description
AUDIT- 00002	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.
AUDIT- 00003	The Vendor must retain all records 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, however, records must be maintained for a period of ten (10) years (3 years in excess of the contract including option years) following resolution of such action or longer if such action is still ongoing.

Table 11. Testing

Requirement #	Requirement Description
TEST-00001	All defects identified during testing must follow the State/Vendor agreed-upon established defect management processes.
TEST-00002	All test environments must have the scale to support both the number of test participants and test storage/processing requirements.
TEST-00003	The Vendor must collaborate with the State and non-State organizations and individuals, as necessary, to align testing processes and activities.
TEST-00004	The Vendor must document test results and obtain Department approval prior to implementing any changes in the production environment.
TEST-00005	The Vendor must ensure that UAT is conducted on a fully tested and operations-ready module component, including all software features.
TEST-00006	The Vendor must include a Testing Traceability Matrix to ensure that all requirements are tested and there are no testing gaps.
TEST-00007	The Vendor must have the capability to mask, sanitize, scramble, or desensitize sensitive data (e.g., PII/PHI) when extracting data from the production environment for use in non-production environments.
TEST-00008	The Vendor must implement version control in all environments.
TEST-00009	The Vendor must make recommendations concerning test execution activities based on the results of testing.
TEST-00010	The Vendor must make recommendations that support testing best practices before and during testing.
TEST-00011	The Vendor must obtain Departmental approval of test results before testing is considered complete.
TEST-00012	The Vendor must perform Operational Readiness Testing that includes a test of actual data processing in a fully operational environment. End-to-end MMIS functionality must be fully tested, including other identified system components.
TEST-00013	The Vendor must perform regression testing for changes to the application, including defects and enhancements.
TEST-00014	The Vendor must plan and manage all required testing phases such as unit, integration, user acceptance, and end-to-end Testing for their solution.
TEST-00015	The Vendor must propose solutions for all issues, problems, and defects for the Vendor’s solution identified through ORR.
TEST-00016	The Vendor must submit their test cases, during State testing, to the State to ensure that State users are testing the same sets of logic.
TEST-00017	The Vendor must provide authorized users access to necessary testing environments from offices and remotely as required for testing during DDI and throughout the life of the Contract.

Requirement #	Requirement Description
TEST-00018	The Vendor must provide training for all testing participants that includes: the system, processes, procedures, and tools used to execute testing.
TEST-00019	The Vendor must schedule and coordinate all testing activities with the system integrator (SI) to ensure that each test is prepared and performed in accordance with the Test Plan.
TEST-00020	The Vendor must support the State in end-to-end and UAT testing activities by providing support staff and technical expertise.
TEST-00021	The Vendor must work with the Department to assist the State in developing test cases that will be used for UAT.
TEST-00022	The Vendor must work with the dependent stakeholders to plan and manage the test schedule including any required coordination across the Department and Department contractors.
TEST-00023	The Vendor must write test plans, test design specifications, test cases, and test procedures for development, functional, and integration testing, in collaboration with the Department SMEs.
TEST-00024	The Vendor must provide the Department access to all test management software and test data including defect tracking, test execution status, test results and test traceability.
TEST-00025	The Vendor’s solution must provide the ability (preferably by the tester) to easily manipulate the system date for temporal testing.
TEST-00026	The Vendor must work with the Department or delegate to identify the timing and content of the testing reports.
TEST-00027	The Vendor must ensure that all test environments for the module, are fully available during scheduled testing.

Table 12. Training

Requirement #	Requirement Description
TRAIN-00001	The Vendor must conduct all training in accordance with the approved solution Training Plan.
TRAIN-00002	The Vendor must coordinate training activities with the MES PMO, the Department, and Department’s contractors.
TRAIN-00003	The Vendor must analyze, define, and tailor training to each specific user role and group.
TRAIN-00004	The vendor must ensure that the end users receive the knowledge and skills 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.
TRAIN-00005	The Vendor must create and maintain all training materials in such a way as to account for any system modifications that are made throughout operations and maintenance.
TRAIN-00006	The Vendor must provide training that describes the features, functions, limitations, standards and governance processes, tools, and other relevant items.
TRAIN-00007	The Vendor must provide a development environment to design training and for training of each user, role, and group.

Table 13. Project Management

Requirement #	Requirement Description
PROJ-00001	The Vendor must participate in an ORR prior to solution implementation. The ORR involves validating all of the operations and hardware, software, and the connectivity aspects of the solution. This review must involve comparing all operational components of the replacement system against the ORR checklists.

Requirement #	Requirement Description
PROJ-00002	The Vendor must participate in the development and execution of ORR Corrective Action Plans (CAPs) within defined timeframes.
PROJ-00003	All Deliverables must be approved by the Department following in accordance with its formal deliverable review process provided by the Department.
PROJ-00004	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.
PROJ-00005	The Vendor must follow the Department processes for the escalation of risks, issues and decisions for both project and operational needs. This includes the adherence to applicable change management, configuration management, incident, and release management disciplines.
PROJ-00006	The Vendor must manage requirements to ensure traceability throughout the project lifecycle (including development, testing, O&M phase, and bug fixes) and support for certifications and audits.
PROJ-00007	The Vendor must participate in Agency integration and program/project management meetings.
PROJ-00008	The Vendor must provide its deliverable tracking method to ensure all Deliverables have been accounted for according to the scheduled due date and coordinated with the MES PMO.
PROJ-00009	The Vendor must review and align their processes with the MES PMO Program Management Plan (PgMP) and select subplans provided by the State.
PROJ-00010	The Vendor must support key project/program milestones: UAT Sign-Off, ORR, and Go-Live.
PROJ-00011	The Vendor must provide a Deliverable Expectation Document (DED) for all Deliverables, using the Department's standard format that provides a brief explanation of tasks, activities, and methods to be used to develop the deliverable.

Table 14. Conditions for Enhanced Funding

Requirement #	Requirement Description
BUS-00054	The Vendor solution must follow regulations 42 CFR 341 Subpart F to safeguard information about applicants and beneficiaries. The following is the set of information that must be safeguarded: a) Names and addresses; b) Medical services provided; c) Social and economic conditions or circumstances; d) Agency evaluation of personal information; e) Medical data, including diagnosis and past history of disease or disability; and f) Any information received for verifying income eligibility and amount of medical assistance payments. Income information received from SSA or the Internal Revenue Service must be safeguarded according to the Requirements of the agency that furnished the data; g) Any information received in connection with the identification of legally liable third-party resources; h) Social Security Numbers.
BUS-00055	The Vendor solution user interfaces must be in alignment with, and incorporation of, industry standards adopted by the Office of the National Coordinator for Health IT in accordance with 45 CFR part 170, subpart B: The HIPAA privacy, security and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act.
BUS-00056	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.

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 is intentional.

3.6.1 SPECIFICATIONS

Table 15. Interoperability

Specification #	Specification Description
BUS-00022	Describe how your solution will provide and maintain a secure, standards-based (HL7 FHIR Release 4.0.1) environment.
BUS-00023	Describe how your solution will access the non-repudiation logs of third-party activity.
BUS-00024	Describe how your solution will facilitate the third-party attestation process that obtains information about a third-party application’s privacy policy.
BUS-00025	Describe how your solution will expose the FHIR compliant API documentation to the public.
BUS-00026	Describe how your solution will create reports/dashboard to report the API-related operational metrics.
BUS-00027	Describe how your solution will provide an internal State employee-facing administrators a dashboard or view of all APIs that are running and historical logs of user activity.
BUS-00028	Describe how your solutions defines data expectations in terms of FHIR JSON inputs or other non-FHIR compliant and JSON sources.
BUS-00029	Describe the number of concurrent API calls that your solution is capable of handling simultaneously given the number of beneficiaries in the user group defined in this RFP. Also include the average response time for the API call.
BUS-00030	Describe if your solution uses a single-tenant environment to eliminate any challenges such as data separation, release planning, scheduling and coordination with other MES modules. Include any documents to fully support the single-tenant environment or describe how these challenges will be mitigated within a multi-tenant configuration.
BUS-00031	Describe the approach your solution uses to make certain the data being ingested into the solution is quality checked to ensure it is valid and properly formed.
BUS-00032	Describe the method or methods your solution used to obtain data from different MES modules.
BUS-00057	Describe your design and development approach that would allow for minimizing the time frame to implement your solution. Include in your narrative an estimated project timeline with timing for each phase of the project. Provide any details on how the estimated timeline was derived such as knowledge of previous deployments of similar solutions.
BUS-00058	Describe how your solution architecture will store and exchange standard Interoperability data to meet the Final Rule. Provide any details how your architecture is extensible to include additional data sources such as Social Determinants of Health (SODH).

Table 16. Patient Access API

Specification #	Specification Description
BUS-00003	Describe how you will develop an API that allows patients to easily access their claims and encounter information, including cost, as well as a defined sub-set of their clinical information through third-party applications of their choice.
BUS-00004	Describe how your solution will exchange US Core Data for Interoperability (USCDI), at the patient’s request, allowing the patient to “take their data with them” as they change plans. This will include claims, clinical encounter data, and other EHI. Include in your response what USCDI data classes and elements are exchanged.

Specification #	Specification Description
BUS-00005	Describe your solution's approach for ingesting FHIR JSON data into the Patient Access API.

Table 17. Payer to Payer API

Specification #	Specification Description
BUS-00039	Describe how your solution will provide the ability to exchange data between the Payers. Please include how you share USCDI clinical, claims, encounter, pharmacy, registries, and lab results data. Also include how admission, discharge and transfer (ADT) data is exchanged.

Table 18. Consent Management

Specification #	Specification Description
BUS-00050	Describe how your solution will facilitate the registration and onboarding Medicaid members interested in accessing their data through FHIR compliant APIs.
BUS-00051	Describe how your solution will incorporate functionality to facilitate the Medicaid member consent of third-party SMART on FHIR applications.
BUS-00052	Describe how your solution will incorporate functionality for the member to view, track, and modify their consent.
BUS-00053	Describe how your solution will exchange the member consent information and associated documents with Payers, Providers and other representatives via 3rd party applications.

Table 19. Interface

Specification #	Specification Description
ARCH-00009	Describe any import/export and/or extraction translation and load tools included in your solution that may benefit the overall solution.

Table 20. Operations and Maintenance

Specification #	Specification Description
OPS-00013	This specification applies only if a SaaS solution is proposed. Describe how you would operate and maintain a SaaS solution in accordance with the Operations and Maintenance requirements and policies contained within this document. This specification will not be evaluated for non-SaaS solutions.

Table 21. Security and Risk Management

Specification #	Specification Description
SEC-00002	Describe your approach to conduct an annual privacy and security assessment based on the CMS published third-party privacy and security assessment framework. Include in your response if you will allow the Department or the Department authorized contractors access to your application infrastructure (network, systems, application, databased, etc.) to perform the privacy and security assessment or if you will provide a HITRUST CSF assessment certification from an independent third party.
SEC-00003	Describe your approach to conduct the third-party privacy and security assessment based on CMS third-party privacy and security assessment framework and Whitebox penetration testing for Operational Readiness Review (ORR) before 90 Days System Go-Live. Include in your response if you will allow the Department or the Department authorized contractors access to your application infrastructure (network, systems, application, databased, etc.) to perform the privacy and security assessment or if you will provide a HITRUST CSF assessment certification from an independent third party.

Specification #	Specification Description
SEC-00023	Describe how your proposed solution complies with applicable security standards identified by the State in this document (*Attachment C: Agency Terms and Conditions*), and describe how compliance can be achieved and verified during Design, Development, and Implementation (DDI) and Operations of the solution.

Table 22. Testing

Specification #	Specification Description
TEST-00028	Describe how you conduct testing using automation testing tools, level of test automation, interactive testing, and interactive debugging available in the test environment.
TEST-00029	Describe your approach to the design and documentation of a combination of positive and negative test case scenarios, including such items as identification, detailed steps, expected results, and actual results for each phase of testing.
TEST-00030	Describe your solution's approach to providing a functional demonstration to the department to show any changes or enhancements to the solution, prior to user acceptance testing.
TEST-00031	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.
TEST-00032	Describe how the Vendor solution will engage with other modules for full end-to-end testing.
TEST-00033	Describe the testing environments your solution will support such as: Unit Testing, System Testing, Integration Testing, Interface Testing, Performance Testing, Regression Testing, User Acceptance Testing, Operational Readiness Tests, and Operational Readiness Review.
TEST-00034	Describe the defect management process and how abnormal results that arise during the execution of identified test cycles (e.g., DDI, Operations, UAT) are resolved.
TEST-00035	Describe how your solution's test environment mirrors the production environment in its size, files, databases, processing, data protection, and reporting.
TEST-00036	Describe how your testing protocols avoid testing conflicts of interest between solution developers and the testing team such as a clear separation of duties from the development and implementation team versus the team performing testing.
TEST-00037	Describe how you ensure testing resources are comprised of qualified personnel with technical knowledge, skills and experience in testing and test management to ensure success.
TEST-00038	Describe how your solution provides performance tests, and reporting of a simulated load consistent with the actual load projected or used in production.

Table 23. Transition

Specification #	Specification Description
OPS-00014	Describe how your solution will provide NCDHHS the ability to export data from the Vendor solution for purposes of future migration to another vendor and continuity of operations.

Table 24. Diversity, Equity, and Inclusion

Specification #	Specification Description
DEI-00001	In alignment with NCDHHS values, describe your approach to ensure diversity, equity, and inclusion (DEI) in the workplace, with an emphasis on diverse hiring practices in management, leadership, and executive roles. Include any documentation and policies that show your commitment to supporting a DEI culture.
DEI-00002	Describe how you will incorporate cultural sensitivity, diversity, equity, and inclusion in your proposed training program.

Table 25. Training

Specification #	Specification Description
TRAIN-00008	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.

3.7 OPTION REQUIREMENTS AND SPECIFICATIONS

This RFP contains an option to purchase the Provider Directory API functionality (API Option) as part of the Interoperability Solution. The State may elect to exercise this API Option in the future at its sole discretion. The Vendor must include a response to the required information associated with the API Option as part of their proposal.

Table 26. Provider Directory API Requirements - OPTION

Requirement #	Requirement Description
BUS-00040	The Vendor solution must provide a Provider Directory API necessary to meet or exceed the Provider Directory Requirements set forth in the CMS Interoperability and Patient Access Rule (CMS-9115-F). See 42 CFR Parts 431, 435, 438, 440, and 457 and https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index and http://hl7.org/fhir/us/davinci-pdex-plan-net/STU1/.
BUS-00041	The Vendor solution must expose the Provider Directory API endpoint accessible via DHHS/MES public-facing website without any consent/authentication/authorization restrictions.

The Vendor must provide a response in their offer to all specifications in Table 27 as part of the technical proposal as defined in *Attachment T: Technical / Management Proposal.*

Table 27. Provider Directory API Specifications - OPTION

Specification #	Specification Description
BUS-00042	Describe how your solution will make a Provider directory publicly available, without API keys, via an HL7 FHIR standards-based API. Please include all search criteria that your solution makes available such as Provider name, NPI, taxonomy (specialty), location, accepting new Medicaid patients, and sex of practitioner.
BUS-00043	Describe the frequency of Provider data updates that are performed to ensure Provider data is reflected in the API.

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:

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

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

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

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

a. Costs must be provided for each year of the Contract term.

b. Operations and Maintenance Costs will begin after Solution Implementation is complete and approved by the Department.

c. Operations and Maintenance Costs will be billed monthly:

   i. Services and Support for the functionality of Items in *Attachment E: Cost Form* will be billed as one-twelfth (1/12th) of the annual cost for the item for the upcoming month.

   ii. Ongoing Maintenance deliverables will be billed by the Vendor upon delivery and approval by the Department.

   iii. Cloud Hosting will be billed as one-twelfth (1/12th) of the annual cost for the upcoming month.

d. Fully Burdened Hourly Labor Rates for all Key Personnel and other project staff must be provided.

e. Additional Costs – The Vendor may provide any additional costs that are specific to the implementation of their solution that are not outlined in the Cost Proposal Workbook referenced in *Attachment E: Cost Form* . Vendors may submit written questions in accordance with *Section 6.2.2 Questions Concerning The RFP*.

f. Assumptions – The Vendor must provide any assumptions made in their cost proposal.

Cost Option: The Provider Directory API is an option. The completed cost form must provide all costs including options in the respective tables within the selected cost form. The costs associated with this option will not be included in the total cost of ownership for evaluation and award purposes.

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

4.2 PAYMENT SCHEDULE

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

5.0 EVALUATION

5.1 SOURCE SELECTION

A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value to the State, recognizing that Best Value may result in 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 non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria.

b. To be eligible for consideration, Vendor's offer must conform to all requirements and must substantially conform to 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 evaluation committee may request clarifications or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, 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.

d. Vendors are advised that the State is not obligated to ask for, or accept data that is essential for a complete and thorough evaluation of the offer after the closing date for receipt of offer.

5.2 EVALUATION CRITERIA

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

a. Business and Technical Specifications of this RFP. Within the business and technical specifications listed in Section 3.6.1 the major categories listed by table are further listed in descending order of importance as provided in Attachment T. For example, the Interoperability category is more important than the Patient Access API category. The specifications listed within a major category, such as Interoperability, are all of equal importance;

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 in the formatted cost tables provided in this RFP.

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

5.2.1 EVALUATION OF OPTIONS

This solicitation contains option provisions. The State will not consider the response for the Provider Directory API Option in its evaluation for award purposes. The state is not obligated to exercise the Provider Directory API Option.

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. Vendors who attempt to gain this 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.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

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.

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

While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:

a. waive any formality;

b. amend the solicitation;

c. cancel or terminate this RFP;

d. reject any or all offers received in response to this RFP;

e. waive any undesirable, inconsequential, or inconsistent provisions of this RFP;

f. if the response to this solicitation demonstrates a lack of competition, negotiate directly with one or more Vendors;

g. not award, or if awarded, terminate any contract if the State determines adequate State funds are not available; or

h. if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply.

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 not an E-Procurement solicitation. Sub-Paragraph #38 of *Attachment B: Department of Information Technology Terms and Conditions* does not apply to this solicitation.

6.1.6 INTERACTIVE PURCHASING SYSTGEM (IPS)

The State has implemented links to the Interactive Purchasing System (IPS) that allow the public to retrieve offer award information electronically from our Internet website: https://www.ips.state.nc.us/ips/. Click on the IPS BIDS icon, click on Search for BID, enter the Agency prefix-offer number 30-22174, and then search. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

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

a. The Vendor shall deliver a written request for a protest meeting to the agency head or the agency head's designee within fifteen (15) calendar days from the date of contract award. The Vendor's request shall contain specific reasons and any supporting documentation regarding why there is a concern with the award. If the request does not contain this information or the agency head determines that a meeting would serve no purpose, then the agency head, within ten (10) calendar days from the date of receipt may respond in writing to the offeror and refuse the protest meeting request.

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. 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 contact person listed on Page One of this RFP may be grounds for rejection of said Vendor’s offer.

Written questions concerning this RFP must be received by the stated deadline. They must be sent via e-mail to **Medicaid.Procurement@dhhs.nc.gov** . Please enter “Questions RFP 30-22174” as the subject for the email. Questions should be submitted in the following format:

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

6.2.3 ADDENDUM TO RFP

If a pre-offer 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 Interactive Purchasing System (IPS), https://www.ips.state.nc.us/ips/, and shall become an Addendum to this RFP. Vendors’ questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer. 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 website for any and all Addenda that may be issued prior to the offer opening date.

6.2.4 COSTS RELATED TO OFFER SUBMISSION

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

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

6.2.5 VENDOR EXCEPTIONS - RESERVED

6.2.6 ALTERNATE OFFERS

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

Alternate offers must be submitted with the primary offer in accordance with the proposal submission instructions and clearly labelled "**RFP 30-22174, Alternate Offer, Name of Vendor**" and numbered sequentially with the first offer if separate offers are submitted. The legend "**Alternate Offer for 'Name of Vendor**' must be in bold type of not less than 14-point type on the face of the offer and on the text of the alternate offer.

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

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

6.2.9 NON-RESPONSIVE OFFERS

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

- "This offer does not constitute a binding offer",
- "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
- "The Vendor does not commit or bind itself to any terms and conditions by this submission",
- "This document and all associated documents are non-binding and shall be used for discussion purposes only",
- "This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties", or
- A statement of similar intent.

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Registration can be completed at the following website: https://www.sosnc.gov/Guides/launching_a_business .

6.2.11 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following website: https://www.ips.state.nc.us/ips/.

This RFP is available electronically on the Interactive Purchasing System at https://www.ips.state.nc.us/ips/.

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** along with detailed description of the Vendor's organization to include the following:
      - Date Established;
      - Ownership (public company, partnership, subsidiary, etc.);
      - If incorporated, state of incorporation must be included;
      - Background of the organization (not to exceed three (3) pages);
      - Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's organization has been in business, whichever is less.
2. **Completed and Signed** version of the **Execution Page**, along with the body of the RFP and signed receipt pages of any addenda released in conjunction with this RFP;
3. **Completed 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:** Cost form to be completed in accordance with **Section 4** and instructions found in Attachment E;.
6. **Completed** and **signed Attachment F**: Vendor Certification Form;
7. **Completed Attachment G:** Location of Workers Utilized by Vendors;
8. **Completed Attachment I:** Financial Review Form and copies of Financial Statements as further described in Section 7.2;
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:** 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. Current independent 3rd party assessment report in accordance with Section 3.3.2, paragraph b, subparagraphs i)-iii).

<u>ADHERENCE TO INSTRUCTIONS</u>: 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 by <u>electronic mail ONLY</u>. Paper 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. **<u>It is the responsibility of the Vendor to submit their proposal in accordance with these instructions by the specified time and date of opening. All electronic proposal submissions are subject to the conditions made a part hereof.</u>**

d. **Proposal and Cost Proposal Workbook must be e-mailed by the stated deadline directly to** Medicaid.Procurement@dhhs.nc.gov**.**

e. Vendor's Proposal and Cost Proposal Workbook may be contained in the same e-mail but must be separate files and clearly named (e.g. **RFP 30-22174, Vendor's Name, Proposal**) and (e.g. **RFP 30-22174, Vendor's Name, Cost Proposal**).

f. If your documents are submitted in multiple emails, that must be stated in the subject line, and the first and final e-mail should be clearly noted. For example: **Subject: RFP 30-22174, Vendor's Name, Proposal Email 1 of 3**; **Subject: RFP 30-22174, Vendor's Name, Proposal Email 3 of 3**.

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 return 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, e-mailed copy of Vendor's **redacted proposal** in accordance with Chapter 132 of the General Statutes, Public Records, identified as **RFP 30-22174, Vendor's Name, 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 30-22174, Vendor's Name, Statement of Confidential Information**.

j. This RFP is available electronically at the State of North Carolina Interactive Purchasing System (IPS), https://www.ips.state.nc.us/ips/.

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.

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

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

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

7.2 FINANCIAL STATEMENTS

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

a. For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

b. For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

c. The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

a. Pursuant to N.C.G.S. §143B-1350(h)(1), Agencies must conduct a risk assessment, including whether the Vendor has sufficient financial resources to satisfy the agreed upon limitation of liability prior to the award of a contract with Vendor.

b. Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.

c. Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

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

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

7.5 RESELLERS - RESERVED

7.6 DISCLOSURE OF LITIGATION

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

a. The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or Key Personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. The Vendor shall promptly notify the State of any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.

b. The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.

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

7.7 CRIMINAL CONVICTION

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

7.8 SECURITY AND BACKGROUND CHECKS

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

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

7.9 ASSURANCES

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

a. the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions, or

b. whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the

State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

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

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

7.11 PROJECT MANAGEMENT

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

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

7.12 MEETINGS

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

a. These meetings will include an agenda containing updates, including but not limited to status, implementation, schedule, testing, training, risks, issues, actions, decisions, defects, and change management functions.

b. The Vendor is required to lead and/or participate in stand-up meetings with the project team to address progress, risks, issues, and roadblocks to ensure the project deliverables and milestones are met as outlined in *Attachment N: Deliverables and Milestone Schedule.*

c. Failure to participate in weekly status and/or stand-up meetings, two (2) consecutive or rescheduled meetings, may result in termination of the Contract.

d. The Vendor is required to meet with State personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Contract. Meetings will occur as problems arise and will be coordinated by the State. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract.

7.13 RECYCLING AND SOURCE REDUCTION

It is the policy of this State to encourage and promote the purchase of products with recycled content to the extent economically practicable, and to purchase items which are reusable, refillable, repairable, more durable, and less toxic to the extent that the purchase or use is practicable and cost-effective. We also encourage and promote using minimal packaging and the use of recycled/recyclable products in the packaging of goods purchased. However, no sacrifice in quality of packaging will be acceptable. The Vendor remains responsible for providing packaging that will protect the commodity and contain it for its intended use. Vendors are strongly urged to bring to the attention of the purchasers at the NCDIT Statewide IT Procurement Office those products or packaging they offer which have recycled content and that are recyclable.

7.14 SPECIAL TERMS AND CONDITIONS

7.14.1 PERFORMANCE BOND – RESERVED

7.14.2 CHANGE MANAGEMENT PROCESS

Vendor must align its Project Change Management Plan with the Department, which describes the processes to be employed by the Division and Vendor to ensure that changes are captured, planned, and implemented in a visible, controlled, and orderly fashion. The State's Consolidated Change Management Plan (herein – the Change Management Plan) will be augmented by the Vendor as specified in this RFP.

a. The Change Management Plan will establish procedures for documenting and controlling changes to ensure all approved changes are:

   i. Necessary;

   ii. Documented correctly in the Project Change Request form, and includes a detailed description of the impact to the project describing its severity and criticality;

   iii. Tracked in a Change Management Log;

   iv. Evaluated to consider interfaces and IT environments;

   v. Evaluated against available resources;

   vi. Evaluated for cost reasonableness versus benefit, schedule, and performance trade-offs.

b. The Change Management Process will include procedures where the Parties interact to propose, refine and, if agreement is reached, sign off on the Change Request forms after approval by the Division's Steering Committees. The Summarized processes by which the Vendor shall comply consists of the following:

   i. Vendor must provide supporting information through the use of their change management processes to facilitate justifying the change meeting item a.i through a.vi outlined in the above section;

   ii. This information will be presented to the program steering committees through the use of two forms: The program "Intake Form" and the Project Change Request." Both are available upon request of the Change Manager. Vendors must allow fourteen (14) days for approval of each submission through the appropriate committee. Additional time will be required for external approvals which may take an additional sixty (60) calendar days. Details for which committee to submit the forms to are managed by the Division's assigned project manager;

   iii. Upon approval of the change and with agreement of the Centers for Medicare & Medicaid Services, the amendment, if required, is signed.

c. The State’s Change 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.

d. Vendor shall not be entitled to compensation for any Services unless the Change Management Process is followed and approved by the governance committees in which all changes will be evaluated.

e. Vendor shall propose the Change Management Process in their Change Management Plan. The Change Management Plan of the Vendor shall not become effective until it has been approved in writing by the State.

f. The Vendor’s plan must take into consideration the minimal steps and time frames aforementioned.

g. The Change Management Process shall apply to all proposed Changes to the Services provided by the Vendor.

h. The Change Management Process shall be documented in the Change Management Log and shall include the following:

   i. Change Requests that include changes to the scope, price, or time schedule of the Services, or to any dates in the Contract of significant consequence to performance of the Services, shall be made effective through the Parties’ execution of a Contract amendment;

   ii. Amendments resulting from the Change Management Process are binding and shall be signed by both the Vendor’s and the State’s respective representatives with appropriate level of signature authority;

   iii. Changes Requests that include but are not limited to changes to the scope, price, time schedule of the Services, dates or to the performance of Services, shall be made effective through the Parties’ execution of a Contract Amendment. Change Requests that do not include such changes (including, for example and without limitation, clarifications of existing requirements or specifications of no price or schedule impact) shall be made effective through the Parties' execution of such documentation as shall be required under the State’s Change Management Plan, except when the Parties may agree in a particular instance that it is appropriate to execute a formal Contract amendment;

   iv. The Change Management Process shall include procedures through which the Parties interact to propose, refine and, if agreement is reached, sign-off or execute documentation binding them to proposed changes;

   v. It is recognized that the State has a change management process that includes governance committees having varied responsibilities for approving changes in scope, time, cost, or services planned which will need to approve all changes initiated by the Vendor of the State for consideration.

i. 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, time frames, or costs shall be made at no additional cost to the State.

7.14.3 MITA 3.0 FRAMEWORK AND TECHNICAL ARCHITECTURE SEVEN STANDARDS AND CONDITIONS

The Medicaid Information Technology Architecture (MITA) 3.0 is an initiative of the Center for Medicaid & State Operations (CMSO). 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 is expected to describe their level of knowledge and understanding of the MITA 3.0 framework and to address how the Vendor will use their experience to leverage the MITA 3.0 framework to help transform the way the Agency conducts its business to operate in accordance with Level 3 or higher MITA capability levels. This also includes the information and technical architectures that support the solution, as well as an overall conformance to both the MITA 3.0 Framework and Seven Standards and Conditions.

7.14.4 PERFORMANCE MANAGEMENT

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

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

a. Service Level Agreements (SLAs)

b. Key Performance Indicators (KPIs)

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 – RESERVED

7.14.7 MODIFICATION POOL

Modification Pool is 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 RFP or in the Vendor's proposal, but is determined by the State as necessary to expand Interoperability functionality.

During the term of the Contract, the Vendor shall make two pools of optional additional labor available to the State to implement changes or add functionality to the Interoperability Solution in ways not specified in this RFP and the Vendor's Proposal. The State may resort to either pool to make such changes or additions to the Interoperability functionality at the State's discretion.

a. Modification Pool – Design, Development, Implement (DDI) Phase

During the DDI phase of the Contract, there shall be an Additional Functionality Pool to address changes to, and the addition of, requirements. Identification of changes to be processed via the DDI Phase Additional Functionality Pool shall be managed in accordance with Section 7.14.2, and the approved Change Management Plan. Offerors shall be required to propose guaranteed rates (onsite and offsite) in the Cost Workbook for labor categories typically used in development work in the Cost Section of their Proposals. This budget line item shall be equal to 10% of the annual contract value per year. During the DDI Phase, the Vendor shall make available up to the total dollar value of additional labor indicated for the DDI Phase Additional Functionality Pool. At the conclusion of each DDI year, the State may carry forward the unused balance of DDI Phase Additional Functionality Pool dollars to the following DDI year to increase the total dollar value of the DDI Phase Modification Pool.

b. Modification Pool - Operations & Maintenance (O&M) Phase

During the O&M phase of the Contract, the Vendor shall perform modifications to the Interoperability Solution, as requested by the State, such as new plan features and initiatives, legislative changes, as well as updating training and documentation associated with these modifications. There shall be pool hours at fixed labor rates (onsite and offsite) in the Cost Workbook of an O&M Phase Modification Pool. This budget line item shall be equal to 10% of the annual contract value per year. During the O&M Phase, the Vendor shall make available up to the total dollar value of additional labor indicated in the Modification Pool line item in the Cost Workbook for the O&M Phase Modification Pool. At the conclusion of each O&M year, the State may carry forward the unused balance of O&M Phase Modification Pool dollars to the following O&M year to increase the total dollar value of the O&M Phase Modification Pool.

Each change or new functionality to the Interoperability Solution using a Modification Pool allocation shall be governed by the Change Management Process, as set forth in Section 7.14.2 of this RFP. Accomplishing approval during a Change Order's Governance stage, means that each change must meet the State's Quality Assurance goals, 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 either pool, 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 Vendor 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 to a Modification Pool allocation.

If the Parties agree that work on an activity utilizing pool labor 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 pool labor 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 either pool, the contractual documentation that authorizes and specifies each pool activity will 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 of each pool is established as a budgeting and administrative convenience to the parties and shall not be construed as a limitation to the Vendor's obligation under Attachment B – "DIT Terms and Conditions - Unanticipated Tasks (paragraph 40)" of this RFP, not to unreasonably refuse amendments to the Contract that may involve additional costs.

7.14.8 ESCROW AGREEMENT

The following section applies only if a non-SaaS solution is being proposed. In addition, if a non-SaaS solution is being proposed, the Deliverable DEL-B-PROJ-004.01, Escrow Agreement as described in Attachment N, is not required.

By no later than ninety (90) days after the Effective Date of the Contract, the Vendor shall establish an Escrow Agreement with a third-party Escrow Agent that has offices within the State of North Carolina, which is acceptable to the Department, and lists the Department as the beneficiary of the Escrow Agreement.

1) The following events constitute release conditions (Release Conditions) of the Escrow Agreement:

   a. The Vendor is insolvent or the filing of involuntary or voluntary bankruptcy proceedings against or by the Vendor pursuant to Chapter 7 of the U.S. Bankruptcy Code, or

   b. The Vendor no longer offers support or maintenance services for the Software, or

   c. The Vendor breaches the Contract, or

   d. The Contract is terminated, or

   e. The Escrow Agent is insolvent.

   In the event that any of the Release Conditions is met, the Department shall notify the Escrow Agent and the Escrow Agreement shall require that the source code and object code for the Solution and any other software licensed to the State in connection with the Contract deposited in accordance with the Escrow Agreement (Deposit Materials) shall be delivered to the Department and the Department shall be granted a perpetual, royalty-free license to use the Deposit Materials solely to repair, maintain and support the software licensed to the Department.

2) The Escrow Agreement shall require that the Vendor do all of the following:

   a. Deposit into the escrow account, all proprietary software that will be used as the solution source code and object code or that will be licensed to the State in connection with the Contract;

   b. Every thirty (30) days, from Contract award until the beginning of the Operations and Maintenance Phase, deposit with the Escrow Agent the most up-to-date versions of the following and certify to the Agency Contract Administrator in writing that the deposit has been made:

i. All deliverable documents that are in process but not yet submitted to the Department for review and approval (in electronic, editable Microsoft formats);

ii. The source code and object code for the solution, and any other software licensed to the State in connection with the Contract;

iii. All technical product specifications documents;

iv. All updated solution test scripts (automated and not automated);

v. Any Vendor-developed software (source code and object code) and documentation used for source code management, builds, run-time management, and automated testing;

vi. Documented reference and release numbers for any third-party software used for the Vendor's development process, including but not limited to, source management tools and automated testing;

vii. Documented reference and release numbers and copies of license agreements held by the Vendor for any third-party software required for the proposed solution, including but not limited to, email software and word processing software.

c. Every one hundred eighty (180) days during the Operations and Maintenance Phase of the Contract until Contract termination, deposit with the Escrow Agent the most up-to-date versions of the following and certify to the Agency Contract Administrator in writing that the deposit has been made:

i. All deliverable documents that have been updated since last deposit (in electronic, editable Microsoft formats);

ii. The source code and Object code for the solution, and any other software licensed to the State in connection with the Contract;

iii. All technical product specifications, including maintenance and modification updates;

iv. All updated solution test scripts (automated and not automated);

v. Updated versions of any Vendor-developed software (source code and object code) and documentation used for source code management, builds, run-time management and automated testing;

vi. Updated documented reference and release numbers for any third-party software used for the Vendor's development process, including but not limited to, source management tools and automated testing;

vii. Updated documented reference and release numbers and copies of license agreements held by the Vendor for any third-party software required for the solution, including but not limited to, email software and word processing software.

3) Escrow Costs

a) The Vendor shall pay all costs related to the Escrow Agreement.

b) The Vendor shall require the Escrow Agent to validate all deposits at the Vendor's expense.

c) The State reserves the right to audit the Deposit Materials periodically. All charges for accessing and replacing these materials shall be paid by the Vendor.

d) The Vendor shall not submit any invoices to the Department for payment until the Escrow Agreement between the Vendor, the Department, and the Escrow Agent has been finalized and signed by all parties, and the source code has been deposited as required by this RFP and the Escrow Agreement.

e) No invoices from Vendor under the Contract created by this RFP will be processed for payment for any services or software until the Escrow Agreement is finalized and the Escrow Agent has certified to the Department that the required deposit materials have been received by the Escrow Agent.

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).

ATTACHMENT A: DEFINITIONS

1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.

2) **Agency:** The term "Agency" within this document refers to the North Carolina Department of Health and Human Services (NCDHHS). Synonymous with Department.

3) **AWS:** Amazon Web Services

4) **AICPA:** Association of International Certified Public Accountants

5) **API:** Application Programming Interface

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

7) **BIA**: Business Impact Analysis. Analysis to identify hierarchy of critical services and infrastructure to determine the order that services will be restored.

8) **Beneficiary**: Synonymous with Recipient or Member. Person enrolled in a participating Medicaid program.

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

10) **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 here: https://oshr.nc.gov/state-employee-resources/benefits/leave/holidays

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

12) **BSD:** Business System Design

13) **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.

14) **CAP:** Corrective Action Plan

15) **CCDA:** Consolidated Clinical Document Architecture

16) **CEF**: Conditions for Enhanced Funding

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

18) **Change Management Process**: Sequence of steps or activities that a change management team or and ensure the project meets its intended outcomes.

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

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

21) **Cloud-Based System**: A solution for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

22) **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.

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

24) **Communications Management Plan:** Policy-driven approach to providing stakeholders with information. The plan formally defines who should be given specific information, when that information should be delivered and what communication channels will be used to deliver the information.

25) **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.

26) **C-SCRM:** Cyber Supply Chain Risk Management

27) **CSV:** Comma-Separated Values

28) **Cybersecurity Incident (GS 143B-1320):** An occurrence that:

    a. Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

    b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

29) **DAST:** Dynamic Application Security Testing

30) **DEI:** Diversity, Equity, and Inclusion

31) **Deliverables**: : Any unique and verifiable product or other tangible material that must be delivered to the State to complete a process, phase, or project.

32) **Department**: The term "Department" within this document refers to the North Carolina Department of Health and Human Services (NCDHHS). Synonymous with Agency.

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

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

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

36) **DHB**: Division of Health Benefits. The division within the NCDHHS responsible for implementing Medicaid transformation and administering the transformed Medicaid and NC Health Choice programs as described in Session Law 2015-245, as amended.

37) **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 healthcare professionals, community leaders and advocacy groups; local, state, and federal entities; and many other stakeholders.

38) **DMH:** Division of Mental Health. This is a 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.

39) **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.

40) **DR:** Disaster Recovery

41) **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

42) **Document Management Plan:** Coordination and control of the flow (storage, retrieval, processing, printing, routing, and distribution) of electronic and paper documents in a secure and efficient manner, to ensure that they are accessible to authorized personnel as and when required.

43) **EHI:** Electronic Health Information

44) **EHR:** Electronic Health Record

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

46) **End User Documentation:** Documentation that contains information on individual user interface elements (such as grids, navigation panes, data editors, charts, etc.), and provides instructions for end-users about how to solve the most-common tasks with these interface elements.

47) **Enterprise Architecture Documentation:** Conceptual blueprint that defines the structure and operation of an organization.

48) **ECM:** Enterprise Content Management. A systematic approach to managing an organization's content throughout its lifecycle.

49) **EPS:** Encounter Processing System which collects and processes Medicaid Encounters for the Managed Care Organizations

50) **FEMA:** Federal Emergency Management Agency

51) **FFP:** Federal Financial Participation

52) **FFS**: Fee-For-Service. A system of payment where a physician or other Provider is paid a fee for each service rendered.

53) **FHIR**: Fast Healthcare Interoperability Resources. A standard that defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems.

54) **FIPS 140-2 or FIPS 140-3**: A specification, which defines a set of requirements for cryptographic processing.

55) **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).

56) **HIE**: Health Information Exchange

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

58) **HITRUST CSF**: Health Information Trust Alliance created to maintain the Common Security Framework.

59) **HL7**: Health Level Seven. A healthcare-specific standards organization focused on creating a defined set of international messaging standards used to support interoperability and communication between applications and devices.

60) **IAST:** Interactive Application Security Testing

61) **ICAM:** Identity, Credential and Access Management

62) **ICD:** Interface Control Document

63) **IG:** Implementation Guideline

64) **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.

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

66) **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.

67) **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.

68) **Interface Testing:** Interface testing is performed by the selected Vendor to ensure Providers, EDI service centers, business partners, and other Department Vendors can submit transactions over appropriate channels and can send and receive proper acknowledgements and negative responses, including the testing of timeframes between the receipt of a transaction and the notification/response to the submitter for all modes of transmission. This includes any interfaces relating to external systems.

69) **iServer:** A software platform, from Orbus Software, which the State uses to manage, govern, and visualize its Enterprise Architecture information and associated artifacts.

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

71) **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.

72) **Medicaid Program**: The joint federal-state health insurance program for low-income individuals and families who cannot afford healthcare costs. Medicaid serves low-income parents, children, seniors, and people with disabilities.

73) **Member**: Synonymous with Recipient or Beneficiary. Person enrolled in a participating Medicaid program.

74) **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.

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

76) **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.

77) **MITA**: The Medicaid Information Technology Architecture (MITA) initiative sponsored by CMS is intended to foster integrated business and IT transformation across the Medicaid enterprise to improve the administration of the Medicaid program.

78) **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.

79) **Monthly Status Report:** Please see Weekly Status Report definition. Monthly Status Report is a high-level summary produced at the end of every month as described in the Communications Plan.

80) **MTQAP**: Master Test Quality Assurance Plan

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

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

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

84) **NCAnalytics:** The current North Carolina Medicaid data warehouse and data analytics system

85) **NCTracks:** The current North Carolina MMIS System

86) **NIST:** National Institute of Standards and Technology

87) **NPI**: National Provider Identifier. Standard unique health identifier for Providers adopted by the Secretary .

88) **OCMP:** Operational Change Management Plan

89) **OIDC:** OpenID Connect. An open authentication identity layer that works on top of the OAuth 2.0 framework.

90) **O&M:** Operations and Maintenance phase of the project.

91) **OMP:** Operations Management Plan

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

93) **ORR:** Operational Readiness Review

94) **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.

95) **OWASP TOP 10**: Open Web Application Security Project. A standards awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

96) **Payer**: Organizations — such as health plan Providers, Medicare, and Medicaid — that set service rates, collect payments, process claims, and pay Provider claims

97) **PCMP** – Project Change Management Plan

98) **PHI:** Protected Health Information, as that term is defined in HIPAA

99) **PII:** Personal Identifiable Information

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

101) **POA&M:** Plan of Action and Milestones

102) **Program Management:** The process of managing several related projects.

103) **PMP - 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.

104) **Project Implementation Schedule:** A comprehensive list of planned dates for performing schedule activities and/or tasks with the associated planned due dates, resources, and durations for meeting schedule milestones required for implementation.

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

106) **Provider:** The umbrella term used to refer to individual practitioners and facilities, entities, organizations, and atypical organizations or institutions

107) **PST:** Production Simulation Test

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

109) **RASP**: Runtime Application Self Protection

110) **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.

111) **Requirements Management:** The process of documenting, analyzing, tracing, prioritizing, and agreeing on requirements and then controlling change and communicating to relevant stakeholders. It is a continuous process throughout a project.

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

113) **Recipient**: Synonymous with Beneficiary or Member. Person enrolled in a participating Medicaid program.

114) **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.

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

116) **RFP:** Request for Proposal is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over $10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services.

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

118) **Rule:** Interoperability and Patient Access Final Rule CMS-9115-F (1)

119) **SaaS**: Software as a Service. A software licensing model, which allows access to software on a subscription basis using external servers.

120) **SAST**: Static Application Security Testing

121) **SDLC**: Software Development Life Cycle

122) **Security Monitoring Plan**: Plan that documents the collection, analysis, and escalation of indications and warnings to detect and respond to security intrusions.

123) **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.

124) **Severity Definitions**: The state reserves the right to adjust the severity level set by the service 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.

125) **(Significant) Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:

    i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or

    ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

126) **SIP:** System Integration Platform. A cohesive set of integration software products that enable users to develop, secure and govern integration flows that connect applications, systems, services, and data stores.

127) **SI:** System Integrator. Vendor managing the System Integration Platform

128) **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.

129) **SLA**: Service Level Agreement. Part of a contract that defines what services a vendor will provide and the required level or standard for those services.

130) **SMART on FHIR:** An open, free, universal and standards-based API developed by SMART Health IT

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

132) **SAE 18 SOC 2 TYPE 2:** A detailed report on the controls of a service organization’s systems used to process customer data and the confidentiality and privacy of the information processed by these systems. This report provides assurance of the security, availability, and process integrity of these systems.

133) **SME:** Subject Matter Expert

134) **SSDF:** Secure Software Development Framework

135) **SSO**: Single Sign On

136) **SSP**: System Security Plan

137) **State Contract Administrator:** A person who performs administrative functions related to dealing with contracts, like 1) request to bid, 2) evaluating bid, 3) allotment of contract, 4) Implementing contract, 5) measuring completed work, and 6) computing payments .

138) **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.

139) **Technical Specifications:** Means, as used herein, a specification that documents Documentation of the requirements of a system or system component. Typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance standards, or similar terms.

140) **Test Management Plan**: Plan that documents the activity of managing the computer software testing process.

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

142) **Transition Plan**: Plan that outlines the processes to be followed during the turnover stage of any project.

143) **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.

144) **TBD**: To be Determined.

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

146) **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.

147) **USCDI**: US Core Data for Interoperability

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

149) **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.

150) **WAF:** Web Application Firewall

151) **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.

152) **Work Product:** Incidental artifact created during the performance of the Contract. All work products created during the performance of the Contract become the property of the State.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

Section 1. General Terms and Conditions Applicable to All Purchases

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

Agreement means the contract awarded pursuant to this RFP.

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:** The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State contracting authority. Vendor shall provide the State with complete copies of any agreements made by and between Vendor and all subcontractors. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor and the Agreement. Any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third-party beneficiary of the Agreement; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.

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:** Vendor 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 the purpose of obtaining any Contract or award issued by the State. Vendor 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 State Purchasing Agent in writing prior to acceptance of the Agreement or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign the Agreement and bind the Party to the terms and conditions of this RFP. Vendor and their 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 Agreement; obligation or Contract for future award of compensation as an inducement or consideration for making the Agreement. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B..1206, or other provision of law.

8) **AVAILABILITY OF FUNDS:** Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in the Agreement. If the Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of the Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in this RFP. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under the Agreement, terminate any Services supplied to the Agency under the Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.

9) **ACCEPTANCE PROCESS:**
   a) 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.
   b) 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.

c) 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.

d) 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) **<u>PAYMENT TERMS</u>:** Monthly Payment terms are Net 30 days after receipt of correct invoice (with completed timesheets for Vendor personnel) and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the Agency will be permitted based upon, or arising from, the Agency'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. Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:

a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or

b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however

c) 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 Contract obligations.

11) **<u>EQUAL EMPLOYMENT OPPORTUNITY</u>:** Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.

12) **<u>ADVERTISING/PRESS RELEASE</u>:** The Vendor absolutely shall not publicly disseminate any information concerning the Agreement without prior written approval from the State or its Agent. For the purpose of this provision of the Agreement, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.

13) **<u>LATE DELIVERY</u>:** 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 so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.

14) **<u>ACCESS TO PERSONS AND RECORDS</u>:** Pursuant to N.C.G.S. §147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any Department, board, officer, commission, institution, or other agency of the State of North Carolina

pursuant to the performance of the Agreement or to costs charged to the Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of the Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation. *Any such audit shall be conducted only upon prior written notice of thirty (30) days or more, and with the concurrence of The State for the date and time of any audit, and adherence to The State's security requirements during regular business hours at The State's offices and shall not unreasonably interfere with The State's business activities.*

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

a) **Worker's Compensation** - The Vendor 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 $100,000.00, covering all of Vendor's employees who are engaged in any work under the Agreement. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Agreement; and

b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of $2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and

c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired, and non-owned vehicles, used in connection with the Agreement. The minimum combined single limit shall be $500,000.00 bodily injury and property damage; $500,000.00 uninsured/under insured motorist; and $5,000.00 medical payment; and

d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of the Agreement. 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 Vendor shall at all times 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 the Agreement. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Agreement.

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) **<u>CONFIDENTIALITY</u>:** In accordance with N.C.G.S. §143B-1350(e) 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) **<u>TERMINATION</u>:** 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) <u>Termination for Cause</u>: 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) <u>Termination for Convenience Without Cause</u>: 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) <u>Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.</u>

22) **<u>LIMITATION OF VENDOR'S LIABILITY</u>:**

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, wilful 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:** Time is of the essence in the performance of the Agreement.

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:** Any notices required under the Agreement should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.

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:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of the Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

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:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

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 State 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) <u>ELECTRONIC PROCUREMENT</u>: **(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 State'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) <u>PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:</u>

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

a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:

   i) Cancel the Stop Work Order, or

   ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.

b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:

   i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and

   ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.

c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.
d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

42) TRANSITION ASSISTANCE

a) If the Contract is not renewed at the end of the Contract Term, or is terminated prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or Termination of the Contract, all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees.
b) Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Contract, (not withstanding this expiration or termination) except for those Vendor terms or conditions that do not reasonably apply to such transition assistance.
c) The State 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 State 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 State 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 Statement 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 perpetual or for the term of the contract (pick one, delete the other), 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) **STATE PROPERTY AND INTANGIBLES RIGHTS:** The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data, and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

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

1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third-party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third-party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).
   a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
   b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
   c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.

2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Statement 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 noticed 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 a 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) **<u>WARRANTY OF NON-INFRINGEMENT; REMEDIES:</u>**

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) **<u>ACCESS AVAILABILITY; REMEDIES</u>**

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) **<u>EXCLUSIONS</u>**:

a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.

b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or services failures substantially caused by:
   - i) Actions of non-Vendor personnel;
   - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
   - iii) Force Majeure conditions set forth hereinbelow.
   - iv) The State's sole misuse of, or its own inability to use, the Services

6) **<u>PEFORMANCE REVIEW AND ACCOUNTABILITY:</u>** 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**:

Reserved

8) **VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:** Reserved

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 above.
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:** Reserved

13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES**: Reserved

14) **AVAILABILITY OF FUNDS:** Reserved

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>: Reserved

17) <u>CONFIDENTIALITY:</u> Reserved

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 controls 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, and other 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 of 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 and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

ATTACHMENT C: AGENCY TERMS AND CONDITIONS

DHHS PRIVACY AND SECURITY OFFICE (PSO)

1) COMPLIANCE WITH APPLICABLE LAWS

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

2) NC STATE AND DEPARTMENT OF HEALTH AND HUMAN SERVICES PRIVACY AND REQUIREMENTS

The Vendor shall implement internal data security measures, and other industry security best practices utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations, DHHS privacy and security policies. The Vendor will maintain all Privacy and security safeguards throughout the term of this agreement. In addition, the Vendor agrees to maintain compliance with the following:

NCDHHS Privacy Manual and Security Manual, both located here:
https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security
NC Statewide Information Security policies, located here:
https://it.nc.gov/resources/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies

3) HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

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, the Vendor agrees to comply with all HIPAA requirements and will execute such agreements and practices as the Division or Office may require ensuring compliance.

HIPAA regulations for privacy and security at:
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

4) CONFIDENTIALITY:

a) **CONFIDENTIALITY:** The Vendor shall protect the confidentiality of all information, data, instruments, documents, studies, or reports given to the Vendor under this agreement in accordance with federal statutes and regulations including: the Privacy Rule at 45 C.F.R. Parts 160 and 164, subparts A and E , Security Standards at 45 C.F.R. Parts 160, 162 and 164, subparts A and C (“the Security Rule”), and the applicable provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH). The Vendor shall not disclose or make information available to any individual or organization without the prior written consent of the DHHS Division or Office except permitted by this contract for performing its obligations. The Vendor acknowledges that in receiving, storing, and processing confidential information, it will implement necessary privacy and security measures to safeguard all information.

b) **ENCRYPTION AND TRANSMISSION:** Reserved

c) **DATA SECURITY:** The Vendor shall implement internal data security measures, environmental safeguards, firewalls, access controls, and other industry security best practices utilizing appropriate hardware and software necessary to monitor, maintain, and ensure data integrity in accordance with all applicable federal regulations, state regulations and DHHS privacy and security policies. In the event the Vendor obtains written consent by a DHHS Division or Office to enter into a third-party agreement to whom the Vendor provides confidential information, the Vendor shall ensure that such agreement contains provisions reflecting obligations of data confidentiality and data security stringent as those set forth in the contract.

d) **DUTY TO REPORT:** In addition to any DHHS Privacy and Security Office (PSO) notification requirements in a Business Associate Agreement (BAA) with a DHHS Division or Office, the Vendor shall report all suspected and confirmed privacy/security incidents or privacy/Security Breaches involving unauthorized access, use, disclosure, modification, or data destruction to the DHHS Privacy and Security Office at https://www.ncdhhs.gov/about/administrative-divisions-offices/office-privacy-security within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare & Medicaid Services (CMS) data, the vendor shall report the incident within one (1) hour after the incident is first discovered. At a minimum, such privacy and security incident report will contain to the extent known: the nature of the incident, specific information about the data compromised, the date the privacy or security incident occurred, the date the Vendor was notified, and the identity of affected or potentially affected individual(s). During the performance of this contract, the vendor is to notify the DHHS Privacy and Security Office of any contact by the federal Office for Civil Rights (OCR) received by the vendor. In addition, the Vendor will reasonably cooperate with DHHS Divisions and Offices to mitigate the damage or harm of such security incidents.

e) **COST BORNE BY VENDOR:** Reserved.

5) CONTINUOUS MONITORING:

a) The Vendor shall maintain compliance with the State Chief Information Officer's (CIO) Continuous Monitoring Process mandate, requiring that Vendors hosting state-owned data outside of NC DIT's infrastructure environment work with state agencies to implement a risk management program that continuously monitors risk through the performance of assessments, risk analysis, and data inventory.

b) To comply with this mandate, set forth in N.C.G.S § 143B-1376 http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_143B.html and based upon NIST 800-137, ""Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", the Vendor shall perform security/risk assessments on its information systems using the latest NIST 800-53 controls to assess its compliance with enterprise security standards as outlined below.

Security Assessment:

i) Vendors providing Infrastructure as a Service, Platform as a Service and/or Software as a Service for the state agency are required to obtain approval from the DHHS Privacy and Security Office to ensure their compliance with statewide security policies.

ii) To obtain such approval, the Vendor shall annually provide 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. State agencies will be 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 to the Vendor's compliance to the State CIO.

c) The Vendor shall work with the state agency to provide a data inventory of all cloud hosted services, by assisting the state agency with completing 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.

d) DHHS 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 DHHS designated resources and DHHS 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 DHHS requirements.

6) OVERSIGHT

a) ACCESS TO PERSONS AND RECORDS: Reserved

b) **RECORD RETENTION:** Records shall not be destroyed, purged, or disposed of without the express written consent of the DHHS Division or Office. State basic records retention policy requires all grant records to be retained for a minimum of five years or until all audit exceptions have been resolved, whichever is longer. If the contract is subject to federal policy and regulations, record retention may be longer than five years. Records must be retained for a period of three years following submission of the final Federal Financial Status Report, if applicable, or three years following the submission of a revised final Federal Financial Status Report. Also, if any litigation, claim, negotiation, audit, disallowance action, or other action involving this Contract has been started before expiration of the five-year retention period described above, the records must be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular five-year period described above, whichever is later. The record retention period for Temporary Assistance for Needy Families (TANF) and MEDICAID and Medical Assistance grants and programs is a minimum of ten years. The record retention period for the Health Insurance Portability and Accountability Act (HIPAA) is six years. For the Internal Revenue Service (IRS) and the Social Security Administration (SSA), the record retention period is seven years.

7) FLOW-DOWN:

If a sub-vendor is used in the performance of this contract, it will be with written approval of NCDHHS including PSO. All the security and privacy requirements stated in the sections titled *Compliance with Applicable Laws, NC State and Department of Health and Human Services Privacy and Security Requirements, Health Insurance Portability and Accountability Act (HIPAA), Confidentiality, Continuous Monitoring, Oversight,* and *Flow-Down,* and all their sub-sections shall be included with no modifications to each sub-contract. Sub-contract language shall be made available to NCDHHS and PSO for review if requested.

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	

HISTORICALLY UNDERUTILIZED BUSINESSES

Historically Underutilized Businesses (HUBs) consist of minority, women and disabled business firms that are at least fifty-one percent owned and operated by an individual(s) of the categories. Also included as HUBs are disabled business enterprises and non-profit work centers for the blind and severely disabled."

Pursuant to N.C.G.S. §§ 143B-1361(a), 143-48 and 143-128.4, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. This includes utilizing subcontractors to perform the required functions in this RFP. Contact the North Carolina Office of historically Underutilized Businesses at 919-807-2330 with questions concerning NC HUB certification. http://ncadmin.nc.gov/businesses/hub

Respond to the questions below.

1. Is Vendor a Historically Underutilized Business? □ Yes □ No

2. Is Vendor Certified with North Carolina as a Historically Underutilized Business? □ Yes □ No

   If so, state HUB classification:
   ____

ATTACHMENT E: COST FORM

INSTRUCTIONS to VENDORS

Pricing Tables Submission Instructions:
The Cost Proposal Workbook is required to be completed in Excel as part of the RFP submission. Describe how the Vendor can 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 sheet 3 Implementation Costs", sheets 4A & 4B O&M Costs, and sheet 6 Additional Costs. Vendors should also supply supporting information in sheet 5 Labor Rates, and sheet 7 Assumptions, sufficient for the State to have a clear understanding of the Vendor's pricing methodology.

To obtain an electronic version of the Cost Proposal Workbook in Excel format, please contact the Contract Specialist listed on the first page of this document.

Basis of Estimates (BOEs):
Vendors must include introductory information in their BOEs in order to describe any general method, assumptions, or other useful information needed to understand the estimates. The State is interested in understanding how each Vendor estimated the prices in its Proposal rather than forcing conformance to a specific format. As such, Vendors may format the BOEs in any reasonable manner that communicates the required information. BOEs are separated by pricing table to ensure consistency.

Vendor's must describe their bases of estimates (BOEs) in support of all pricing tabs in their Cost Proposal Workbook, and the awarded Vendor shall continue this practice throughout the life of the Contract. Each pricing table shall have a basis of estimate associated with it. 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

Bases of estimates may be submitted in any reasonable format that is easy to understand and which includes, at a minimum, the above elements. BOEs should **not** be included on the same excel workbook as the Vendor's Cost Proposal Workbook. Note that BOEs are not required to describe the derivation of labor rates (compensation, benefits, etc.). In addition, statements such as, "in our experience, it takes approximately XXX hours to complete this effort," do not, by themselves, constitute sufficient BOEs. BOEs should be responded to in the same sequence as the cost tables.

Department will not pay separately for implementation costs incurred in standing up Vendor's solution. Those cost should be included in their respective year along with all other associated costs during that timeframe.

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 Cost Proposal Tables contained in the Excel Workbook must be completed and submitted by Vendor in accordance with these INSTRUCTIONS to VENDORS and the Cost Proposal Workbook format.

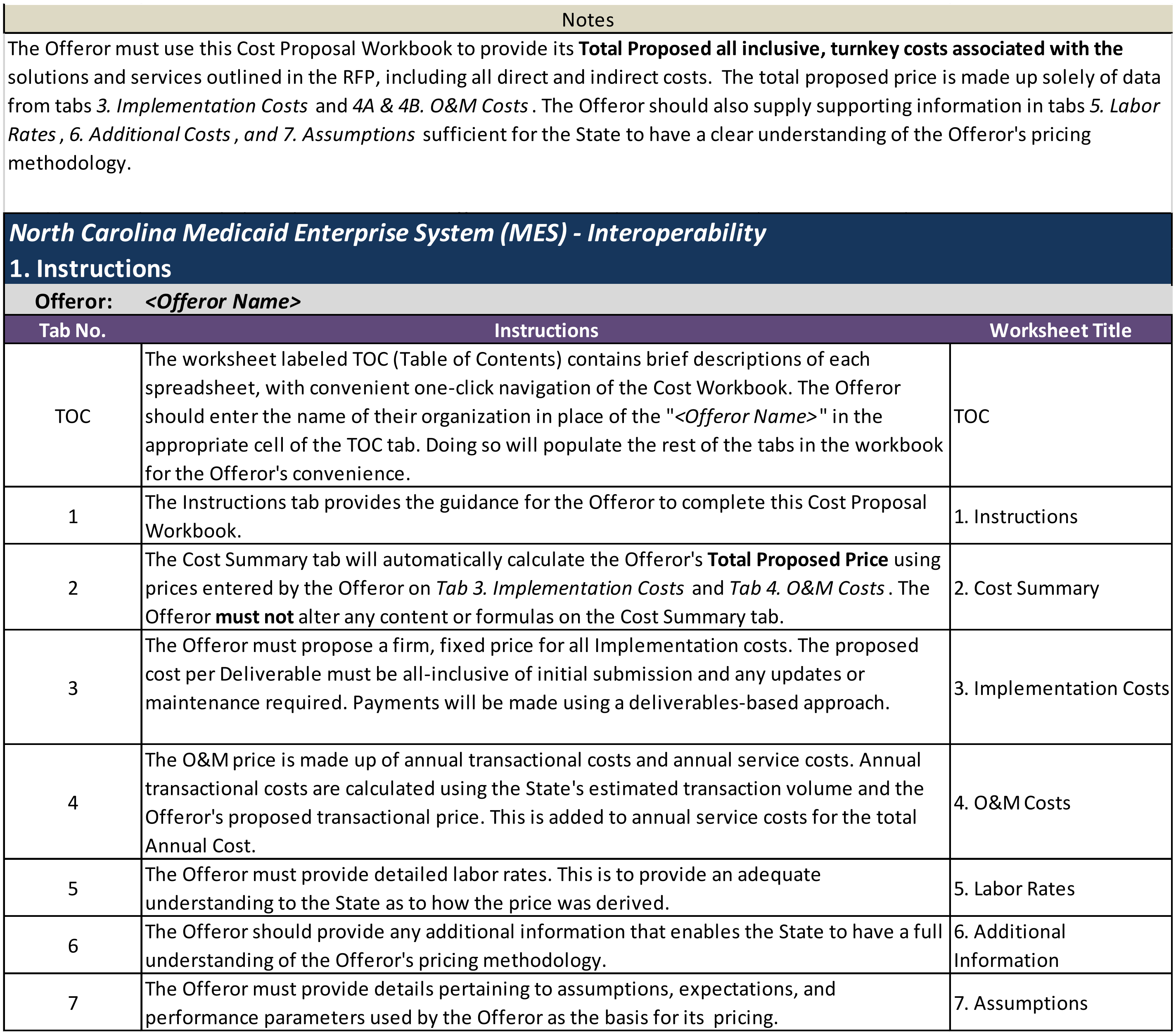
Note: The screen images in the following pages are captured from the Cost Proposal Workbook and are provided for reference only. The Cost Proposal Workbook must be completed in Excel format. To obtain an electronic version of the Cost Proposal Workbook in Excel format, please contact the Contract Specialist listed on the first page of this document.

Cost Proposal Workbook

North Carolina Medicaid Enterprise System (MES) - Interoperability & Patient Access

Enter Offeror Name: ***<Offeror Name>***

Table of Contents



Notes

The Offeror must use this Cost Proposal Workbook to provide its **Total Proposed all inclusive, turnkey costs associated with the** solutions and services outlined in the RFP, including all direct and indirect costs. The total proposed price is made up solely of data from tabs *3. Implementation Costs* and *4A & 4B. O&M Costs*. The Offeror should also supply supporting information in tabs *5. Labor Rates*, *6. Additional Costs*, *and 7. Assumptions* sufficient for the State to have a clear understanding of the Offeror's pricing methodology.

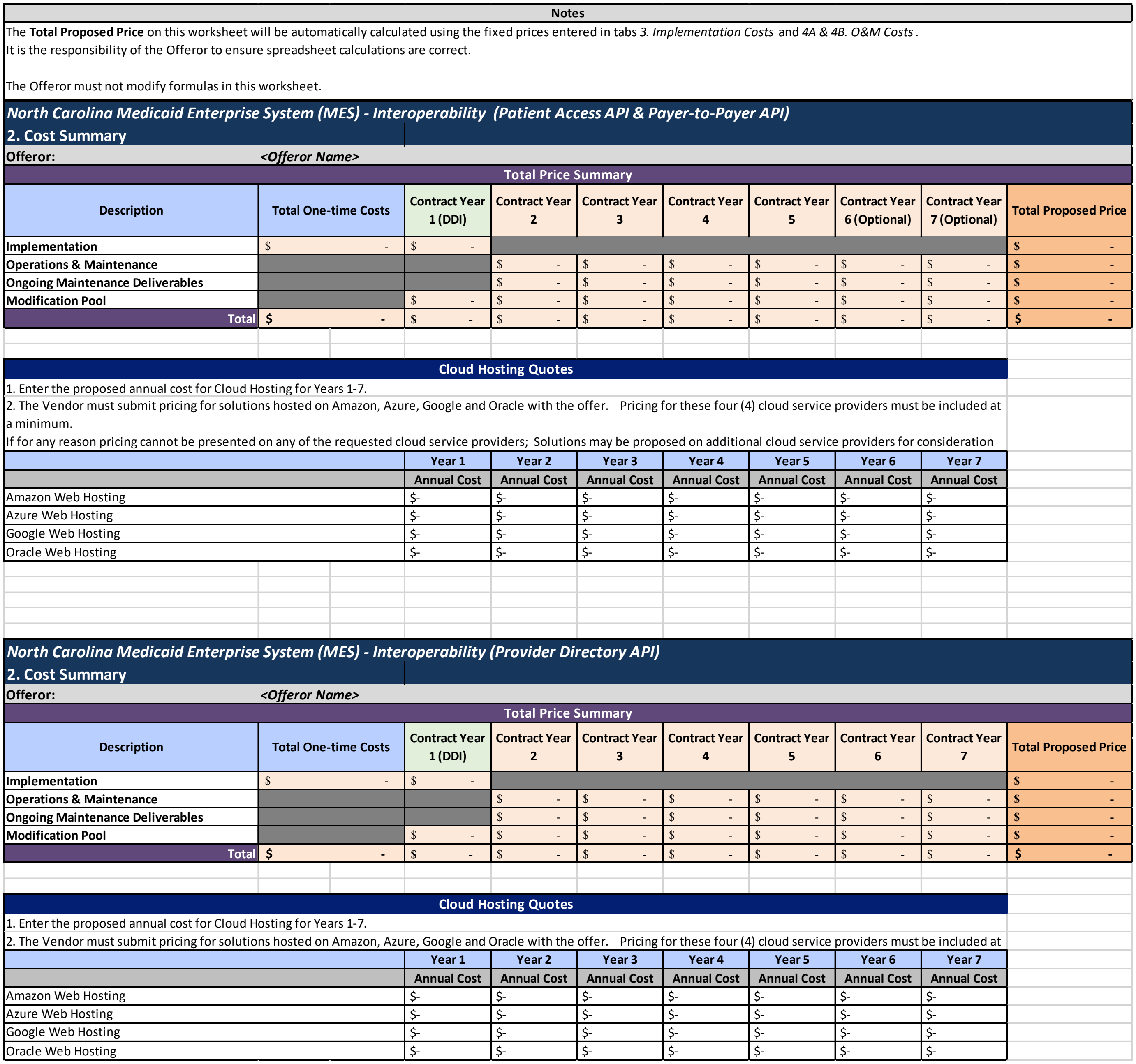
North Carolina Medicaid Enterprise System (MES) - Interoperability

1. Instructions

Offeror: ***<Offeror Name>***

Tab No.	Instructions	Worksheet Title
TOC	The worksheet labeled TOC (Table of Contents) contains brief descriptions of each spreadsheet, with convenient one-click navigation of the Cost Workbook. The Offeror should enter the name of their organization in place of the "*<Offeror Name>*" in the appropriate cell of the TOC tab. Doing so will populate the rest of the tabs in the workbook for the Offeror's convenience.	TOC
1	The Instructions tab provides the guidance for the Offeror to complete this Cost Proposal Workbook.	1. Instructions
2	The Cost Summary tab will automatically calculate the Offeror's **Total Proposed Price** using prices entered by the Offeror on *Tab 3. Implementation Costs* and *Tab 4. O&M Costs*. The Offeror **must not** alter any content or formulas on the Cost Summary tab.	2. Cost Summary
3	The Offeror must propose a firm, fixed price for all Implementation costs. The proposed cost per Deliverable must be all-inclusive of initial submission and any updates or maintenance required. Payments will be made using a deliverables-based approach.	3. Implementation Costs
4	The O&M price is made up of annual transactional costs and annual service costs. Annual transactional costs are calculated using the State's estimated transaction volume and the Offeror's proposed transactional price. This is added to annual service costs for the total Annual Cost.	4. O&M Costs
5	The Offeror must provide detailed labor rates. This is to provide an adequate understanding to the State as to how the price was derived.	5. Labor Rates
6	The Offeror should provide any additional information that enables the State to have a full understanding of the Offeror's pricing methodology.	6. Additional Information
7	The Offeror must provide details pertaining to assumptions, expectations, and performance parameters used by the Offeror as the basis for its pricing.	7. Assumptions

1. Instructions



Notes

The **Total Proposed Price** on this worksheet will be automatically calculated using the fixed prices entered in tabs *3. Implementation Costs* and *4A & 4B. O&M Costs*.
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.

The Offeror must not modify formulas in this worksheet.

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

2. Cost Summary

Offeror: ***<Offeror Name>***

Total Price Summary

Description	Total One-time Costs	Contract Year 1 (DDI)	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Contract Year 6 (Optional)	Contract Year 7 (Optional)	Total Proposed Price
Implementation	$ -	$ -							$ -
Operations & Maintenance			$ -	$ -	$ -	$ -	$ -	$ -	$ -
Ongoing Maintenance Deliverables			$ -	$ -	$ -	$ -	$ -	$ -	$ -
Modification Pool		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total	**$ -**	$ -	$ -	$ -	$ -	$ -	$ -	$ -	**$ -**

Cloud Hosting Quotes

1. Enter the proposed annual cost for Cloud Hosting for Years 1-7.
2. The Vendor must submit pricing for solutions hosted on Amazon, Azure, Google and Oracle with the offer. Pricing for these four (4) cloud service providers must be included at a minimum.

If for any reason pricing cannot be presented on any of the requested cloud service providers; Solutions may be proposed on additional cloud service providers for consideration

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost
Amazon Web Hosting	$-	$-	$-	$-	$-	$-	$-
Azure Web Hosting	$-	$-	$-	$-	$-	$-	$-
Google Web Hosting	$-	$-	$-	$-	$-	$-	$-
Oracle Web Hosting	$-	$-	$-	$-	$-	$-	$-

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

2. Cost Summary

Offeror: ***<Offeror Name>***

Total Price Summary

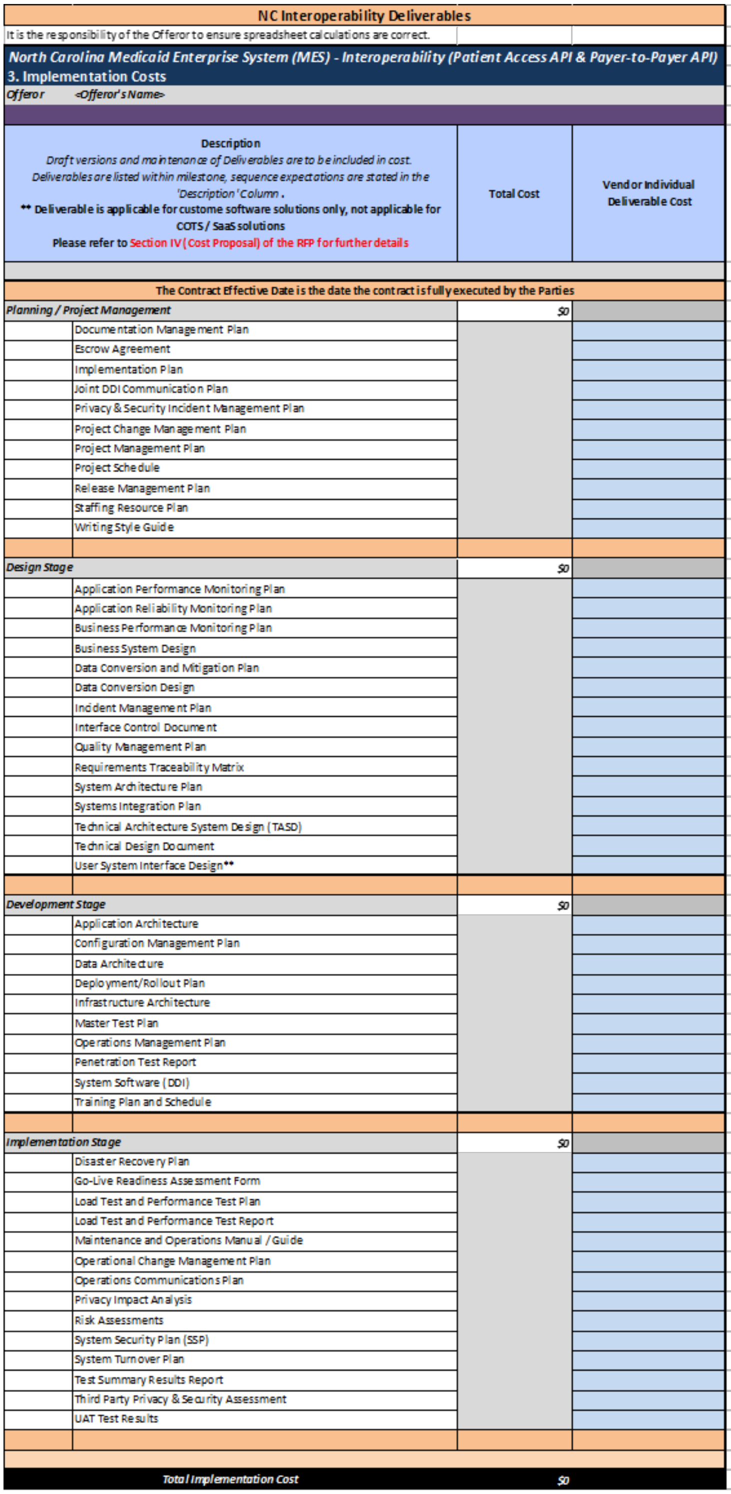
Description	Total One-time Costs	Contract Year 1 (DDI)	Contract Year 2	Contract Year 3	Contract Year 4	Contract Year 5	Contract Year 6	Contract Year 7	Total Proposed Price
Implementation	$ -	$ -							$ -
Operations & Maintenance			$ -	$ -	$ -	$ -	$ -	$ -	$ -
Ongoing Maintenance Deliverables			$ -	$ -	$ -	$ -	$ -	$ -	$ -
Modification Pool		$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Total	**$ -**	$ -	$ -	$ -	$ -	$ -	$ -	$ -	**$ -**

Cloud Hosting Quotes

1. Enter the proposed annual cost for Cloud Hosting for Years 1-7.
2. The Vendor must submit pricing for solutions hosted on Amazon, Azure, Google and Oracle with the offer. Pricing for these four (4) cloud service providers must be included at

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost	Annual Cost
Amazon Web Hosting	$-	$-	$-	$-	$-	$-	$-
Azure Web Hosting	$-	$-	$-	$-	$-	$-	$-
Google Web Hosting	$-	$-	$-	$-	$-	$-	$-
Oracle Web Hosting	$-	$-	$-	$-	$-	$-	$-

2. Cost Summary: The Cost Summary tab calculates the Total Proposed Price based on data from the Implementation Costs and O&M Costs tabs..



NC Interoperability Deliverables

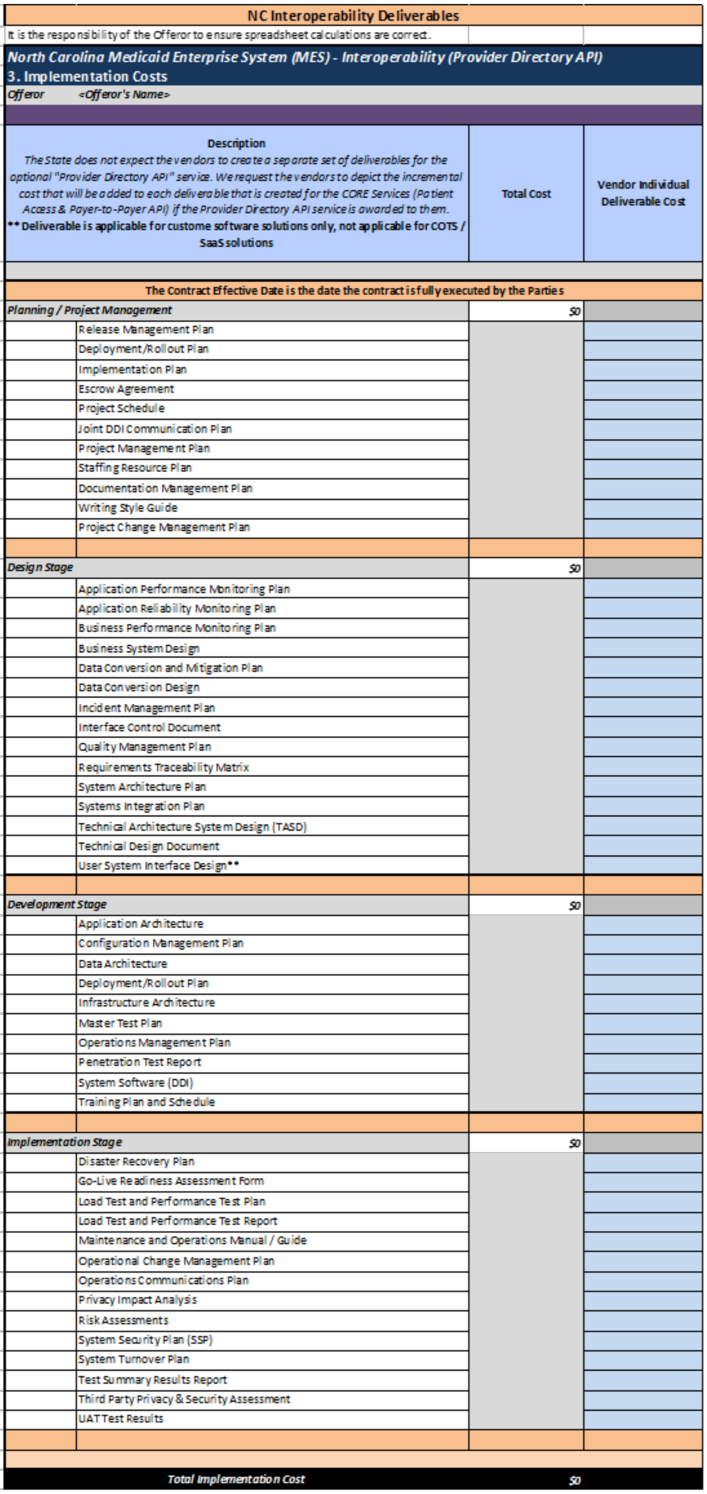
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

3. Implementation Costs

Offeror *<Offeror's Name>*

Description *Draft versions and maintenance of Deliverables are to be included in cost. Deliverables are listed within milestone, sequence expectations are stated in the 'Description' Column .* **** Deliverable is applicable for custome software solutions only, not applicable for COTS / SaaS solutions** **Please refer to Section IV (Cost Proposal) of the RFP for further details**	**Total Cost**	**Vendor Individual Deliverable Cost**
The Contract Effective Date is the date the contract is fully executed by the Parties		
Planning / Project Management	*$0*	
Documentation Management Plan		
Escrow Agreement		
Implementation Plan		
Joint DDI Communication Plan		
Privacy & Security Incident Management Plan		
Project Change Management Plan		
Project Management Plan		
Project Schedule		
Release Management Plan		
Staffing Resource Plan		
Writing Style Guide		
Design Stage	*$0*	
Application Performance Monitoring Plan		
Application Reliability Monitoring Plan		
Business Performance Monitoring Plan		
Business System Design		
Data Conversion and Mitigation Plan		
Data Conversion Design		
Incident Management Plan		
Interface Control Document		
Quality Management Plan		
Requirements Traceability Matrix		
System Architecture Plan		
Systems Integration Plan		
Technical Architecture System Design (TASD)		
Technical Design Document		
User System Interface Design**		
Development Stage	*$0*	
Application Architecture		
Configuration Management Plan		
Data Architecture		
Deployment/Rollout Plan		
Infrastructure Architecture		
Master Test Plan		
Operations Management Plan		
Penetration Test Report		
System Software (DDI)		
Training Plan and Schedule		
Implementation Stage	*$0*	
Disaster Recovery Plan		
Go-Live Readiness Assessment Form		
Load Test and Performance Test Plan		
Load Test and Performance Test Report		
Maintenance and Operations Manual / Guide		
Operational Change Management Plan		
Operations Communications Plan		
Privacy Impact Analysis		
Risk Assessments		
System Security Plan (SSP)		
System Turnover Plan		
Test Summary Results Report		
Third Party Privacy & Security Assessment		
UAT Test Results		
Total Implementation Cost	*$0*	



NC Interoperability Deliverables

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

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

3. Implementation Costs

Offeror *<Offeror's Name>*

Description *The State does not expect the vendors to create a separate set of deliverables for the optional "Provider Directory API" service. We request the vendors to depict the incremental cost that will be added to each deliverable that is created for the CORE Services (Patient Access & Payer-to-Payer API) if the Provider Directory API service is awarded to them.* **** Deliverable is applicable for custome software solutions only, not applicable for COTS / SaaS solutions**	**Total Cost**	**Vendor Individual Deliverable Cost**
The Contract Effective Date is the date the contract is fully executed by the Parties		
Planning / Project Management	*$0*	
Release Management Plan		
Deployment/Rollout Plan		
Implementation Plan		
Escrow Agreement		
Project Schedule		
Joint DDI Communication Plan		
Project Management Plan		
Staffing Resource Plan		
Documentation Management Plan		
Writing Style Guide		
Project Change Management Plan		
Design Stage	*$0*	
Application Performance Monitoring Plan		
Application Reliability Monitoring Plan		
Business Performance Monitoring Plan		
Business System Design		
Data Conversion and Mitigation Plan		
Data Conversion Design		
Incident Management Plan		
Interface Control Document		
Quality Management Plan		
Requirements Traceability Matrix		
System Architecture Plan		
Systems Integration Plan		
Technical Architecture System Design (TASD)		
Technical Design Document		
User System Interface Design**		
Development Stage	*$0*	
Application Architecture		
Configuration Management Plan		
Data Architecture		
Deployment/Rollout Plan		
Infrastructure Architecture		
Master Test Plan		
Operations Management Plan		
Penetration Test Report		
System Software (DDI)		
Training Plan and Schedule		
Implementation Stage	*$0*	
Disaster Recovery Plan		
Go-Live Readiness Assessment Form		
Load Test and Performance Test Plan		
Load Test and Performance Test Report		
Maintenance and Operations Manual / Guide		
Operational Change Management Plan		
Operations Communications Plan		
Privacy Impact Analysis		
Risk Assessments		
System Security Plan (SSP)		
System Turnover Plan		
Test Summary Results Report		
Third Party Privacy & Security Assessment		
UAT Test Results		
Total Implementation Cost	*$0*	

3. Implementation Costs: Worksheet for one-time implementation costs based on deliverables. Total Implementation Costs is one element of the Total Proposed Price.

Notes

The workbook will calculate Total Annual Cost for costs on this page and include it as part of the Total Proposed Price in *Tab 2 - Cost Summary*.
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

4A. O&M Cost (PA API & P2P API)

Offeror <Offeror's Name>

Operations and Maintenance - Proposed Service Volumes and Costs

	Year 1	Year 2	Year 3	Year 4	Year 5	Optional Year 6	Optional Year 7
Statement of Work Services Section (Vendor Please include your Proposed O&M SOW items here)	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
Total Annual Cost	***No Charge***	$ -	$ -	$ -	$ -	$ -	$ -

Ongoing Maintenance Deliverables

Operation Stage - **Updated Upon Changing Information or by Department Request** **** Deliverable is applicable for custom software solutions only, not applicable for COTS / SaaS solutions**	Year 1	Year 2	Year 3	Year 4	Year 5	Optional Year 6	Optional Year 7
	Annual Cost	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**
Annual Survey Results	***No Charge***						
Business Continuity Plan	***No Charge***						
Configuration Management Plan	***No Charge***						
Disaster Recovery and Business Continuity Testing with the After Action Report	***No Charge***						
Disaster Recovery Plan	***No Charge***						
Lessons Learned Final Report	***No Charge***						
Maintenance and Operations Manual / Guide	***No Charge***						
Operations Communications Plan	***No Charge***						
Operations Management Plan	***No Charge***						
Penetration Test Report	***No Charge***						
Privacy Impact Analysis	***No Charge***						
Risk Assessments	***No Charge***						
SLA Self Assessment Report - Operations Phase	***No Charge***						
SOC2 TYPE 2 Report (Security Audit Reports)	***No Charge***						
Staffing Resource Plan	***No Charge***						
System Software (Operations)**	***No Charge***						
System Turnover Plan	***No Charge***						
Third Party Privacy & Security Assessment	***No Charge***						
Total Annual Cost	***No Charge***	$ -	$ -	$ -	$ -	$ -	$ -

4A. O&M Cost (PA API & P2P API): Worksheet for Operations and Maintenance costs. The total of Annual Cost is one element of the Total Proposed Price.

Notes

The workbook will calculate Total Annual Cost for costs on this page and include it as part of the Total Proposed Price in *Tab 2 - Cost Summary*.
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

4B. O&M Costs (PD API)

Offeror <Offeror's Name>

Operations and Maintenance - Proposed Service Volumes and Costs

	Year 1	Year 2	Year 3	Year 4	Year 5	Optional Year 6	Optional Year 7
Statement of Work Services Section (Vendor Please include your Proposed O&M SOW items here)	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
	No Charge						
Total Annual Cost	***No Charge***	$ -	$ -	$ -	$ -	$ -	$ -

Ongoing Maintenance Deliverables

Operation Stage - **Updated Upon Changing Information or by Department Request** **** Deliverable is applicable for custome software solutions only, not applicable for COTS / SaaS solutions**	Year 1	Year 2	Year 3	Year 4	Year 5	Optional Year 6	Optional Year 7
	Annual Cost	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**	**Annual Cost**
Annual Survey Results	***No Charge***						
Business Continuity Plan	***No Charge***						
Configuration Management Plan	***No Charge***						
Disaster Recovery and Business Continuity Testing with the After Action Report	***No Charge***						
Disaster Recovery Plan	***No Charge***						
Lessons Learned Final Report	***No Charge***						
Maintenance and Operations Manual / Guide	***No Charge***						
Operations Communications Plan	***No Charge***						
Operations Management Plan	***No Charge***						
Penetration Test Report	***No Charge***						
Privacy Impact Analysis	***No Charge***						
Risk Assessments	***No Charge***						
SLA Self Assessment Report - Operations Phase	***No Charge***						
SOC2 TYPE 2 Report (Security Audit Reports)	***No Charge***						
Staffing Resource Plan	***No Charge***						
System Software (Operations)**	***No Charge***						
System Turnover Plan	***No Charge***						
Third Party Privacy & Security Assessment	***No Charge***						
Total Annual Cost	***No Charge***	$ -	$ -	$ -	$ -	$ -	$ -

4B. O&M Costs (PD API): Worksheet for Operations and Maintenance costs. The total of Annual Cost is one element of the Total Proposed Price..

Please Estimate the time required by the State Team for the

It is the responsibility of the Offeror to ensure spreadsheet calculations are c

The Vendor shall propose a "Blended Labor Rate" for the use of OnSite Modification Pool hours here $___

The Vendor shall propose a "Blended Labor Rate" for the use of OffSite Modification Pool hours here $___

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

5. Labor Rates

Offeror: *<Offeror Name>*

Vendor Validate your DDI Staff/Role needs (Fully Loaded) - Modify as necessary

Vendor Validate your O & M Staff/Role needs (Fully Loaded) - Modify as necessary

Implementation Services		Operations & Maintenance Services	
			O&M Years 1, 2, 3, 4, & 5.
Key Personnel Roles	**Rate**	**Key Personnel Roles**	**Rate**
Account Manager	$ -	Account Manager	$ -
Contract / Vendor Performance Manager	$ -	Contract / Vendor Performance Manager	$ -
Technical Architect / Lead	$ -	Technical Architect / Lead	$ -
Technical Program Manager / Implementation Lead	$ -	Technical Program Manager / Implementation Lead	$ -
Senior Project Manager / Operations Manager	$ -	Senior Project Manager / Operations Manager	$ -
Senior Test Manager	$ -	Senior Test Manager	$ -
Senior Test Engineer	$ -	Senior Test Engineer	$ -
IT Security Manager	$ -	IT Security Manager	$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
Additional Role 1	$ -	Additional Role 1	$ -
Additional Role 2	$ -	Additional Role 2	$ -
Additional Role 3	$ -	Additional Role 3	$ -

Notes

This tab must be used to provide contractor / subcontractor hourly labor rates for the various classifications and grades of personnel. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Offeror's staff training, project facility, and any other expenses associated with the delivery and implementation of the proposed items must be included in the Offeror's costs and fixed hourly rates. The yellow highlighted titles reflect Key Personnel Roles as described in Attachment C of the RFP.

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

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

The Vendor shall propose a "Blended Labor Rate" for the use of OnSite Modification Pool hours here $___

The Vendor shall propose a "Blended Labor Rate" for the use of OffSite Modification Pool hours here $___

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

5. Labor Rates

Offeror: *<Offeror Name>*

Vendor Validate your DDI Staff/Role needs (Fully Loaded) - Modify as necessary

Vendor Validate your O & M Staff/Role needs (Fully Loaded) - Modify as necessary

Implementation Services		Operations & Maintenance Services	
			O&M Years 1, 2, 3, 4, & 5.
Key Personnel Roles	**Rate**	**Key Personnel Roles**	**Rate**
Account Manager	$ -	Account Manager	$ -
Contract / Vendor Performance Manager	$ -	Contract / Vendor Performance Manager	$ -
Technical Architect / Lead	$ -	Technical Architect / Lead	$ -
Technical Program Manager / Implementation Lead	$ -	Technical Program Manager / Implementation Lead	$ -
Senior Project Manager / Operations Manager	$ -	Senior Project Manager / Operations Manager	$ -
Senior Test Manager	$ -	Senior Test Manager	$ -
Senior Test Engineer	$ -	Senior Test Engineer	$ -
IT Security Manager	$ -	IT Security Manager	$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
	$ -		$ -
Additional Role 1	$ -	Additional Role 1	$ -
Additional Role 2	$ -	Additional Role 2	$ -
Additional Role 3	$ -	Additional Role 3	$ -

Notes

This tab must be used to provide contractor / subcontractor hourly labor rates for the various classifications and grades of personnel. Applicable purchase, delivery, tax, services, safety, license, travel, per diem, Offeror's staff training, project facility, and any other expenses associated with the delivery and implementation of the proposed items must be included in the Offeror's costs and fixed hourly rates. The yellow highlighted titles reflect Key Personnel Roles as described in Attachment C of the RFP.

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

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

5. Labor Rates: Worksheet for Offeror to itemize hourly rate structures used in developing Offeror's proposed price.

Notes

Offeror should provide any additional information it deems necessary to providing a full understanding of the Offeror's pricing methodology. Provide reference to RFP component and section if appropriate.
It is the responsibility of the Offeror to ensure spreadsheet calculations are correct.

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

6. Additional Costs

Offeror: *<Offeror Name>*

Item #	RFP Component	RFP Section	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

6. Additional Costs

Offeror: *<Offeror Name>*

Item #	RFP Component	RFP Section	Description
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

6a. Additional Costs: Worksheet for Offeror to provide additional details of their pricing methodology for this project.

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

North Carolina Medicaid Enterprise System (MES) - Interoperability (Patient Access API & Payer-to-Payer API)

7. Assumptions

Offeror: ***<Offeror Name>***

Item #	Response Template	Template Section	Description	Rationale	Cost Impact If Assumption is Invalid
1					$ -
2					$ -
3					$ -
4					$ -
5					$ -
6					$ -
7					$ -
8					$ -
9					$ -

Notes

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

The Offeror shall provide pricing consistent with the following:

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

North Carolina Medicaid Enterprise System (MES) - Interoperability (Provider Directory API)

7. Assumptions

Offeror: ***<Offeror Name>***

Item #	Response Template	Template Section	Description	Rationale	Cost Impact If Assumption is Invalid
1					$ -
2					$ -
3					$ -
4					$ -
5					$ -
6					$ -
7					$ -
8					$ -
9					$ -

Notes

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

The Offeror shall provide pricing consistent with the following:

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

7. Assumptions: Worksheet for Offeror to itemize all assumptions upon which its pricing is dependent.

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

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

a) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the United States.

b) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.

Will Vendor perform any work outside of the United States? □ YES □ NO

ATTACHMENT H: VENDOR REFERENCES/PAST PERFORMANCE

The electronic version of the template for the Past Performance Questionnaire, found in this Attachment H, may be requested by contacting the Contract Specialist.

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: 30-22174
Interoperability – Patient Access

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 CMS Interoperability Patient Access Final Rule 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 Interoperability Solution to a State Medicaid program.						
SUPPORTING INFORMATION:	**E**	**V**	**S**	**M**	**U**	**N/A**

TE4: Contractor provided an effective solution for the Patient Access API, Provider Directory API, and Payer to Payer API.						
SUPPORTING INFORMATION:	**E**	**V**	**S**	**M**	**U**	**N/A**

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

QUALITY OF SERVICES

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

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

SCHEDULE AND COST

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

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

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

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

PART E: General Comments and Signature

PLEASE PROVIDE ANY ADDITIONAL COMMENTS CONCERNING THIS CONTRACTOR’S PERFORMANCE, AS DESIRED.

Based on what you know today about the Contractor’s ability to execute what they promised in their proposal, would you award another contract to the Contractor, if given the choice? Yes or No. Please explain in the area below.

Have there been any indications that the Contractor has had any financial problems? Yes or No. Please explain in the area below.	
RESPONDENT SIGNATURE: Please provide your signature confirming the information you have provided is an objective assessment of the Contractor’s past performance.	DATE:

Thank you for your prompt response and assistance!

ATTACHMENT I: FINANCIAL REVIEW FORM

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

1. Vendor Name:
2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):
3. Have you been in business for more than three years? ☒
   ☒ Yes ☐ No
4. Have you filed for bankruptcy in the past three years? ☐ Yes ☐ No
5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copyof the notification letters. ☐ Yes ☐ No

6. Are the financial figures below based on audited financial statements? ☐ Yes ☐ No
7. Start Date of financial statements:
   End Date of financial statements:
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:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
Cash and Temporary Investments			
Accounts Receivable (beginning of year)			
Accounts Receivable (end of year)			
Average Account Receivable for the Year (calculated)			
Inventory (beginning of year)			
Inventory (end of year)			
Average Inventory for the Year (calculated)			
Current Assets			
Current Liabilities			
Total Liabilities			
Total Stockholders’ Equity (beginning of year)			
Total Stockholders’ Equity (end of year)			
Average Stockholders’ Equity during the year (calculated)			
INCOME STATEMENT DATA			
Net Sales			
Cost of Goods Sold (COGS)			
Gross Profit (Net Sales minus COGS) (calculated)			
Interest Expense for the Year			
Net Income after Tax			
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)			

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 iServer (Orbus Software) as a central repository for all MES EA information and artifacts. All MES vendors will be given access to the iServer environment and will be required to enter architectural details into this system. The iServer 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 iServer 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 iServer 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. Key Personnel cost should be included in the fixed support cost and not be viewed as resources billable at an hourly rate. NCDHHS shall have full access to key personnel and 100% of their time must be dedicated to this Contract. Any resources proposed as shared must be identified along with the percentage of time expected on this project. Any resources proposed at less than 100% (excluding the Account Manager) must be approved by the State Contract Manager. All other staff should be included in the fixed cost and not be listed as Key.

b) Vendor must identify key personnel to be assigned for the duration of the Contract. Key Personnel must be identified and mapped to the staffing roles provided in *Attachment K: Table 1: Key Personnel.* Vendor must indicate the name of the proposed individual to perform each role. If an individual is not available a sample position description along with the Knowledge, Skills, and Abilities (KSAs) required for the position should be included

c) If the Vendor must provide additional Key Personnel for consideration, the following information must be provided:

   i) Role

   ii) Experience relevant to the services to be provided under this Contract

   iii) Certifications or credentials for the role suggested

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

Note: Additional provisions regarding Key Personnel can be found in the Department of Information Technology Terms and Conditions paragraph entitled *Personnel.*

Table 1: Key Personnel

Key Personnel Role	Duties and Responsibilities of the Role	Minimum Certifications or Credentials Preferred by NCDHHS
Account Manager	Serves as the point-person for management of the relationship Vendor maintains with the Department and manages all escalations from DHHS and MES Vendors.	Ten (10) years of experience managing large government accounts and contracts. Significant experience with stakeholder engagement and focused on customer experience.
Contract / Vendor Performance Manager	Serves as the point-person for all Contract management, Vendor performance management, and escalations. Provides MES Vendor Performance and SLA support to DHHS as defined throughout this RFP.	Ten (10) years of experience managing large service and contracts. Significant experience with stakeholder engagement and focused on customer experience.
Technical Architect / Lead	Leads all architecture, design, development, testing, and implementation work that is done to support system integrations across the MES. Interfaces heavily with business stakeholders, state IT Architects, and Engineers on all technology matters. This is the lead technical architect responsible for	Ten (10) years of experience leading large-scale technology initiatives with significant system integration and API design implementation experience.

Key Personnel Role	Duties and Responsibilities of the Role	Minimum Certifications or Credentials Preferred by NCDHHS
	resolving complex technology issues and providing strategic direction.	
Technical Program Manager / **Implementation Lead**	Serves as the technical manager, responsible for program level technology coordination across the MES environment and vendors. Develops and manages all related plans and schedules. This is the lead technical manager responsible for coordination and management of complex technology issues and enabling implementation of the technology strategy.	Ten (10) years of experience managing a similar program / portfolio of equal or greater scope.
Senior Project Manager / Operations Manager	Serves as the project manager, responsible for orchestrating activities that support both the MES Project in addition to Interoperability Operations and Maintenance. Responsible for coordination and management of complex project issues and enabling implementation of the project. These roles coordinate multi-vendor incident, change, release management. Interfaces with all technology deployments as the lead. Develops and manages all related project plans and schedules.	Ten (10) years of experience managing a similar project of equal or greater scope.
Senior Test Manager	Leads test activities including supervision of Vendor personnel. Leads test activities to include planning, execution, and reporting. Advises the State on test strategy and its relationship to other project activities.	Eight (8) plus years IT development / operations. Four (4) plus years IT test Two (2) plus years test automation; and Two (2) plus years management
Senior Test Engineer	Performs and provides technical leadership of test activities to include planning, execution, and reporting.	Eight (8) plus years IT development / operations. Four (4) plus years IT test Two (2) plus years test automation
IT Security Manager	Performs, Provides and Manages Privacy, Security, and Business Continuality Planning/Disaster Recovery (BCP/DR), Leadership, Oversight, and Coordination across MES and in coordination with DIT and our Single Sign-On vendor.	Five (5) plus years IT Privacy and Security; and five (5) plus BCP/DR

ATTACHMENT L: SERVICE LEVEL AGREEMENT (SLA) TERMS

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

NCDHHS has identified the following Service Level Agreements (SLA)s and Key Performance Indicators (KPI)s that will be monitored throughout the life of the contract. If a Vendor fails to meet a (any) defined KPI(s) for three (3) consecutive months, that State will have the option to replace a current SLA with the failing KPI. In the event a KPI is moved to an SLA, the State-selected SLA will become a KPI. A KPI that becomes an SLA will be assigned the compensation reduction percentage formerly assigned to the SLA it replaced.

The State and Vendor agree that failure to meet certain performance standards will result in a reduction in compensation as set forth in the table below. The State reserves the right to adjust the compensation reduction percentage in alignment with the 10% retainage cap (RC) of any of the SLAs with thirty (30) days' notice to the Vendor of changes in the percentage. The change will go into effect upon execution of Amendment.

The SLA damages assessed to a vendor will at no time exceed 10% of the monthly fees due per contract.

The Vendor must work with the State to drive the automation of all SLA validation, verification, and reporting.

Example:

> The monthly invoice is $1,000,000. The RC running total is 10%, $100,000. Vendor fails on one SLA metric that has a 3% compensation reduction for a total of $100,000 x 3% = $3,000 compensation reduction. In addition, a KPI has now failed three consecutive months. In the next month, the State has elected to change this KPI to an SLA, replacing a current SLA. The SLA being replaced had 3% compensation reduction which will be assigned to the former KPI, newly SLA. For avoidance of doubt, there is no compensation reduction for the failed KPI. Compensation reduction only occurs when an SLA fails to meet the assigned metric.

A. Service Level Agreements

SLA ID #	SLA Description	Metric	Category	Compensation Reduction
SLA 001	Vendor shall notify the Department of any Major or Emergency Deficiencies, as defined by the Agency, causing serious and or severe financial and or productivity impacts, causing serious disruption to Operations and Services, including Module Downtime, where there is no alternative or workaround, within one (1) hour of the initial Deficiency or within thirty (30) minutes of becoming aware of the issue, whichever is earlier. Vendor shall provide its plan for resolution within four (4) hours of the notification of the Deficiency to the Agency and resolve the Deficiency within twenty-four (24) hours of the notification of the Deficiency to the Agency.	Failure to Notify Agency and remediate deficiencies within the times and methods specified in the SLA, and as directed by the Agency	Deliverable	10% of monthly retainage for each failure within the notification and or resolution times described in the SLA and for each 24-hour period the issue continues without a cure
SLA 002	Vendor shall notify the Agency of any Moderate Deficiency, as defined by the Agency, it identifies that affects a small number of users, causes inconvenience, or delays business or prevents use of a fully supported Service, within 24 hours of becoming aware of the issue.	Failure to Comply	Deliverable	1% of monthly retainage for each occurrence.

SLA ID #	SLA Description	Metric	Category	Compensation Reduction
SLA 003	Online access to all system data, system logs, correspondence and system reports must be available to the State for one hundred eighty (180) days, with additional access to archived data within forty-eight (48) hours and at no additional cost to the state.	Failure to maintain at least one hundred and eighty (180) days of online log data	Compliance	1% of monthly retainage for each failure to maintain 180 days of log data and State access to Archived data within 48 hours
SLA 004	The Vendor must perform Disaster Recovery Testing at a minimum annually once to verify and validate the state-approved Business Continuity Plan and Disaster Recovery Plan and report the DR test results using the standard After Action Report Template provided by DHHS PSO	Failure to Comply 100% of the time	Disaster Recovery	10% of monthly retainage for each loss of data.
SLA 005	The Vendor shall report Security Breaches to the DHHS Privacy & Security Office and the Department Contract Administrator within one (1) hour.	Failure to comply as initiated by the timestamp of the reporting mechanism to the Contract Administrator of Any confirmed Security Breach	Security	10% of monthly retainage for each failure to report any Security Breach within 1hour.
SLA 006	If the Vendor is out of compliance with the Federal, State, and DHHS privacy & security policies, a mitigation plan to regain compliance is due to the Department within ten (10) State Business Days, with mitigation and testing to be completed in the timeframe defined in the mitigation plan.	Failure to Comply	Security	5% of monthly retainage for each occurrence.
SLA 007	Vendor will provide a monthly summary report that describes any notifications they have received regarding system problems, incidents, or defects. This report must be provided to the Department Contract Administrator on the first State business day of the month.	Failure to Comply	Performance	1% of monthly retainage for each occurrence.
SLA 008	Vendor shall document all Configuration items applicable to the Solution and update Documentation within 10 Business Days of the Implementation of a change.	All Solution's configuration components documented and or updated within ten (10) business days of the Implementation of a change	Deliverable	1% of monthly retainage for each missed occurrence.
SLA 009	Vendor shall request any planned Downtime due to scheduled upgrades or Maintenance, outside the normal Maintenance Window as agreed by the Agency, to the Agency five (5) Business Days prior to	Failure to Comply	Deliverable	5% of monthly retainage for Any failure to comply

SLA ID #	SLA Description	Metric	Category	Compensation Reduction
	Downtime. Unless the Agency consents, it does not qualify as approved Downtime.			
SLA 010	The Vendor shall perform patching and corrections to mitigate security vulnerabilities of a critical level risk within seven (7) State Business Days and those of a high-level risk within thirty (30) State Business Days. For a list of Vulnerability Risk Ratings, see section "SI-2-Flaw Remediation" in the System And Information Integrity Policy document at https://it.nc.gov/media/1210/download?attachment	Failure to comply	Security	5% of monthly retainage for each occurrence.
SLA 011	The Vendor must ensure that the solution is available for all NC users 24 hours a day, 7 days a week, 365 days a year, with a monthly availability of 99.95% uptime, excluding approved planned maintenance downtime. The solution is considered unavailable when any of the capabilities or integrations do not function as described in this RFP and subsequent documentation.	Availability must meet or exceed 99.95% over each Monthly audit period. The Agency equates this to less than 53 minutes of downtime per calendar year.	Availability	5% of annual retainage evaluated every month for noncompliance.
SLA 012	The Vendor must ensure that all test environments for the module, are fully available during scheduled testing. The module is considered unavailable when any of the capabilities do not function as described in this RFP and subsequent documentation.	Test environments availability must be 100% during scheduled testing.	Availability	1% of monthly retainage for each occurrence.
SLA 013	The Vendor shall provide the Corrective Action Plans (CAP) or Plan of Action Milestones (PO&AM) for mitigating the identified gaps in the internal risk assessments, third-party privacy & security assessments, or security audits to the DHHS Privacy & Security Office (PSO) within ten (10) State Business Days from the time the reports submitted to the Vendor.	Failure to Comply	Security	10% of monthly retainage for each failure to pass any Security Audit as identified in the SLA, 100% of the time, or Failure to provide a Corrective Action Plan to the DHHS Privacy & Security Office within 10 Business Days
SLA 014	The Vendor must provide and obtain Agency approval of a Corrective Action Plan (CAP) for audit failures. This approved CAP must include a schedule for resolution and must be submitted to the Agency Contract Administrator within five (5) business days of the audit failure.	CAP must be completed within five (5) business days of schedule.	Quality	1% of monthly retainage for failure to complete a CAP within five (5) business days of the scheduled completion date.
SLA 015	In the event of a Service disruption (incident), the Vendor must notify the Agency Contract Administrator in writing within sixty (60) minutes of confirming the	Notification must occur	Quality	1% of monthly retainage for each failure to notify the

SLA ID #	SLA Description	Metric	Category	Compensation Reduction
	occurrence. This notification must include the incident priority, date and time the service disruption started and, if resolved, when the disruption ended.	within sixty (60) minutes or less		Department in writing as required within 30 minutes of an incident resulting in Service disruption
SLA 016	The Vendor shall provide a written report and assessment to the Department Privacy & Security Office within twenty-four (24) hours following the identification of any Security Incident detailing all actions taken concerning the incident, including the type of incident, the current status, and any potential impact(s).	Failure to Comply	Security	5% of monthly retainage for each occurrence.
SLA 017	The Vendor must setup the alternate processing site and the procedures to restore essential services with a Recovery Time Objective (RTO) of eight (8) hours and a Recovery Point Objective (RPO) of eight (8) hours from the time a disaster is declared.	Failure to Comply	Disaster Recovery	5% of monthly retainage for each occurrence.
SLA 018	The Vendor shall respond in writing of potential compliance issues raised by Department staff, Department Vendors, and any other stakeholders, within forty-eight (48) hours from when the issue was first reported to the Vendor, to the Department Contract Administrator and the DHHS PSO.	Failure to Comply	Security	1% of monthly retainage for each occurrence.
SLA 019	The Vendor shall report all including suspicious privacy/security incidents involving unauthorized access, use, disclosure, modification, or data destruction to the DHHS Privacy and Security Office within twenty-four (24) hours after the incident is first discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare & Medicaid Services (CMS) data, the contractor shall report the incident within one (1) hour after the incident is first discovered.	Failure to Comply	Security	0.5% of monthly retainage for each failure within the notification periods identified in the SLA

B. Key Performance Indicators

KPI ID #	KPI Description	KPI Calculation	Category	Reporting Frequency
KPI 01	Vendor's Solution shall ensure Data received from real-time Interfaces will be accessible in the Module within three seconds at least 99.95% of the time; excluding batch interface updates. Performance is measured by a predefined sample measuring timestamp	Failure to comply Equals none or incomplete assurance that each Data Timestamp of Data received from real-time	Performance	Monthly

KPI ID #	KPI Description	KPI Calculation	Category	Reporting Frequency
	Data was received to the time the Data is available to query in the Module database or presented to the user via a Module user interface.	Interfaces, is accessible in the Module within >three seconds >99.95% of the time;		
KPI 02	Vendor shall have an acceptable documented risk mitigation plan submitted to the Department within 5 business days of risk identification for 100% of high or critical risks. The Department, after consulting with Vendor, will determine the level of criticality of each risk.	Failure to Comply Equals Once collaboration to determine Risk criticality has finalized its levels with the vendor, their Submission of an acceptable Risk Mitigation Plan for 100% of high and critical risks in >5 business days	Deliverable	Quarterly
KPI 03	Vendor shall work cooperatively with all other Vendors and offer timely support in integrating Solutions within the State's healthcare programs enterprise. Timely shall be defined as scheduling of a meeting within five (5) business days, the review of applicable documentation within five (5) business days and the scheduling of testing within five (5) business Days and ensuring the appropriate Vendor staff is participating. Days begin based on a request by the Department or another Vendor.	Failure to Comply **Equals** failure to offer timely support in integrating Solutions within the State's healthcare programs enterprise. Scheduling meetings >5 business days Scheduling Testing >5 business days Appropriate Vendor staff participating	Deliverable	Quarterly
KPI 04	From SLAs, number of issues/problems resolved within the approved timeframe (timeframes determined jointly by NCDHHS and Vendor).	Issue/problem resolution efficiency shall not fall below 95%	Performance	Monthly
KPI 05	From reports issues/problems and resolutions, number of complaints/problems effectively resolved versus number of complaints/problems not resolved but identified for each month (reported in monthly performance review meeting for prior month).	Complaints/problems resolution effectiveness shall not fall below 95%	Performance	Monthly
KPI 06	Service rating of Customer satisfaction based on perception of overall quality of delivered service (NCDHHS to conduct survey).	% of CSATs that overall satisfaction results are over 80%	Performance	Quarterly

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

State Contract Administrator for all contractual communication:

Name & Title	Donald Rowe, IT Contracts Administrator
Address 1: Physical Address	695 Palmer Drive Raleigh, NC 27603
Address 2 Mail Service Center Address	2015 Mail Service Center Raleigh, NC 27699
Email Address	Donald.Rowe@dhhs.nc.gov

State Technical Point of Contact:

Contact	NC Department of Health and Human Services Information Technology Division
Address 1: Physical Address	695 Palmer Drive Raleigh, NC 27603
Address 2 Mail Service Center Address	2015 Mail Service Center Raleigh, NC 27699
Telephone Number	(919) 855-3132
Attention:	Service Management Office

Invoices Submission electronically contact:

Contact	NC Department of Health and Human Services Information Technology Division
Address 1: Physical Address	695 Palmer Drive Raleigh, NC 27603
Address 2 Mail Service Center Address	2015 Mail Service Center Raleigh, NC 27699
Email Address	DHHSIT.CONTRACTS@dhhs.nc.gov
Attention:	IT Service Management Office

For the Vendor

Contract Administrator for all contractual communication:

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

Vendor’s Technology contact for technical matters:

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

ATTACHMENT N: DELIVERABLES AND MILESTONES SCHEDULE

The tables below lists the Deliverables to be provided by the Vendor for this project, along with the anticipated due date and frequency for each Deliverable. Deliverables submitted by the Vendor should follow industry standards, best practices, and the description provided. Upon submission of the Deliverable(s), the State will review that Deliverable and acceptance will be in accordance with the *Attachment B: Department of Information Technology Terms and Conditions Acceptance Criteria.*

1.0 DELIVERABLES

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-APP-013.01	Project Lifecycle	Release Management Plan	60 Days After Contract Award	When Changed	Describes activities associated with managing a software build through different stages, environments, testing stability and deployment.
DEL-B-PROJ-004.01	Project Lifecycle	Escrow Agreement	90 Days after Contract Award	Quarterly	This document describes the Escrow Agreement deliverable to the State within 90 days of State's acceptance of the contract. The Contractor will enter into an agreement with the State and an off-site storage vendor, to comply with the escrow agreement requirements. The Escrow Agreement will specify, among other things, that the Contractor will regularly deposit into escrow the specified source code, object code, and documentation required by the State. Further, the Contractor will make its initial deposit of Source Code within fifteen (15) days after the effective date of the Escrow Agreement.
DEL-B-PROJ-005.01	Project Lifecycle	Project Schedule	45 Days after Project Kick-off	Monthly	The Contractor shall provide a Project Schedule that describes the scheduled detailed activities and tasks necessary to provide contractually required services. This document is a work break down containing established dates, predecessors, successors, and dependencies with assigned resources for items needed to complete DDI, operations, and turnover activities and milestones. It reflects how and when a project's objectives are to be achieved by showing the major progress and milestones required on the project. The schedule will provide a minimum three-month projection for future DDI, operations, and turnover activities. Specific milestones are identified as those that: - Require NC DHHS acknowledgement or approval - Indicate completion of an activity that DHHS should know about or will enable DHHS to perform a related activity - Deliverables to which DHHS must review or approve

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Indicate start/end date of activities requiring DHHS performance
DEL-B-PROJ-006.01	Project Lifecycle	Joint DDI Communication Plan	60 Days after Project Kick-off	When Changed	This document will define the methodology for sharing project-specific communications among all project stakeholders during the DDI Phase. It will describe the processes to ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information. It 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 - Meeting protocol procedures–noting when minutes are taken, etc. - Stakeholder communications approach—to include interactions among the State and other Stakeholders - Incident reporting and escalation—to include reporting of security Incidents The State and Contractor will develop a mutually acceptable Joint DDI Communications Plan after Contract award. Updates/modifications to the Joint DDI Communication Plan, as mutually agreed, will occur as needed.
DEL-B-PROJ-010.01	Project Lifecycle	Project Management Plan	30 Days after Project Kick-off	When Changed	The Contractor shall develop and maintain a Project Management Plan (PMP): The purpose of the Project Management Plan is 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, NC DHHS, and federal policies, standards, guidelines, and procedures. Significant portions of the PMP are contained in other deliverables and the PMP references these documents rather than duplicating the information. This plan must align with the centralized Technical Program Management being conducted by the MES Systems Integrator.
DEL-B-PROJ-012.01	Project Lifecycle	Documentation Management Plan	120 Days After Contract Award	When Changed	Describes the process of organizing, storing, protecting and sharing documents.
DEL-B-PROJ-016.01	Project Lifecycle	Writing Style Guide	120 Days After Contract Award	Once	Set of standards for writing, formatting and designing of documents to provide uniformity across multiple documents.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-PROJ-018.01	Planning	Project Change Management Plan	60 Days After Contract Award	When Changed	The PCMP establishes the CM organization roles and responsibilities, policies, guidelines and procedures necessary for the Design, Development and Implementation of the solution. The plan should describe the business governance and operation of the Change Control Board (CCB) during the project phases of the solution. This plan must align with the centralized work being conducted by the MES Systems Integrator.
DEL-B-PROJ-019.01	Project Lifecycle	Implementation Plan	30 Days after Project Kick-off	When Changed	The Contractor shall provide an Implementation Plan that includes, but is not limited to: i. The identification and execution of any software customization and/or configuration ii. A high level project schedule mapping the proposed timeline of events iii. A project charter iv. A budget and adherence thereto v. A list of all assumptions, constraints, risks/issues, and risk/issue mitigation strategies with target resolution dates vi. All other milestones and deliverables along with the methodology and sequencing that will be needed for a successful implementation
DEL-B-SEC-013.01	Planning	Privacy & Security Incident Management Plan	30 Days from Project Start Date	Annually during O&M or Upon Changes	Organization established processes that: - 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 Incident Management Plan should follow https://it.nc.gov/documents/statewide-policies/scio-incident-response/download?attachment
DEL-B-APP-002.01	Design	System Architecture Plan	5 Days Prior to Development Phase	When Changed	The system architecture plan describes in sufficient detail the physical characteristics of the hardware, system software, and network components to build and integrate the architectural solution. It includes: - System Architecture Diagram which describes the overall system architecture - Security systems, data protection safeguards, and system access - Node and link definitions in terms of capacity, reliability, service capabilities and standards

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-APP-003.01	Design	Technical Design Document	5 Days Prior to Development Phase	When Changed	The Technical Design Document will provide a record of system architecture documentation that comprises the baseline configuration of the solution. This will include: - Account for all asynchronous processing and batch (background) versus interactive functions. - Identify all modules and objects that will be embedded in other modules or objects and not coded separately. - Modify the idealized design, as needed, to use or interface with existing software. - If additional constraints on the USI design are identified, modify the USI design accordingly. (Constraints may arise from hardware or software performance limitations or the capabilities of a COTS or client-supplied reusable system component.) - Document the design primarily in the form of work products that show the hierarchy of control among the modules that constitute the application software, the purpose of each module, and the data interfaces among them. A module (for example, a subroutine) is a single item (source file) to a compiler or assembler. For idealized and finalized designs, each module should represent an item that will contain less than 100 source instructions (excluding comment lines) when coded. Expand the current data dictionary to include definitions for all data interfaces shown in the architecture diagrams. - Sequence design diagrams to show a smooth top-down progression from the highest to the lowest level. Supplement each diagram with information that summarizes the illustrated function or data and that highlights important performance and design issues relevant to the diagram.
DEL-B-APP-005.01	Design	Application Performance Monitoring Plan	5 Days Prior to Development Phase	When Changed	The Application Performance Monitoring Plan describes what application performance objectives must be measured and precisely how these measurements will be conducted and reported upon. This plan will further describe the metrics for each measurement and what action must be taken if certain thresholds are exceeded.
DEL-B-APP-006.01	Design	Application Reliability Monitoring Plan	5 Days Prior to Development Phase	When Changed	The Application Reliability Monitoring Plan describes what application service level objectives must be measured and precisely how these measurements will be conducted and reported upon. This plan will further describe the metrics for each measurement and what action must be taken if certain thresholds are exceeded.
DEL-B-APP-008.01	Design	User System Interface Design	5 Days Prior to Development Phase	When Changed	Establish the user system interface (USI) structure for the application, including the central metaphor, menus, action bars, and important buttons or keys. The user system interface design will incorporate interface solutions for all stakeholders.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-APP-014.01	Design	Technical Architecture System Design (TASD)	90 Days After Contract Award	When Changed	Enables agencies to provide an increasing amount of detail to the Enterprise Technology Strategies (ETS) over the life of the project.
DEL-B-BUS-001.01	Design	Business System Design	5 Days Prior to Development Phase	When Changed	The Business System Design (BSD) document describes the business process design, application requirements and design to produce a picture of what the new business system functionality, how the new business processes will flow, and what the top-level application structure will be. The BSD document contains the following information: - Subsystem overview - Design Baseline − Business process scope − Organizational scope − Design assumptions and constraints − Business volumes and service levels - Business Process Model Summary − Business process hierarchy − Business process flows/work flow description − Event / Result definitions − Elementary business process descriptions/business rules − Business volumes − Input forms layout - Application Design and Approach − Top-level subsystem model − Subsystem design (diagram) − Subsystem module definition − Subsystem data − Subsystem Screens, Reports, and Interface layouts − Data rules and edits - Organization model − Role definition and mapping − Location definition and mapping
DEL-B-BUS-002.01	Design	Requirements Traceability Matrix	60 Days after Contract Award	When Changed	The requirements traceability matrix defines and traces relationships between the contract requirements (functional, operational, and performance) to the deliverables or artifacts generated and modified to meet those identified requirements. It will contain the following: - Requirement number and description - Definition of how the requirement will be satisfied - Physical mapping of the requirement to the specific artifact.
DEL-B-BUS-003.01	Design	Business Performance Monitoring Plan	10 Days Prior to Development Phase	When Changed	The Business Performance Monitoring Plan describes what business objectives must be measured and precisely how these measurements will be conducted and reported upon. This plan will further describe the metrics for each measurement and what action must be taken if certain thresholds are exceeded.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-CONV-001.01	Design	Data Conversion and Mitigation Plan	5 Days Prior to Development Phase	When Changed	The plan describes the processes that will be used to develop, execute, and maintain the Data Conversions and Migrations. The plan describes a comprehensive plan to convert and migrate all required data from the existing systems into the Contractor's solution. It includes strategies and activities required to support development, testing, certification, and long-term operations. The IMP will identify key events, accomplishments, and data criteria. The plan will document processes and activities to include analysis of the conversion and migration requirements; design and construction of solutions; testing of these solutions; identification of documentation required to support conversion and migration activities; and the processes that will actually be used to convert and migrate the data. The plan will clearly identify the data to be converted, the specific methods to be applied to these data (both automatic and manual), data cleansing and validation, data security, and the strategy to ensure that the data are converted and migrated in a timely fashion to support testing and implementation. Additionally, the plan describes the roles and responsibilities of the parties involved in these activities.
DEL-B-CONV-006.01	Design	Data Conversion Design	10 Days Prior to Development Phase	Each System Build	At the conclusion of the Data Conversion and Migration Planning phase, the Contractor will document the step-by-step process to convert source(s) to target(s) by subsystem. This will include documenting the mapping of each data source to the target data, documenting the outputs from each executed process (i.e. Input-Output Counts, Data Sampling Reports, Error Handling, etc.), and documenting the verification checkpoints within the process.
DEL-B-OPS-011.01	Design	Incident Management Plan	90 Days After Contract Award	When Changed	Describes the process used to respond to an unplanned event or service interruption and restore it to its operational state.
DEL-B-SYSINT-003.01	Design	Interface Control Document	10 Days Prior to Development Phase	When Changed	The Contractor will produce an Interface Control Document (ICD) in accordance with the State standard to fully describe integrations and interfaces into or out of the Contractor's solution. This document will be used to request State approval of the integration or interface prior to the start of this development work. ICD's must also be loaded into iServer as part of the Data Architecture.
DEL-B-SYSINT-004.01	Design	Systems Integration Plan	15 Days Prior to Development Phase	When Changed	The Contractor must work in coordination with the Department and Department Contractors to develop an Integration Plan that ensures integration and transitions are implemented.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-TEST-001.01	Design	Quality Management Plan	90 Days After Contract Award	When Changed	This document describes the processes to be applied for testing and quality assurance from software development and systems engineering methodology to the project to include test and quality assurance activities and results required for success. Key events and their objectives, along with roles, responsibilities, and resources needed for these events to be successful are listed in the plan. The MTQAP also provides detail to items in the IMP related to testing and quality assurance.
DEL-B-APP-001.01	Development	System Software (DDI)	5 Days Prior to Implementation	Each System Build	The software development information/data to be provided to the State relevant to each build will include, but not limited to the following: - Object Code - Source Code - Executables - Configuration Files Release Notes - Database Scripts - Shell Scripts - Demonstration Software - Demonstration Data - Release Notes - Configuration Files
DEL-B-APP-009.01	Development	Application Architecture	30 Days Prior to Implementation Phase	When Changed	Application Architecture: The Application Architecture will consist of several sections that collectively 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. - Application Functional Design – The Functional Design will describe the business flow of the application and must include examples for each associated use case. - Application Conceptual Design – The Conceptual Design is a pre-build document that describes the end-to-end solution in terms of software, services, platforms, etc. This document must show how each of the requirements are being met as related to the Functional Design. - Application Detailed Design – The Detailed Design is a post-build document that finalizes the Conceptual Design prior to operations. - Application Data Exchanges – Provides clear details that describe events, triggers, timings, initiators, protocols, synchronous/asynchronous characteristics and all other details that will be required for solutioning. - Application Maintenance Procedures – Documentation on what

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					maintenance is required to maintain the health and well-being of the application. This includes back-up, recovery, scheduled and unscheduled maintenance, etc. - Disaster Recovery Plan – Documentation on how disaster recovery (DR) requirements are met in the Application Design, how DR processes work, how DR processes can be tested and how data integrity and data consistency can be validated. - Software Inventory: Provides a comprehensive list of software that is used by the application along with license information, license renewal information and any associated agreements. - Service Inventory: Provides a comprehensive list of services that are used by the application along contract terms, contract renewal information and any associated agreements. - Security: Documentation of verified and allowed products and services along with specific security controls for the Application or any of the application components. Some of this information may be contained within other deliverables and can be included as attachments to the Application Architecture. All Enterprise Architecture documentation must be entered into the iServer tool or attached to the appropriate iServer record where applicable. The Contractor must work with the State for details.
DEL-B-DATA-001.01	Development	Data Architecture	10 Days Prior to Implementation	When Changed	The Data Architecture describes the Contractor's solution's data, how it is used, stored and transmitted. Data Governance: Defines the authority and control over the management of data assets. 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: Plans and defines 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 – Designing, implementing and maintaining the solutions to meet the data needs of an organization. - Data Operations Management – Planning, monitoring, control and support of structured and unstructured data assets across the data assets lifecycle. - Data Security Management – Planning, development, and

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					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 security analysis along with requirements for encryption during processing, transmission and storage. - Data Quality Management – Planning, implementation, and control activities that apply data quality management techniques to measure, assess, improve, and ensure the fitness of data for use. Data Dictionary: Defines information about data such as name, type, range of values, source, and authorization for access for each data element in the files and databases. Logical Data Model: Describes the data in as much detail as possible, without regard to how the data will be physically implemented. Features of a logical data model include: entities and relationships, attributes for each entity, primary and foreign keys. Physical Data Model (Optional): Represents how the Logical Data Model will be built. A Physical Data Model describes all table structures, including column names, column data types, column constraints, primary keys, foreign keys, and relationships. A Physical Data Model may be optional when acquiring SaaS based or complete turnkey solutions. Data Integration and Exchange and Interfaces: Describes specifically how data must be combined (integrated) or transformed (exchanged) in preparation for interfaces or other data sharing. Some of this information may be contained within other deliverables and can be included as attachments to the Application Architecture. All Enterprise Architecture documentation must be entered into the iServer tool or attached to the appropriate iServer record where applicable. The Contractor must work with the State for details.
DEL-B-INFRA-001.01	Development	Infrastructure Architecture	10 Days Prior to Implementation Phase	When Changed	The Infrastructure Architecture describes the hardware, platforms or infrastructure services used by the Contractor's solution. Infrastructure Diagram: Describes specifically how the communications flow between systems. The Infrastructure Diagram must include virtual and physical servers, data networks and other specialized devices such as Virtual Private Networks

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					and proxies that must be contemplated during system implementation or operation. Special consideration must be made for Infrastructure or Platform services (IaaS, PaaS) to ensure that enough of the logical implementation details are documented even though physical information may not be available. When documenting IaaS or PaaS services, it is important to specify geographic regions where services are hosted and to call out any points-of-failure that may be relevant to the application. Hosting Concept of Operations: Describes the high level functional architecture, organization, roles, responsibilities, processes, metrics and strategic plan for hosting and the use of hosting services. Security: Documentation of verified and allowed products, services and networks along with specific security controls for the infrastructure components as needed. Additional documentation on cryptographic requirements, governance and key management may also be required. Some of this information may be contained within other deliverables and can be included as attachments to the Application Architecture. All Enterprise Architecture documentation must be entered into the iServer tool or attached to the appropriate iServer record where applicable. The Contractor must work with the State for details.
DEL-B-PROJ-001.01	Development	Deployment/Rollout Plan	60 Days Prior to Implementation Phase	When Changed	The Contractor will develop, execute, and maintain the Deployment/Rollout Plan. This document will describe the detailed plan for implementing the solution (including any future integrations with other systems) It will include the processes and planning activities, roles and responsibilities, and schedule for all activities related to cut-over from the existing system to the Contractor's solution without impacting system processing. It will establish success criteria and provide for a post-implementation evaluation, including metrics for measurement of successful implementation and defines how release and deployment packages can be tracked, installed, tested, verified and/or uninstalled or backed out, if appropriate. Other considerations for inclusion are: - Communication of the plan - Disaster recovery and backup procedures

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Training manuals - System documentation - Back-out plan - Software support (help desk and break fix) - Monitoring system performance - Deployment transition
DEL-B-TEST-002.01	Development	Master Test Plan	30 Days Prior to Implementation Phase	Each System Build	The Master Test Plan Documents the overall testing approach and plan for each testing phase (Functional/Regression/Integration/Load and Stress/UAT/PST). The Master Test Plan will include at a minimum: - Definition and scope/out of scope of testing for all test phases - Assumptions/Risks/Dependencies - Data Strategy and Plan per phase - Defect Process - Environment and Code Configuration for each test phase - Automation and Manual testing and tools for each test phase - Entrance/Exit Criteria for each test phase - Management and testing team procedures/roles and responsibilities/testing procedures/reporting procedures/escalation procedures - Integration strategies – describes the integration build process and verification approach - Test design – defines the test scenarios in scope/out of scope per test phase
DEL-B-TRAIN-003.01	Development	Training Plan and Schedule	30 Days Prior to Implementation Phase	Annually or When Changed	This document describes the Contractors cohesive and responsive training to ensure that all users can be efficient and effective while using the system, including Contractors staff, State staff, and external users,. The plan reflects the relative lead-time for the development of training materials prior to conducting training classes (including the training of testing participants and all training before implementation); how users' skills will remain current throughout the operations phase; and how the Contractor will build and maintain the training environment. Additionally, it specifies the planned duration of implementation training rollout, including development of Desk Procedures (User Manual) for use in the Operations Phase. The plan specifies delivery media to be used for each training activity and the accessibility of training materials and/or training news before, during, and after training. It describes the process used to identify and track training needs and to evaluate trainee feedback to improve course materials and methods. The Training Plan will be updated annually to define the approach

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					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.
DEL-B-OPS-001.01	Implementation	Operational Change Management Plan	30 Days Prior to Go-Live	When Changed	The OCMP establishes the CM organization roles and responsibilities, policies, guidelines and procedures necessary for controlling and managing technical changes, and associated operations. The plan should describe the operation of the Technical Change Advisory Board (CAB) during the operations and maintenance of the solution. This plan must align with the centralized work being conducted by the MES Systems Integrator.
DEL-B-OPS-010.01	Implementation	Go-Live Readiness Assessment Form	5 Days Prior to Go-Live	Once	The Contractor will provide a formal assessment to conclude a go-live decision between the Business Owner, stakeholders and the vendors.
DEL-B-SEC-005.01	Implementation	System Security Plan (SSP)	60 Days Prior to UAT Testing	Annually during O&M or Upon Changes	State SSP Template https://it.nc.gov/documents/files/system-security-plan-template/open The SSP must address the following topics: - Adherence to the State's requirements outlined in the "Security and Privacy Controls Requirements" document, included in the Procurement Library; - Compliance with the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) to assess CIA and NIST SP 800-53 Rev 5 (Latest) at a "moderate" control level; - Data center physical security. - Network segmentation, access controls, and forensics; - Perimeter security; - Application security and data sensitivity classification, including Protected Health Information (PHI) and Personally Identifiable Information (PII); - Nd-point protections such as multiple redundant firewalls and host-based intrusion detection systems; - Identification and prevention of the use of prohibited functions, ports, protocols, and services; - Network, firewall, server and other security-related configurations and changes; - Intrusion detection and prevention; - Network scanning tools; - Host hardening; - Internet filtering; - Remote access; - Encryption of data at rest and in transit;

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- User authentication and directory services; - Interfaces and exchange of data with external entities; - System penetration testing; - Management of operating system and security patches; - Anti-Virus and malware detection and email gateways; - Assessment and testing of system and code modifications; and - Allowable internal and external communication protocols. - Compliance with the Federal Risk and Authorization Management Program (FedRAMP) Certification, FedRAMP Risk Assessment that indicates compliance or documented NIST 800-53 rev 5 (latest) at a “moderate” system risk assessment designation for Contractor hosted solutions; - Compliance with Statement on Standards for Attestation Engagements (SSAE-18) SOC 2 Type 2.
DEL-B-TEST-003.01	Implementation	Load Test and Performance Test Plan	30 Days Prior to Scheduled Testing	Each System Build	Load/Performance Testing will be conducted on an environment that ‘mirrors’ the configuration of the production environment at the time of implementation. The Load/Performance Testing will utilize automated test tools to simulate the production load in order to validate the stability, speed, scalability, responsiveness, and performance kpi’s (application output/processing speed/data transfer velocity/network bandwidth usage/maximum concurrent users/memory utilization/response times). The results of these tests will be captured and included as the Load/Performance Test Results. The Load/Performance Test Plan will outline the testing scope, environment and configuration, tools, schedule, and resources. The Load/Performance Test Plan will also outline any testing out of scope, associated assumptions and risks as well as any testing dependencies. Both the Load/Performance Testing Test Plan and Test Results will be reviewed and approved prior to the production go-live.
DEL-B-TEST-004.01	Implementation	UAT Test Results	5 Days after UAT Testing	Each System Build	The User Acceptance Test (UAT) provides the business users with the opportunity to test the system’s functionality. UAT Test Cases are typically based on a subset of the SIT Test cases, utilizing scrubbed production test data, and may include test case enhancements as requested by the business users. UAT testing may also include 'End to End' test cases with all other integrated modules/systems. The Contractor will assist the business users with the execution of their UAT. UAT test results are documented and submitted to the State for final approval.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
DEL-B-TEST-005.01	Implementation	Load Test and Performance Test Report	5 Days after Load and Performance Tests	For Each Test	The Production Simulation Test (PST) is the final set of tests executed during the Testing Phase. The objective is to install the developed software application system onto the target production system, prior to go-live, copy transactions from current production cycles, and compare the developed application test results against current production results. The Production environment is in place, including hardware and software, converted data, and the developed applications. The PST Test Plan is developed detailing test requirements, including identification of test data and cycles required. As Production Simulation Testing is underway, comparisons between current system and new system results will be made to determine the pass/fail rating of the Test Scenarios in accordance with the PST Test Plan. PST Test Results document will be prepared and submitted for State review.
DEL-B-TEST-007.01	Implementation	Test Summary Results Report	5 Days after the Associated Testing	Each System Build	For each test phase, the Contractor will develop a comprehensive Test Summary Result Report that describes all completed activities associated with conducting each test. The Test Summary Result Reports are used as ‘tollgates’/exit criteria to current test phase and entrance criteria to the next test phase. The Test Summary Results Report is also used in order to document the final test results of all QA activities for each test phase to ensure complete traceability to ensure there are no testing gaps. Each Test Summary Results report contains the following: - Overview of testing activities/Test Phase/Test Dates/Test Environment(configuration) -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) -Traceability Matrix mapping test cases to requirements proving no gaps in testing coverage
DEL-B-APP-011.01	Operations	System Software (Operations)	15 Days after Go-Live	When Changed	The software development information/data to be provided to the State relevant to each system change/update will include, but not limited to the following: - Object Code - Source Code - Executables - Configuration Files Release Notes - Database Scripts

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Shell Scripts - Demonstration Software - Demonstration Data - Release Notes - Configuration Files
DEL-B-OPS-002.01	Operations	Configuration Management Plan	10 Days Prior to Implementation Phase	Annually or When Changed	Configuration Management Plan describes the Contractors 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. The Configuration Management Plan specifies: - How the project 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) The Configuration Management Plan must align with the NC Medicaid centralized configuration management practice.
DEL-B-OPS-003.01	Operations	Operations Management Plan	60 Days Prior to Implementation	Annually or When Changed	The Operations Management Plan strategically describes how the Contractor will successfully deliver and support all operational services. Processes include software testing and system engineering, monitoring the system, producing printed and electronic output, and performing daily activities related to database administration, backup and restoration, contingency and disaster recovery testing, training, and problem prevention. The Plan will document Contractors approach to operations and communicate and understand of how we will operate the Contractors solution. Roles and responsibilities of the State and Contractor will be clearly delineated. The following areas will be included in the OMP, either by incorporating the topic in the document or referring to other stand-alone documents: - Strategic plan for operations - Process improvement - Quality management - Performance metrics - Operations management reviews - Change and configuration management - ITIL alignment reviews

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Risk and issue management plan - Resource management - Security plan - Disaster recovery/continuity of operations plan - Training plan - Communications process/procedure
DEL-B-OPS-004.01	Operations	Operations Communications Plan	60 Days Prior to Go-Live	Annually or When Changed	This document will define the methodology for communications with stakeholders during the Operations Phase. It will describe the processes to ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information. It must include, but is not limited to: - Information communications - Information communication requirements/needs - How, where, and when communications will occur - Who will provide/receive the communication - Meeting protocol procedures–noting when minutes are taken, etc. - To include interactions among the State, the Contractor, and other stakeholders - The Contractor's approach to provide awareness following Contract award; and the facilitation of ongoing project status communications - Incident reporting and escalation—to include reporting of security Incidents The State and the Contractor will develop a mutually acceptable Operations Communications Plan prior to start of Operations. Updates or modifications to the Operations Communication Plan, as mutually agreed, will occur as needed.
DEL-B-OPS-007.01	Operations	Annual Survey Results	1 Year after Go-Live	Annually	The Contractor will conduct an annual customer service survey that address the services selected by the State. The survey will, at a minimum, cover a representative sampling of end-users and senior management of the State and Providers as specified by the State. Timing, content, scope and method of the survey will be directed by the State. The Contractor will document the survey findings including a summary and analysis and analysis of the data in the Annual Survey Results Report.
DEL-B-OPS-012.01	Operations	Maintenance and Operations Manual / Guide	60 Days Prior to Go-Live	Annually or When Changed	Provides comprehensive details to run maintenance and operations smoothly (call center, performance reporting, support, etc.).
DEL-B-OPS-019.01	Operations	SLA Self Assessment Report - Operations Phase	30 Days after Go-Live	Monthly	The Contractor must minimally include the following in SLA self-assessment report: Contractor not meeting SLA, SLA number not

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					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
DEL-B-PROJ-002.01	Operations	Lessons Learned Final Report	90 Days after Go-Live	Once	The Contractor will record 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 DHHS. Lessons learned will be incorporated into the Contractors overall quality management process. Lessons learned will also be a key element of our approach to configuration/change management and process improvement.
DEL-B-PROJ-011.01	Operations	Staffing Resource Plan	120 Days after Contract Award	When Changed	The Contractor will prepare and submit a Staffing Resource Plan for the NC Medicaid program. The aim of the plan is to establish procedures and processes to ensure that the Contractor attracts, recruits, retains, and trains a qualified workforce to successfully design, maintain, and provide operations throughout the life-cycle of the contract. The plan will identify resource requirements, personnel identification and recruitment strategies, retention programs, diversity programs, position descriptions, roles and responsibilities of the human resources personnel, and personnel certification requirements.
DEL-B-SEC-003.01	Operations	Business Continuity Plan	90 Days Prior to Go-Live	Annually during O&M or Upon Change	This document describes the processes required to ensure the continuation of critical business processes and the information systems and services supporting them in the event of a disruption of the system itself, the loss of key personnel, and/or the loss of facilities housing operations. The plan and processes documented in this plan shall be consistent with those identified in State requirements and referenced documents. The Contractor's Business Continuity portion of the plan must include the following: - 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. - Procedures for activating any special teams for business continuity. - A plan for recovery of business functions, units, processes, human resources, and technology infrastructure.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					- Communication protocols and process for restoring operations in a timely manner.
DEL-B-SEC-004.01	Operations	Disaster Recovery Plan	90 Days Prior to Go-Live	Annually during O&M or Upon Change	The disaster recovery plan (DRP) contains detailed instructions on how the Contractor will respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events. The plan must contain strategies on minimizing the effects of a disaster, helping an organization to quickly resume key operations or continue to operate as if there was no disruption. The Contractor's Disaster Recovery portion of the plan must address, at a minimum: - 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.
DEL-B-SEC-006.01	Operations	Disaster Recovery and Business Continuity Testing with the After Action Report	No later than 90 Days after Go-Live	Annually during O&M or Upon Change	The Contractor shall conduct an annual test of the Disaster Recovery and Business Continuity Plan and submit the Disaster Recover/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Department.
DEL-B-SEC-007.01	Operations	Penetration Test Report	30 Days Prior to Implementation Phase	Annually during O&M or Upon Changes	The Contractor shall provide an independent third party to perform 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 shall be supplied to the Department and any major or critical vulnerabilities mitigated.
DEL-B-SEC-008.01	Operations	SOC2 TYPE 2 Report (Security Audit Reports)	After 6 months of Operations	Annually	The Contractor will provide a completed Security Audit Report with results to the Department by the 30th of September each year.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					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.
DEL-B-SEC-010.01	Operations	Privacy Impact Analysis	90 Days Before Go-Live	Annually during O&M or Upon Change	The Contractor shall support the State in developing a Privacy Impact Analysis for 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 - 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
DEL-B-SEC-011.01	Operations	Risk Assessments	90 Days Before Go-Live	Annually during O&M or Upon Change	Internal Risk assessments shall be completed on an annual basis and when additions or changes to functionality impact the security framework, architecture or when a new vulnerability exists.
DEL-B-SEC-016.01	Operations	Third Party Privacy & Security Assessment	60 Days before Go Live	Annually during O&M or Upon Change	The Contractor must provide, at the State's request, a Privacy and Security assessment in compliance with the latest NIST 800-53 requirements overlaid with the HIPAA privacy & security requirements and the penetration testing results. The State will accept either: 1) an assessment from a State contracted third party Vendor who will be provided access to the solution's infrastructure and systems to perform the required testing; or 2) Detailed HITRUST CSF Assessment Reports for the Contractor solution, (not a cloud service provider HITRUST CSF).
DEL-B-TURN-002.01	Operations	System Turnover Plan	60 Days after start of Implementation Phase	When Changed or Upon Request	This document describes the activities needed to ensure an uninterrupted and transparent turnover to a new Contractor at the completion of this Contract. This plan shall describe the activities that will be performed to ensure that required system and operational knowledge will be transferred to the new Contractor. This includes the conversion and migration of all pertinent

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					information and work in progress, leases, etc. Additionally, the plan shall discuss roles and responsibilities of the organizations and the workflow between the current Contractor and the new Contractor. High-level timelines and contingency plans should be included.

2.0 MILESTONES

The vendor must provide a detailed approach for implementing the Interoperability and Patient Access solution, as well as a high-level timeline and list of key milestones required during the DDI phase of the project.

Following the award of the contract, the State will collaborate with the Vendor to finalize the timeline and key milestones.

ATTACHMENT O: BUSINESS CONTINUITY PLAN

Vendor shall provide, in Vendor's response to this RFP, a narrative describing Vendor's approach to business continuity and disaster recovery, 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. Sever OS;
   b. Server Location; and
   c. IP Address.

4. Failover Site Information

   a. Server(s) Name;
   b. Server Type;
   c. Sever 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; and
      v. Customer Recovery Procedures.
      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

G.S. 133-32:
http://www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=133-32
Executive Order No. 24 (Perdue, Gov., Oct. 1, 2009):
https://ethics.nc.gov/media/242/download?attachment
G.S. 105-164.8(b):
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_105/GS_105-164.8.pdf
G.S. 143-48.5:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-48.5.html
G.S. 143-59.1:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.1.pdf
G.S. 143-59.2:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/PDF/BySection/Chapter_143/GS_143-59.2.pdf
G.S. 143-133.3:
http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_143/GS_143-133.3.html
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 <u>ONE</u> 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 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 Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended

(42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (h) the Food Stamp Act and USDA policy, which prohibit discrimination on the basis of religion and political beliefs; and (i) the requirements of any other nondiscrimination statutes which may apply to this Agreement.

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. loan insurance

2.Status of Federal Action:

a. Bid/offer/application
b. Initial Award
c. Post-Award

3.Report Type:

a. initial filing
b. material change
For Material Change Only:

Year___________

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

12. Form of Payment (*check all that apply*):

a. cash
b. In-kind; specify:

Nature_____________________________
Value ______________________

13. Type of Payment (*check all that apply*):

a. retainer
b. one-time fee
c. commission
d. contingent fee
e. deferred
f. other; specify:

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

The MS Word template for *Attachment S: Business Associate Agreement* may be requested by contacting Contract Specialist.

NORTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES
BUSINESS ASSOCIATE AGREEMENT

This Agreement is made effective the _____of ___________, 20___, by and between the North Carolina Department of Health and Human Services ("Covered Entity") and _____________________________________ ("Business Associate") (collectively the "Parties").

1. BACKGROUND

a. Covered Entity and Business Associate are parties to a Contract entitled ______________________, 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 ("Department" or "Agency") that has been designated in whole or in part by the Department as a healthcare 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 Addendum 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 heath 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" 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. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. § Part 160 and Part 164.
e. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
f. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
g. "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.
h. 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 Protected Health Information 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. § 164 with respect to electronic protected health information, to prevent use or disclosure of the Protected Health Information 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 Protected Health Information by Business Associate in violation of the requirements of this Agreement.

d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware, including breaches of unsecured protected health information as required by 45 C.F.R. § 164.410.

e. 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 protected health information on behalf of Business Associate agree to the same restrictions and conditions that apply to Business Associate with respect to such information.

f. Business Associate agrees to make available protected health information as necessary to satisfy Covered Entity’s obligations in accordance with 45 C.F.R. § 164.524.

g. Business Associate agrees to make available Protected Health Information for amendment and incorporate any amendment(s) to Protected Health Information in accordance with 45 C.F.R. § 164.526.

h. Unless otherwise prohibited by law, Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, 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.

i. Business Associate agrees to make available the information required to provide an accounting of disclosures of Protected Health Information 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 Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Contract, provided that such use or disclosure:

   i) would not violate the Privacy Rule if done by Covered Entity; or

   ii) 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 Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that:

   i) The disclosures are Required by Law; or

   ii) 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 Protected Health Information 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 may not use or disclose Protected Health Information if the use or disclosure would violate any term of the Contract or other applicable law or agreements.

5. TERM AND TERMINATION

a. Term. The Term shall begin on the Effective Date stated above and shall continue until the Contract expires or is terminated.

b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, at its option:

i) 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;

ii) Immediately terminate this Agreement and services provided by Business Associate, to the extent permissible by law; or

iii) If neither termination nor cure is feasible, report the violation to the Secretary as provided in the Privacy Rule.

c. Effect of Termination.

i) 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 Protected Health Information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

ii) If Business Associate determines that returning or destroying the Protected Health Information is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction not feasible. Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

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. If 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.

______________________________	______________________________
Signature of Authorized Representative	Name of Entity
______________________________	______________________________
Name and Title	Date

ATTACHMENT T: TECHNICAL / MANAGEMENT PROPOSAL

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

The Vendor will provide an attestation statement agreeing to meet all Requirements in the tables provided in Section 3.5.1. If any of these Requirements cannot be met, the State will disqualify the Vendor from further evaluation. Post award, failure to comply with any requirement constitutes a material breach of the contract and will result in immediate termination of the contract.

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

RFP Section	Area	Page Limitation
Section 3.1.1	Scope of Work: Implementation of Patient Access API	15
Section 3.1.2	Scope of Work: Implementation of Provider Directory API	15
Section 3.1.3	Scope of Work: Implementation of Payer-To-Payer Data Exchange API	15
Section 3.1.4	Scope of Work: System Integration Platform Integration	10
Section 3.1.5	Scope of Work: Identity Management	5
Section 3.1.6	Scope of Work: Consent Management Solution	5
Section 3.1.7	Scope of Work: Extraction, Translation, and Load Services	5
Section 3.1.8	Scope of Work: Migration Activities	5
Section 3.1.9	Scope of Work: Ongoing Operations and Maintenance	5
Section 3.2.3	General Requirements and Specifications: Site and System Preparation	5
Section 3.2.4	General Requirements and Specifications: Equivalent Items	2
Section 3.2.5	General Requirements and Specifications: Enterprise Licensing	2
Section 3.4.1	Enterprise Specifications: Enterprise Strategies, Services, And Standards	5
Section 3.4.2	Enterprise Specifications: Architecture Diagrams Defined	10
Section 3.4.4	Enterprise Specifications: Identity, Credential, and Access Management	5
Section 3.4.5	Enterprise Specifications: Cloud Service Providers	5
Section 7.1	Vendor Utilization of Workers Outside the U.S.	2
Section 7.4	Vendor’s License or Support Agreements	10
Section 7.6	Disclosure of Litigation	2
Section 7.14.3	MITA 3.0 Framework and Technical Architecture Seven Standards and Conditions	2

Vendor to provide a response for all Specifications in the tables provided in Section 3.6.1 and Table 27 in Section 3.7 for the Provider Directory API Option. Each Specification must have a response provided in a format with a header to include two columns: a) the Specification number as provided in the RFP, and b) the Specification Description as provided in the RFP, and then an area following the header that contains the narrative response to the Specification. The narrative can contain diagrams, process flows, exhibits, examples, sketches, relevant descriptive literature, or other information to demonstrate how the Vendor's solution(s) will address each Specification.

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

RFP Section	Area	Page Limitation
Section 3.6.1: Table15	Interoperability	n/a
Section 3.6.1: Table16	Patient Access API	n/a
Section 3.6.1: Table17	Payer to Payer API	n/a
Section 3.6.1: Table18	Consent Management	n/a
Section 3.6.1: Table19	Interface	n/a
Section 3.6.1: Table20	Operations and Maintenance	n/a
Section 3.6.1: Table21	Security and Risk Management	n/a
Section 3.6.1: Table22	Testing	n/a
Section 3.6.1: Table23	Transition	n/a
Section 3.6.1: Table24	Diversity, Equity, and Inclusion	n/a
Section 3.6.1: Table25	Training	n/a

The following section will not be considered for evaluation purposes

RFP Section	Area	Page Limitation
Section 3.7: Table27	Provider Directory API – Option	n/a

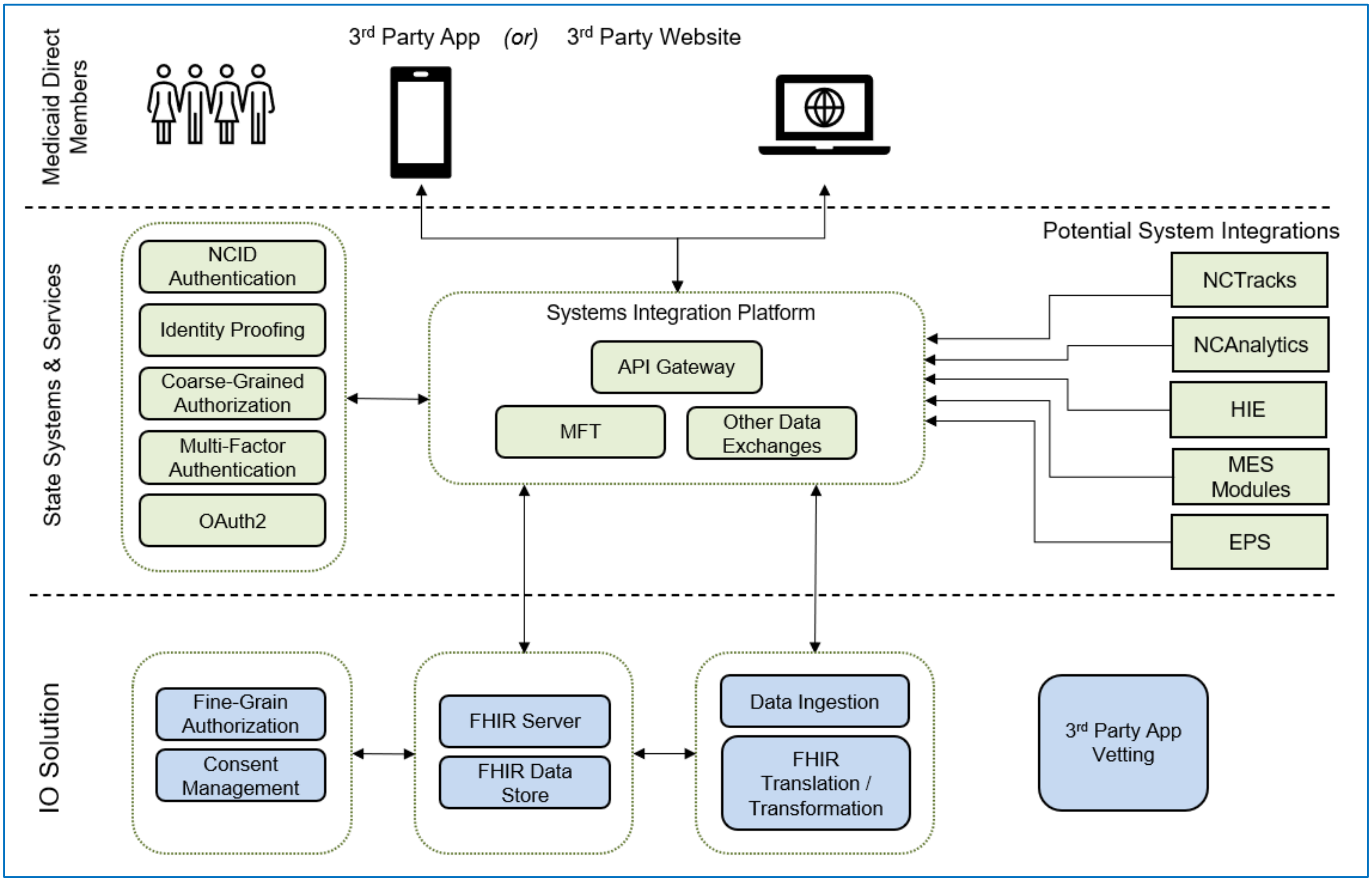
Vendor to provide a narrative of the Vendor's approach to managing the project phases including 1) Pre-Go Live, Implementation Phase and 2) Post-Go Live, Steady State Phase in the section areas listed below. Each response may be in the form of a narrative, disclosure, attachment, or other documentation.

RFP Section	Area	Page Limitation
Section 7.11	Project Management	2
Section 7.12	Meetings	2
Section 7.14.2	Change Management Process	5
Section 7.14.4	Performance Management	5

ATTACHMENT U: CONCEPTUAL ARCHITECTURAL DIAGRAMS

The following figures show conceptual architectural diagrams relating to the future state of the APIs contained within the Interoperability Solution.

Figure 1: Future State – Conceptual Architectural Diagram



Disclaimer: These future state diagrams are subject to changes made by NCDHHS.

ATTACHMENT V: SYSTEM INTEGRATION PLATFORM CORE CAPABILITIES

Introduction

The North Carolina DHS is in the process of implementing a System Integration Platform (SIP) that will provide all the current and future module vendors with a common infrastructure to communicate and integrate using a consistent standards-based approach.

The SIP is being 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 some of these core services:

Core SIP Services

1. Application Program Interface (API) Management

The SIP 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 SIP 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 SIP. The SIP will use the **API Management Portal** to design, secure, publish, monitor, manage, and deploy interfaces across multiple vendor cloud environments. Using the portal, the SIP 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 SIP 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	SIP API Gateway	SIP 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	SIP API Gateway	SIP 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	SIP Service APIs	These are APIs that provide access to the SIP 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 SIP platform **recommends the use of API first style-based integration approach** for module interactions and integration points. The SIP 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 SIP also **supports Simple Object Access Protocol (SOAP)-based web services** and other integration approaches like **message queues**. The SIP 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 SIP preferred and recommended style is to use Representational State Transfer (REST)-based APIs for integration.

2. Messaging

The SIP platform provides capabilities such as queue-based messaging and publish/subscribe message services for integration between modules. The reliable messaging capability enables the SIP with fast, reliable, low-latency messaging, guaranteed delivery, and integration solutions based on proven messaging patterns. The SIP platform uses the Red Hat AMQ as the basis to provide reliable messaging between MES modules. The SIP Platform provides support for open standards including Java Message Service (JMS) 1.1 and 2.0, Transmission Control Protocol (TCP), Secure Sockets Layer (SSL) and Advanced Message Queueing Protocol (AMQP) 1.0.

3. Managed File Transfer

The SIP 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 SIP published APIs (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 SIP 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.

4. ICAM

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

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	SIP ICAM Solution	• Act as a Service Provider(SP) to NCID • Act as an Identity Provider (IdP) to the module vendor • Users registered in the NCID system will be then provisioned in the SIP ICAM infrastructure
3	Module Vendor	• Act as a Service Provider (SP) to SIP ICAM

The ICAM solution works in tandem with NCID to offer the Authentication and Authorization service in the SIP platform. ICAM will rely on NCID (acting as an IDP) for authenticating the end users before proceeding with coarse authorization and granting access to the target MES modules. The table below outlines the responsibility distribution between the module vendor and the SIP ICAM as it pertains to authorization.

S No.	System	Authorization Role
1	SIP ICAM	The SIP ICAM only provides coarse grained authorization which is limited to whether a registered user has access to an application or module or not
2	Module Vendor	Module vendor will be responsible for fine grained authorization and access preferably using role-based access control (RBAC) in their respective module

5. Enterprise Content Management

The SIP provides a cloud-based content management platform to provide a central repository for enterprise content management (ECM). It provides document collaboration and management, lightweight document workflow automation, business process enablement, and platform APIs for customizations. The ECM stores unstructured data in the form of hard copy scanned documents, reports outputs, and other documents of varying file formats received or created by MES modules.

The ECM solution offers a complete set of capabilities including document workflow, metadata management, and content collaboration capabilities. All documents stored in the ECM module get tagged with a unique identifier, date, and timestamp for tracking and easy recall.

The following table identifies some of the core APIs available to interact with the Enterprise Content Management System:

ECM Service API	Purpose	Module Vendor Interaction
Submit and Upload Document	The ability to submit and upload a document(s)	Module vendor may invoke this service API whenever they need to store documents, attachments to support their business operations
Search Document	The ability to search for a document in the content repository	Module vendor may invoke this service API whenever they need to look up a document
Retrieve Document	The ability to retrieve the document and view its content	Module vendor may invoke this service API to retrieve a specific document from the repository

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

The SIP provides a unified web-based operations portal to allow for performing various operations including request, monitor, configure, control and report on each of the SIP platform services. The SIP operations platform serves as a single pane of glass for the UI based access to the SIP Platform Services. The operations portal will **provide a module specific view** of all relevant transactions flowing through the SIP platform.

The SIP platform will provide the infrastructure to support centralized ITSM capabilities in the following business areas:

- Change Management
- Incident Management
- Problem Management
- Configuration Management

a. Change Management

All State initiated change(s) or changes that impact Medicaid production operations will be centrally tracked in the central change management infrastructure. All module vendors will be required to use this infrastructure 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 centralized system for review and to manage communication and escalation to the appropriate module vendor partner for resolution.

c. Problem Management

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

d. Configuration Management

The centralized Configuration Management (CM) is geared to track configuration items that are critical to support the integrated MES Enterprise operations. For every module these configuration items will be managed in this central repository.

7. **Defect Tracking**

The SIP platform will provide the capability to support a centralized defect tracking solution. 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 central system for module-to-module integration testing and User acceptance testing for modules.

8. **Test Management**

The SIP platform will provide a test management infrastructure and service to support centralized test management across all MES modules and the System Integration Platform. This service will allow DHHS to monitor and report on testing progress. The module vendors will be required to provide data to the centralized test management system to support consolidated reporting including generation of key metrics and reporting progress.

9. Centralized EDI Gateway Capabilities

The system integration platform provides a comprehensive EDI gateway solution with support for all HIPAA transactions and compliance requirements. The platform provides support for all HIPAA X12 transactions and provides out of the box Strategic National Implementation Process (SNIP) level edits (1-6). The platform also provides EDI to non-EDI And non-EDI to EDI data mapping and processing capability. The module vendors will be required to centralized EDI gateway for trading partner management and EDI processing capabilities. The SIP platform provides the feature to implement pass through capabilities if required to support deeply integrated EDI processing capabilities in a module.

ATTACHMENT W: WORK PRODUCTS

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

1.0 WORK PRODUCTS

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-OPS-009.01	Project Lifecycle	Defect Tracking	10 Days After Contract Award	Throughout DDI and O&M	The Contractor will work with the States Systems Integrator to track all Defects using the provided tools. This is in addition to any Defect Management functions that the Contractor may typically operate.
WP-B-OPS-013.01	Project Lifecycle	Risk and Issue Tracking	10 Days After Contract Award	Throughout DDI and O&M	The Contractor will work with the States Systems Integrator to track all Risks and Issues using the provided tools.
WP-B-OPS-018.01	Project Lifecycle	SLA Self-Assessment Report - Project Phase	60 Days After Contract Award	Monthly	The Contractor must minimally include the following in SLA self-assessment report: Contractor not meeting SLA, SLA number not being met, Evidence used for determination, Date SLA became out of compliance, Resolution Process (if known), Planned Resolution Date (if known), Criticality Level, Escalation Required (Y/N), Corrective Action
WP-B-PROJ-007.01	Project Lifecycle	Project Status Meeting Agenda	10 Days after Project Kick-off	Monthly	The Project Status Meeting Agenda is designed to provide a listing of discussion topics for the Monthly Status Meeting attended by NC DHHS and Contractor. At a minimum, the Agenda will include the following topics that is also required in the project status report among others: - Overall project status/health by phases/major functions in progress - Progress summary information - Project timeline - Risks and Issues - Potential scope changes - Staffing, changes - Sub-contractor status - Project metrics - Open action items
WP-B-PROJ-008.01	Project Lifecycle	Project Status Meeting Minutes	2 Days after Project Status Meeting	Monthly	The Project Status Meeting Minutes will provide a detailed summary of items discussed during the initial contract meeting between NC DHHS personnel and Contractor. The purpose of the Project Status Meeting is to discuss program progress, escalate issues, evaluate performance, review additional program requirements, and discuss other management topics as identified

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					by program management. The Minutes may provide a summary of the following topics among others: - Date, Meeting location, Meeting start time - Name of individual chairing the Meeting and meeting attendees - Report on motion to approve previous Meeting's published Minutes - Summary of general announcements - Summary of meeting discussion and action item outcomes, by item - Announcement of Date, time, and location of next scheduled Meeting - Time of meeting adjournment
WP-B-PROJ-009.01	Project Lifecycle	Project Status Report	30 Days after Project Kick-off	Monthly	The Project Status Report communicates a concise management view of progress made to the mutually agreed project plan provided at a minimum weekly (or on an agreed upon cadence with DHHS). At a minimum, this report provides the following information: - Overall project status/health by phases/major functions in progress - Accomplishments in the current reporting period, planned activities for the next two reporting periods - Project timeline, earned value metrics with explanation of performance status, variances, corrective action plans, estimated cost to complete remaining work, and estimated cost at completion of work - Active risks, mitigation plans and activities - Major project issues that require NC DHHS attention and resolution - Potential scope changes - Staffing changes - Sub-contractor status, if applicable - Project metrics (i.e., cost and schedule performance, measurement of performance, etc.), trend analysis (i.e., KPIs against targets) - Action items status The information generated and provided must be timely and reliable
WP-B-PROJ-013.01	Planning	Vendor Kickoff Presentation	30 Days After Contract Award	Once	The Contractor will work jointly with DHHS to develop, design and present the kickoff presentation that will provide a clear overview of the project implementation plan which marks the start of vendor onboarding.
WP-B-PROJ-014.01	Project Lifecycle	Weekly Status Report	10 Days After Internal Project Kickoff	Weekly	Summarizes project team accomplishments, planned work, actual statuses and trends for key performance indicators against targets.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-PROJ-015.01	Project Lifecycle	Meeting Agendas	48 hours prior to Scheduled Meeting	Each Meeting	Provides a listing of discussion topics for the meeting attended by NC DHHS and Contractor.
WP-B-PROJ-017.01	Project Lifecycle	Meeting Minutes	48 hours after Scheduled Meeting	Each Meeting	Provides a detailed summary of items discussed during the meeting between NC DHHS personnel and Contractor.
WP-B-TEST-006.01	Project Lifecycle	Test Cases / Scripts / Results	15 Days Prior to Scheduled Testing	As Needed	Test Cases provide detailed test steps to be performed on a system to validate it operates as expected as well as the expected results. Actual Test Results will match the documented expected results in order to pass. All Test Results will be captured and stored with each test case.
WP-B-APP-004.01	Design	Business Process Model	5 Days Prior to Development Phase	When Changed	The Contractor will work with the State to ensure that Business Process Models are maintained to accurately reflect the processes supported by the Contractor's solution. Upon State request, the Contractor will update and maintain the Business Process Models along with the business process information stored within the iServer tool.
WP-B-SEC-001.01	Design	Application Security Model - Roles	10 Days Prior to Development Phase	When Changed	The Application Security Model defines the roles required at the subsystem level and describes the type of security access needed. An application CRUD (Create/Read/Update/Delete) matrix will be generated to show what access is provided to each role. This model will include: - Organizations impacted - Complete list of application roles and definitions - Role mapping to subsystem - Must include administrator security For each function: - Role to application CRUD Matrix - Role definitions - Data context parameters and role restrictions - Rules for segregation of duties - Role access rights
WP-B-SEC-002.01	Design	Security Management / Monitoring Plan	45 Days After Contract Award	When Changed	Continuous, automatic security monitoring of cyber threats, security misconfigurations and other vulnerabilities.
WP-B-SYSINT-002.01	Design	Integration Specifications	10 Days Prior to Development Phase	When Changed	The Contractor will document integration specifications in accordance with the State standard to fully describe the data elements, data format and selection criteria that will be used for each integration or interface. Integration specifications must also be loaded into iServer as part of the Data Architecture.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-APP-007.01	Development	Enterprise Architecture Documentation	10 Days Prior to Implementation Phase	When Changed	Enterprise Architecture Documentation will contain data and information regarding the total solution to include each subsystem. The Enterprise Architecture includes data and information related to the: Application Architecture, Data Architecture, Infrastructure Architecture, Security Architecture, Performance Architecture and Business Architecture as defined within the Federal Enterprise Architecture Framework. This data and information will be provided through input into the MES EA repository along with artifacts that are in alignment with MITA and the MES EA standards.
WP-B-APP-010.01	Development	IT Inventory/Configuration	10 Days Prior to Implementation Phase	When Changed	IT Inventory and Configuration information related to the system will be maintained in the States EA repository, CMDB and other systems of record.
WP-B-DATA-002.01	Development	Data Element Dictionary	10 Days Prior to Implementation Phase	When Changed	The Data Element Dictionary defines information about data such as name, type, range of values, source, and authorization for access for each data element in the files and databases. The Contractor must create and maintain the Data Element Dictionary in accordance with State standards.
WP-B-SYSINT-001.01	Development	Data Integration and Interface Documentation	10 Days Prior to Implementation Phase	When Changed	The Contractor will create and maintain an inventory of internal and external interfaces and full specifications with related information throughout DDI and the life of the contract. Team will work with all holders of external databases to create prototype databases for testing the transfer of data to ensure 100 percent success upon implementation.
WP-B-CONV-002.01	Implementation	Data Conversion Test Run Results	5 Days after Data Conversion Test Runs	Each System Build	Converted data will be reviewed during a separate test initiative to validate the converted data for each build. Reviewing the conversion results of selected converted file records or database rows will also be used as a part of data conversion testing to ensure that the data conversion process executed as documented and planned for in the Data Conversion Design document. Randomly selected converted file records or database rows will be chosen for a field-by-field examination to ensure that the conversion results were as expected. This data validation process will verify the expected conversion results were achieved. Balancing reports (results) for account for all input data being transformed into output data will also be produced and anomalies investigated and resolved. Data which fails the conversion process will be reported on in exception reports. Conversion strategies for dispositioning exception data will be developed and included in the conversion process.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-CONV-003.01	Implementation	Data Conversion Test Runs	5 Days After Start of Implementation	When Changed	The data conversion mock runs simulate the execution to convert production data required for the deployment of the application. Each Test Run focuses on performance and refining the schedule to convert the data in the shortest timeframe possible. The deliverable to NC DHHS for all Test Runs will be the target database and a predefined set of reports generated from the execution of the converted processes. NC DHHS will have access to the database to allow them to run “ad hoc” queries against the data. These reports will contain DHHS accepted data conversion technical design documents to reference conversion mapping rules.
WP-B-CONV-004.01	Implementation	Final Data Conversion Run (Production)	1 Day Prior to Go-Live	When Changed	The Final Data Conversion Run for Production will be used to validate that identified data has been successfully converted, using specified methods to these data (both automatic and manual), data cleansing and validation, data security, and the strategy to ensure that the data are converted and migrated as outlined in the Data Conversion and Migration Plan.
WP-B-CONV-005.01	Implementation	Final Data Conversion Run (UAT/PST)	5 Days Prior to UAT Testing	When Changed	The Final Data Conversion Run for UAT/PST will be used to validate that identified data has been successfully converted, using specified methods to these data (both automatic and manual), data cleansing and validation, data security, and the strategy to ensure that the data are converted and migrated as outlined in the Data Conversion and Migration Plan.
WP-B-OPS-014.01	Implementation	User Manuals / Online Help	90 Days Before Go-Live	When Changed	Procedural or reference information delivered through computer software to present information on a broad range of topics or subjects.
WP-B-SEC-015.01	Implementation	Vulnerability Management Reports	30 Days Before Go-Live	Monthly during O&M	Report of all servers and systems patched proactively/timely to mitigate the vulnerabilities. Report of the application components security scanning reports for identifying OWASP TOP 10 vulnerabilities
WP-B-TRAIN-001.01	Implementation	Desk Procedures	30 Days before Scheduled Training	When Changed	The Contractor will develop a Desk Procedure to ensure that all users can be efficient and effective while using the system, including the Contractor's staff, State staff, and external users. The training plan will reflect the relative lead-time for the development of desk procedures 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 Contractor will build and maintain the training environment. Additionally, it must specify the planned duration of the implementation training rollout during the Operations Phase.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					The Contractor will conduct surveys and monitor training effectiveness among all user groups and prepare corrective action(s) for process improvement where indicated. All findings, corrective actions, and recommendations will be documented in the Training Evaluation report.
WP-B-TRAIN-002.01	Implementation	Training Evaluation Report	5 Days after Associated Training	When Changed	The Contractor will develop a training evaluation report that details 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 Contractor 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 Contractor will document any training gaps, lessons learned, and opportunities for improvement in the evaluation report
WP-B-TRAIN-004.01	Implementation	Training Components (Media)	30 Days Prior to Scheduled Training	When Changed	The Contractor will provide dedicated training specialists who will provide input to the development of training materials such as CBT courses that will be available to these audiences in conjunction with instructor-led training courses in a location in accordance program requirements. The Contractor shall produce State-approved initial and ongoing updates to training materials and secure, browser-based, Web-enabled tutorials in the content, frequency, format, and all media as directed by the State. The Contractor will 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 or exceed the established goals. The methods will include self-help tools such as CBT courses as well as instructor-led training courses to provide hands-on experience to users of the replacement system. The goal will be to insure efficient and effective use of the new system.
WP-B-APP-012.01	Operations	Program Performance Monitoring and Report	30 Days after Go-Live	Monthly	The purpose of this report is to document the overall performance health of the Contractor solution. The document outlines those performance areas that are monitored to pre-established standards. The aim of the document is to communicate project goals to all management levels and monitor the solution

Number	Phase / Stage	Title	First Version Due	Frequency	Description
					performance against those goals and alert management to approaching potential performance issues before they occur. Although performance will be monitored daily through using electronic tools and reported to the Department, summaries of project management scorecards and dashboards, and corrective actions taken in response to performance flagged as below standard during the month will be captured in this document. Specific topic monitored among others include: - Project technical metrics, analysis of trends, and corrective action plans - Significant technical progress/problems during the preceding period - Actual accomplishments in current reporting period - Planned accomplishments for the next reporting period - Issues requiring resolution - Status of all assigned action items - Current project risks and risk mitigation plans and activities - Contract status
WP-B-OPS-005.01	Operations	Monthly Operations Meeting Minutes	30 Days after Go-Live	Monthly	Monthly Operations Meeting Minutes will provide a detailed summary of items discussed during the Monthly Operations Meetings. The purpose of the Monthly Operations Meetings are to discuss program progress, escalate issues, evaluate performance, review additional program requirements, and discuss other management topics as identified by program management. The Minutes may provide a summary of the following topics among others: - Date, Meeting location, Meeting start time - Name of individual chairing the Meeting and meeting attendees - Report on motion to approve previous Meeting’s published Minutes - Summary of general announcements - Summary of meeting discussion and action item outcomes, by item - Announcement of Date, time, and location of next scheduled Meeting - Time of meeting adjournment
WP-B-OPS-006.01	Operations	Operations Reports	30 Days after Go-Live	Monthly	The Operations Reports documents the Contractor's operations achievements compared to planned activities where appropriate for the reporting period. The Operations Report does not include program management data contained in the overall PMO monthly report such as quality assurance, staffing, and EVMS.

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-OPS-015.01	Operations	System Backup Report	30 Days after Go-Live	Monthly	The Contractor must provide a report of its backup reviews monthly. The report shall include, at a minimum: - List of successful jobs - List of failed jobs - Confirmation that failed jobs re-ran successfully - A list of failed backups over the last month - A list of the number of failures on each server over the last month - Failures over consecutive attempts - Remediation efforts for those that have multiple back failures over the last month - Remediation efforts for those that have failed multiple consecutive attempts
WP-B-OPS-016.01	Operations	System Patching Report	30 Days after Go-Live	Monthly	The Contractor must provide patching reports on its failed patching attempts monthly. The report must include: - The servers that failed during the week - The number of times each failed - For those that fail two (2) or more consecutive attempts - The number of consecutive attempts - The remediation plan for each
WP-B-OPS-017.01	Operations	Capacity Planning Report	30 Days after Go-Live	Monthly	The Contractor must provide capacity planning reports monthly. The report must include, at a minimum: - Utilization trends for servers, storage, network, backup hardware and security devices - Thresholds where capacity would be increased - The interval that each of these are measured - Trend of utilization over the previous six (6) months
WP-B-PROJ-003.01	Operations	Operations Acceptance Transmittal	5 Days Prior to Go-Live	When Changed	The Contractor will submit a transmittal to the State indicating all hardware and software, and systems have been designed and tested, technical documentation has been submitted and approved by the State, and that the Contractor is prepared to assume operations with State approval.
WP-B-SEC-009.01	Operations	Plan of Action and Milestones (POA&M)	Upon findings from any security assessments	As Required by Security Policy	The Contractor shall 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
WP-B-SEC-012.01	Operations	User Access Control Reports	No later than 90 Days after Go-Live	Annually during O&M or Upon Change	The list of users who have access and what level of access to the system. Ensure that only legitimate users have access to the system

Number	Phase / Stage	Title	First Version Due	Frequency	Description
WP-B-SEC-014.01	Operations	Privileged User Access Control Reports	No later than 30 Days after Go-Live	Quarterly during O&M or Upon Change	Privileged access must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know basis. A document outlining separation of duties should be kept as a reference for who should have what access and to ensure no conflict of access or roles.
WP-B-TURN-001.01	Operations	Post Turnover Report	10 Days after System Turnover	Once	The Report will document that all Contractor turnover activities have been completed 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 Contractor as appropriate.