STATE OF NORTH CAROLINA **North Carolina Department of Information Technology**	**REQUEST FOR PROPOSAL NO. DIT 500874-001**
	Contract Name: Cybersecurity Professional Services
	Bid Opening Date: 09/9/2025
Refer ALL inquiries regarding this RFP to: **Name:** Allison Howard **Email:** Allison.Howard@nc.gov	**Issue Date: 07/17/2025**
	Commodity Code: 801015
	Purchasing Agency: North Carolina Department of Information Technology

OFFER

The Purchasing Agency is soliciting offers for the Professional Cybersecurity Services 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 (RFP), 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
NAME & TITLE OF PERSON SIGNING:		FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:	

Offer valid for two hundred eighty (280) days from date of offer opening unless otherwise stated here: ____ days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of the North Carolina Department of information Technology ("NCDIT") 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 DEPARTMENT OF INFORMATION TECHNOLOGY USE ONLY

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

by (Authorized representative of the NC Department of Information

Technology).

Table of Contents

1.0 PROCUREMENT SCHEDULE

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

Action	Responsibility	Date
RFP Issued	Agency	7/17/2025
Pre-Bid Presentation/Conference* **Please register at https://events.gcc.teams.microsoft.com/event/f07906 51-df77-495d-acd9-e7001e50247a@7a7681dc-b9d0-449a-85c3-ecc26cd7ed19**	Agency	7/31/2025
Written Questions Deadline	Vendors	8/7/2025
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	8/18/2025
Bid Opening	Agency	9/9/2025
Contract Award	Agency	**TBD**
Protest Deadline	Responding Vendors	15 days after **group/category /contract** award
*The State will share information intended to assist Vendors in the preparation of their bid responses. However, the state will not be able to entertain Vendor questions during the conference.		

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The North Carolina Department of Information Technology (NCDIT) is the primary technology advisor to state agencies and operates as a central IT service provider. NCDIT's mission is to deliver secure, reliable technologies to help agencies serve citizens in the digital age. NCDIT oversees state IT procurements and manages contracts for goods and services related to information technology. As part of its responsibilities, NCDIT ensures that state agencies have access to cost-effective, high-quality IT solutions.

The procurement of cybersecurity services through this RFP is an extension of NCDIT's commitment to safeguarding North Carolina's digital infrastructure and enhancing the state's cybersecurity posture.

The purpose of this RFP is to solicit Offers for cybersecurity professional services across several distinct service categories. This procurement significantly expands the State's cybersecurity capabilities beyond traditional assessment services to include operational security services, implementation and integration, governance and compliance, and specialized security domains.

The State will issue a solicitation for cybersecurity products after the cybersecurity professional services contract is awarded.

Services range from foundational security program assessments to advanced capabilities including Security Operations Center (SOC) services, incident response, DevSecOps, cloud security, and critical infrastructure protection.

This contract will establish a pool of qualified Vendors to provide cybersecurity expertise and services to support the State of North Carolina's agencies in protecting critical systems, data, and infrastructure from evolving cyber threats.

This solicitation will enable state agencies and other governmental entities to procure multiple cybersecurity professional services using a single contract vehicle.
This contract will include professional services for End Point Protection (208M) and Tanium 208T. Also, the contract will consolidate the services in the Security Assessments and Testing (918A) contract. The Security Assessments and Testing (918A) contract will terminate when those bid categories are fully awarded in this solicitation.

Therefore, Vendors currently awarded on Security Assessments and Testing, (918A), contract must bid on this solicitation to continue providing cybersecurity professional services to the State of North Carolina.

IT Infrastructure Solutions (204X) contract Vendors must not duplicate their 204X catalog items in this bid. Cybersecurity services catalog items that are inherently connected and bundled with IT infrastructure solutions or platforms must remain on the 204X contract.

However, cybersecurity professional service catalog items that are not dependent on specific IT infrastructure solutions or platforms can be offered in this bid.

Vendors with NCDIT enterprise or master cybersecurity contracts must not duplicate their enterprise or master cybersecurity professional services in this bid.

Currently contracted enterprise cybersecurity Vendors or master cybersecurity Vendors should seek to amend their contracts to include additional cybersecurity professional services.

NOTE: This bid is not for a specific solution. Instead, the bid will provide Vendors with the opportunity to describe their ability to provide the professional services requested in the bid specifications.

The resulting cybersecurity contracts will be used statewide across small, medium, large and extra-large/enterprise governmental entities.

Therefore, the State is unable to provide user specific architecture, software, hardware or other specific information across all agencies and other governmental entities that will be eligible to use the Cybersecurity Services Contract.

The State of North Carolina has adopted a Zero Trust Architecture framework based on NIST SP 800-207 principles.

Governmental entities using the contract will provide more specific information, using Scopes of Work (SOWs), to the Vendor selected for procurement of cybersecurity professional services.

Only time-limited, fixed priced, Scopes of Work (SOWs) for professional services are allowed using this contract.

This contract shall not be used for any kind of staff augmentation.

Staff augmentation needs must be satisfied using the IT Staffing State Term Contract.

Vendors may submit proposals for one or more of the bid categories set forth below and in Attachment I.

NCDIT will review and evaluate responses by category and may make multiple awards to Vendors by category.

NCDIT may, in its discretion, provide notice of the contract award to Vendors, or groups of Vendors, on a staggered basis.

CATEGORY SPECIFIC SCOPES OF WORK

Category A. Security Program Assessment and Consulting Services
Category B. Application Risk Assessment and Consulting Services
Category C. Penetration Test and Security Assessment Services
Category D. Security Incident Readiness and Response Services
Category E. Vulnerability Management Services
Category F. Network Security Services
Category G. Security Awareness and Training Services
Category H. Security Implementation and Integration Services
Category I. Security Operations Services
Category J. Governance, Risk, and Compliance Services
Category K. Application Security Services
Category L. DevSecOps and Security Automation Services
Category M. Identity and Access Security Services
Category N. Data Security Services
Category O. Cloud Security Services
Category P. Third-Party Risk Management Services
Category Q. Mobile Security Services
Category R. Critical Infrastructure and Operational Technology (OT) Security Services
Category S. Endpoint Security Services

Vendors are NOT required to provide offers for each service category.

Vendors who choose to respond to multiple categories must submit the general proposal response information and the category specific information for each responding bid category.

Refer to the main RFP document, RFP category Scopes of Work and the RFP Submittal Checklist, for response requirements and details.

Recognizing that information technologies and services are rapidly evolving and advancing, and that Vendors may be testing new technologies or developing new services that are not yet available to the public at the time of the submission of proposals, NCDIT reserves the right to issue an amendment to awarded contractors to include new service offerings at NCDIT's sole discretion.

DO NOT MARK YOUR ENTIRE PROPOSAL AS "CONFIDENTIAL" OR "PROPRIETARY."

DO NOT SUBMIT MARKETING MATERIALS IN LIEU OF PROVIDING SPECIFIC ANSWERS TO THE SPECIFICATIONS.

MARKETING MATERIALS WILL NOT BE ACCEPTED NOR EVALUATED AND YOUR BID RESPONSE MAY BE DEEMED INCOMPLETE AND/OR NON-RESPONSIVE.

EXCEPTIONS TAKEN TO THE TERMS AND CONDITIONS WILL MAKE A VENDOR'S OFFER NON-RESPONSIVE.

2.2 SUMMARY OF PROBLEM STATEMENT

North Carolina State agencies face increasingly sophisticated cyber threats that require comprehensive security capabilities beyond traditional assessment services. The current cybersecurity landscape demands not only identification of vulnerabilities but also active defense, continuous monitoring, rapid incident response, and proactive security implementation.

North Carolina's agencies need access to a full spectrum of defensive cybersecurity professional services—from foundational governance and risk management to advanced threat detection and response capabilities.

This procurement addresses the critical need for vendors who can provide expertise across all cybersecurity domains, enabling agencies to build resilient security programs, protect sensitive citizen data, ensure continuity of government services, and respond effectively to evolving threats.

The breadth of services in this RFP reflects the reality that effective cybersecurity requires an integrated approach encompassing people, processes, and technology across the entire security lifecycle.

2.3 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be five (5) year(s) and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for five (5) additional one (1) year periods at its sole discretion.

2.4 EFFECTIVE DATE

This solicitation 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.

2.5 CONTRACT TYPE

Pursuant to 9 NCAC 6B.0701, this solicitation will establish an indefinite quantity agency specific contract between a Vendor and the State. The quantity of Goods or Services that may be used by the State is undetermined. An estimated quantity based on history or other means may be used as a guide but shall not be a representation by the State of any anticipated purchase volume under any contract made pursuant to this solicitation.

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

Vendors are cautioned that the State cannot, does not, and will not guarantee purchase quantities to be made under this contract.

This solicitation will result in a Term Contract pursuant to 9 NCAC 06B.0701(1) to consolidate the normal anticipated requirements of state agencies.

The Agreement shall be and operate as a multiple Vendor contract. This shall be a Mandatory Statewide Term Contract for the use of Executive State Agencies.

Further, it may be used as a Convenience Contract, available, but not mandatory, for the use of non-state agencies as permitted by law. Such entities include the North Carolina University System and its member campuses, public education entities of the Department of Public Instruction and the North Carolina Community College System, as well as local (municipal and county) governments.

Vendors are not required to meet any required Minimum Sales Volume to bid on the requested cybersecurity professional services.

2.6 OPEN ENROLLMENT

The State may, in its discretion, periodically conduct open enrollment of the contract for consideration of new Vendors. Open enrollment will only be by invitation to selected Vendors whom the State determines will add value to the contract.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.1.1 REQUIREMENTS

Requirement means, as used herein, a function, feature, or performance that the System must provide. If the offer cannot meet the requirements, it will not be evaluated.

3.1.2 SPECIFICATIONS

Specification means, as used herein, a detailed description that 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, shall be regarded as meaning 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.

3.1.3 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.

3.1.4 EQUIVALENT ITEMS RESERVED.

3.1.5 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.

3.2 SECURITY SPECIFICATIONS

3.2.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE

Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website:

https://it.nc.gov/documents/vendor-readiness-assessment-report

VRARs must be provided for each bid category proposed by the Vendor.

Vendors may consolidate their VRAR submissions into one or more VRARs if their VRAR responses are the same or overlap across multiple bid categories.

Vendors choosing to consolidate must reference the specific bid categories in the VRAR submission(s).

The Cybersecurity Professional Services contract will be required to receive and securely manage data that is classified as *Highly Risk (Highly Restricted)*. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding this data classification. The policy is located at the following website: 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 NIST 800-53 controls.

Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(ii) below prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(ii) 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.

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 to the State on an annual basis a current independent 3rd party assessment report. Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred reports.

The State reserves the right to request VRARs from Vendors during the contract term as the State deems necessary.

A Vendor's access to a State entity's networks/systems, to provide contracted services, will be rendered via the issuance of a state-owned device or virtual desktop to Vendor's staff.

3.2.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE RESERVED.

3.3 ENTERPRISE SPECIFICATIONS RESERVED.

3.3.1 ARCHITECTURE DIAGRAMS RESERVED.

3.3.2 SOLUTION ROADMAP RESERVED.

3.3.3 IDENTITY AND ACCESS MANAGEMENT RESERVED.

3.3.4 INTEGRATION APPROACH RESERVED.

3.3.5 DISASTER RECOVERY AND BUSINESS CONTINUITY RESERVED.

3.3.6 DATA MIGRATION RESERVED.

3.3.7 APPLICATION MANAGEMENT RESERVED.

3.3.8 ACCESSIBILITY RESERVED.

3.3.9 ENTERPRISE, SERVICES, AND STANDARDS

Vendors should refer to the Vendor Resources Page for information on North Carolina Department of Information Technology regarding architecture, security, strategy, data, digital, identity and access management and other general information on doing business with state IT process.

The Vendor Resources Page 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 BUSINESS AND TECHNICAL REQUIREMENTS RESERVED.

3.5 BUSINESS AND TECHNICAL SPECIFICATIONS

SEE ATTACHMENT I: SCOPE OF WORK AND SPECIFICATIONS FOR FURTHER DETAILS.

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must list, itemize, and describe any applicable offer costs.

SEE ATTACHMENT D: CATEGORY COST FORMS FOR FURTHER DETAILS.

4.2 PAYMENT SCHEDULE RESERVED.

5.0 EVALUATION

N.C.G.S §143B-1350(h): All offers are subject to evaluation of the most advantageous offer to the State. 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, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation.

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 and recognizing that Best Value may result in award to other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with or traded off against other non-price factors.

a) Evaluation Process Explanation. State Agency employees will review all offers. 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. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.
b) To be eligible for consideration, Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to anyone (1) factor may be grounds for rejection regardless of overall score.
c) The evaluation committee may request clarifications, an interview with 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.
d) Vendors are advised that the State is not obligated to ask for or to accept after the closing date for offer receipt, data that is essential for a complete and thorough evaluation of the 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 weighted **Order of Importance**.

a. How well the Vendor's offer conforms with the specifications, ***(Attachment I)****, including risks associated with the Vendor's proposal* ***(Attachment F)*** *and a*dherence to the Section 3.2 Security Specifications.
b. How each Vendor's offer compares with other Vendors' offers.
c. Financial Stability **(Attachment H)**
d. Strength of references relevant to Specifications and Vendor Past Performance. **(Attachment G)**
e. Total Cost of Ownership. ***(Attachment D)***

Evaluation Criteria	**Maximum Points**
a. How well the Vendor's offer conforms with each category specifications, including *risks associated with the Vendor's proposal and* adherence to Section 3.2 Security Specifications.	40
b. How each Vendor's offer compares with other Vendors' offers.	20
c. Financial Stability.	15
d. Strength of references relevant to Specifications and Vendor Past Performance.	15
e. Total Cost of Ownership.	10
TOTAL POINTS	**100**

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 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 (i.e. assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

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

5.5 PAST PERFORMANCE

The Vendor may be disqualified from any evaluation or award if the Vendor or any key personnel proposed previously failed to perform satisfactorily during the performance of any contract with the State or violated rules or statutes applicable to public bidding in the State.

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 its 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 demonstrate 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 bid process or after award. Vendor 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. See Attachment B, Paragraph #38 of the attached North Carolina Department of Information Technology Terms and Conditions.

The Terms and Conditions made part of this solicitation contain language necessary for the implementation of North Carolina's statewide E-Procurement initiative. It is the Vendor's responsibility to read these terms and conditions carefully and to consider them in preparing the offer. By signature, the Vendor acknowledges acceptance of all terms and conditions including those related to E-Procurement.

a) General information on the E-Procurement service can be found at http://eprocurement.nc.gov/

b) Within two days after notification of award of a contract, the Vendor must register in NCE-Procurement@Your Service at the following website: http://eprocurement.nc.gov/Vendor.html

c) As of the RFP submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this RFP.

6.1.6 ELECTRONIC VENDOR PORTAL (EVP)

The State has implemented the electronic Vendor Portal (eVP) to allow the public to retrieve award notices and information from the Internet at https://evp.nc.gov. https://www.ips.state.nc.us/ips/. Results may be found by searching the Solicitation Number or the agency name. This information may not be available for several weeks depending on the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

Protests of awards exceeding $25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in the purchasing agency's office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests are governed by Title 9, Department of**

Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 PRE-OFFER CONFERENCE

Urged and Cautioned Pre-Offer Conference

Date: **7/31/2025**
Time: **1:00 PM ET**

Instructions: Vendor representatives are URGED and CAUTIONED to attend the meeting and apprise themselves of the conditions and requirements which will affect the performance of the work called for by this Request for Proposal. A non-mandatory meeting is scheduled for [HH:MM AM/PM] ET ***via Microsoft Teams***.

Submission of a proposal shall constitute sufficient evidence of this compliance and no allowance will be made for unreported conditions which a prudent Vendor would recognize as affecting the performance of the work called for in this proposal.

6.2.2 QUESTIONS CONCERNING THE RFP

All inquiries regarding the solicitation specifications or requirements are to be addressed to the contact person listed on Page One of this solicitation via the Ariba Sourcing Tool's message board. Vendor contact regarding this Solicitation with anyone other than the contact person listed on Page One of this Solicitation may be grounds for rejection of said Vendor's offer.

Vendors should focus their questions on the needed clarification of specifications and requirements. At this stage in the procurement, the State will not entertain in depth questions regarding contract award or post award contract administration.

Vendors should not identify their company name in Vendor questions which will be publicly posted as part of the procurement.

Written questions concerning this Solicitation will be received until **August 7, 2025 at 2:00 PM ET**

Questions must be submitted to the contact person listed on Page One of this Solicitation via **allison.howard@nc.gov**.

Please enter "Questions Solicitation "ITS 500874-001" as the subject for the message. Questions should be submitted in the following format:

REFERENCE	VENDOR QUESTION
RFP Section, Page Number	

6.2.3 ADDENDUM TO RFP

If 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 shall become an Addendum to this RFP and provided via the State's electronic Vendor Portal (eVP). 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's eVP website for 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 ERRATA AND EXCEPTIONS

Exceptions taken to the terms and conditions will make Vendors offers non-responsive.

6.2.6 ALTERNATE OFFERS RESERVED.

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 are not required to be registered to do business in the state with the NC Secretary of State ("NCSOS") to submit an offer. However, before contract award, Vendors must provide proof that the Vendor is registered with NCSOS to do business in the state.

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 at the following website: **https://evp.nc.gov.**

This RFP is available electronically on the electronic Vendor Portal (eVP) at the following website: **https://evp.nc.gov.**

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 pursuant to the instructions in Attachment J.

b) Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Do not include marketing materials or brochures.

c) **RESERVED**.

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 suffice 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, attachments or exhibits, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of offered costs, rates, or expenses must be presented in **Section 4.0. Cost of Vendor's Offer**.

THE OFFER SHOULD BE ORGANIZED AND INDEXED AS SPECIFIED IN ATTACHMENT J: - RFP SUBMITTAL.

6.3.3 OFFER SUBMITTAL

Due Date: **September 9, 2025**
Time: **2:00 PM ET**

IMPORTANT NOTE: *It is the Vendor's sole responsibility to upload their offer to the Ariba Sourcing Module by the specified time and date of opening. Vendor shall bear the risk for late electronic*

submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues.

Vendors must include all the pages of this solicitation in their response.

Only one consolidated response and one consolidated redacted response, if applicable, should be submitted.

The maximum file size for electronic submittal is 100 MB.

Sealed offers, subject to the conditions made a part hereof, will be received until **2:00 PM** Eastern Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted via the Ariba Sourcing Module with the Execution page signed and dated by an official authorized to bind the Vendor's firm. **Failure to return a signed offer shall result in disqualification.**

Attempts to submit a proposal via facsimile (FAX) machine, telephone, email, email attachments, or in any hardcopy format in response to this Bid WILL NOT be accepted and will automatically be deemed Non-Responsive.

a) Submit **one (1) signed, original electronic offer** through the Ariba Sourcing Module.
b) The Ariba Sourcing Module document number is: **WS WS1641013910**
c) All File names should start with the Vendor name first, in order to easily determine all the files to be included as part of the vendor's response. For example, files should be named as follows: Vendor Name-your file name.
d) File contents **SHALL NOT** be password protected, the file formats must be in .PDF, .JPEG, .DOC or .XLS format, and shall be capable of being copied to other sources. Inability by the State to open the Vendor's files may result in the Vendor's offer(s) being rejected as Non-Responsive.
e) If the Vendor's proposal contains any confidential information (as defined in **Attachment B, Section 1, Paragraph #18**), then the Vendor **must provide** one (1) signed, original electronic offer and one (1) redacted electronic copy.

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

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

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 F - LOCATION OF WORKERS UTILIZED BY VENDOR AND SUBMIT WITH YOUR OFFER.

7.2 FINANCIAL STATEMENTS

The Vendor must provide evidence of financial stability by returning with its offer **A**) completed Financial Review Form (Attachment I), **and B**) copies of Financial Statements as further described below. **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.

COMPLETE ATTACHMENT H – FINANCIAL REVIEW FORMS.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY RESERVED.

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

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

The Agency 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 Agency's security or other similar requirements.

All State and Vendor personnel that have access to data restricted by the State Security Manual and Policies must have a security background check performed. The Vendors are responsible for performing all background checks of their workforce and subcontractors. The State reserves the right to check for non-compliance.

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 RESERVED.

7.12 MEETINGS RESERVED.

7.13 RECYCLING AND SOURCE REDUCTION RESERVED.

7.14 SPECIAL TERMS AND CONDITIONS RESERVED.

7.15 AGENCY TERMS AND CONDITIONS RESERVED.

7.16 CONTRACT ADMINISTRATION

NCDIT Contract Administrator will monitor Vendor performance as necessary over the duration of the contract with respect to satisfactory fulfillment of all contractual obligations. Performance assessments may be comprised of compliance with the specifications for Services, prompt and appropriate resolution of warranty claims, adequate servicing of contract in any and all aspects which the contract has stipulated, maintaining current State pricing on the web site, and prompt, complete and satisfactory resolution of any contractual discrepancies.

Further, if a Vendor fails to adhere to the terms and conditions or other requirements of this contract or any subsequent solicitation issued under this contract, then the State, at its sole discretion, may remove the Vendor from the contract (or subsequent solicitation requests issued under this contract). The State may elect to remove the Vendor on a temporary or permanent basis.

Vendors shall provide the NCDIT Contract Administrator with the following reports, using the sample template provided below to support contract administration activities:

a. Purchase Activity Report: Vendor agrees to provide to the NCDIT Contract Administrator reports of sales achieved under the contract. These reports shall be provided quarterly, within thirty (30) calendar days from the last day of the reporting quarter. Reports shall include the data requested in the electronic template that can be accessed using the State's eVP portal.

   Emailed sales reports will not be accepted for this contract.

b. Vendor shall work with the NCDIT's Statewide IT Strategic Sourcing Office or Agency to address any special reporting requests.

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) **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.

3) **Deliverables**: Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include "Work Product" and means any expression of Licensor's findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information, but not source and object code or software.

4) **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).

5) **NCDIT or DIT:** The NC Department of Information Technology.

6) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.

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

8) **Request for Proposal (RFP):** The RFP 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. User should add Supplemental Terms and Conditions for Software and Services, when applicable.

9) **Security Breach:** As defined in N.C.G.S. §75-61.

10) **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 time lines 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.

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

12) **Small** as used in Attachment D: Category Cost Forms, means an entity with less than fifty (50) endpoints.

Medium as used in Attachment D: Category Cost Forms means an entity with fifty-one (51) to five hundred (500) endpoints.

Large as used in Attachment D: Category Cost Forms means an entity with five hundred one (501) to fifteen hundred (1,500) endpoints.

X-Large/Enterprise as used in Attachment D: Category Cost Forms means an entity with fifteen hundred one (1,501) and greater endpoints.

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.

   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: RESERVED.**

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 contract 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 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) **PAYMENT TERMS:** 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 in Paragraph 9 (Acceptance), or 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) **EQUAL EMPLOYMENT OPPORTUNITY:** 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) **ADVERTISING/PRESS RELEASE:** 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) **LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
14) **ACCESS TO PERSONS AND RECORDS:** 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. *The Joint Legislative Commission on Governmental Operations and the legislative employees whose primary responsibility is to provide professional or administrative services to the Commission may audit the records of the Vendor during and after the term of this Agreement to verify accounts and data affecting fees or performance in accordance with Chapter 120, Article 13.*
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) **CONFIDENTIALITY:** 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 Vendors 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) <u>DEFAULT</u>: 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's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.
c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9) of the DIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

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

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

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

ii) **Termination For Convenience Without Cause**: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.

iii) **Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.**

22) LIMITATION OF VENDOR'S LIABILITY:

a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.

b) The Vendor's liability for damages to the State arising under the contract shall be limited to two (2) times the value of the Contract. The value of the Contract is defined as two times the value of the Statement of Work (SOW).

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 Vendors 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 - CHANGES**) 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) **ELECTRONIC PROCUREMENT (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document):** Purchasing shall be conducted through the Statewide E-Procurement Services. The 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 the invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.

c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.

d) Vendor agrees at all times to maintain the confidentiality of its username and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.

b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.

c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:

   i. That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,

   ii. That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.

d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become non-infringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist

the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.

e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.

f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) <u>UNANTICIPATED TASKS:</u> 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:

a. 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

b. Terminate the work authorization, or

c. Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.

d. The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

41) STOP WORK ORDER RESERVED.

42) TRANSITION ASSISTANCE If the Agreement is not renewed at the end of the term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement, all reasonable transition assistance requested by the State, to allow for the expired or canceled 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. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement 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.

43) CLICKWRAP 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 for 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.

SECTION 2: TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY GOODS AND SERVICES RESERVED.

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.

3) 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) Unless otherwise provided by the Agency, the Vendor shall furnish all necessary personnel, Services, and otherwise perform all acts, duties and responsibilities necessary or incidental to the accomplishment of the tasks specified in the Agreement. The Vendor shall be legally and financially responsible for its personnel including, but not limited to, any deductions for social security and other withholding taxes required by state or federal law. The Vendor shall be solely responsible for acquiring any equipment, furniture, and office space not furnished by the State necessary for the Vendor to comply with the Agreement. The Vendor personnel shall comply with any applicable State facilities or other security rules and regulations.

4) PERSONAL SERVICES: **RESERVED.**

SECTION 4: SUPPLEMENTAL TERMS AND CONDITIONS APPLICABLE TO ARTIFICAL INTELLIGENCE ("AI")

1) Definitions:

"Algorithm"*:* A set of computational rules to be followed to solve a mathematical problem. More recently, the term has been adopted to refer to a process to be followed, often by a computer (NIST Glossary of AI Terms, March 2023).

"Artificial Intelligence (AI)": Artificial intelligence (AI) is a broad term used to describe an engineered system where machines learn from experience, adjusting to new inputs, and potentially performing tasks previously done by humans. More specifically, it is a field of computer science dedicated to simulating intelligent behavior in computers. It may include automated decision-making (International Association of Privacy Professionals, Glossary, https://iapp.org/resources/glossary/, 2024). This definition provides a high-level summary of AI definitions found in NIST's *The Language of Trustworthy AI: An In-Depth Glossary of Terms* (March 22, 2023).

"Generative Artificial Intelligence (GenAI)" A kind of artificial intelligence capable of generating new content such as code, images, music, text (Ex: ChatGPT), simulations, 3D objects, videos, and so on. It is considered an important part of AI research and development, as it has the potential to revolutionize many industries, including entertainment, art, and design (NIST Glossary of AI Terms, March 2023).

"Hallucination": Generated content that is nonsensical or unfaithful to the provided source content (NIST Glossary of AI Terms, March 2023).

For purposes of this Agreement, all references to "AI" shall be deemed to include both Artificial Intelligence (AI) and Generative AI (GenAI), collectively.

2) AI Prohibited Absent Authorization. Except as expressly disclosed and described by Vendor and expressly approved in writing by the State, Vendor represents and warrants that it will not provide any Software or other Deliverables, or perform any Services that use or incorporate, in whole or in part, any AI (or depends in any way upon any AI), including without limitation, any collection or processing of any of the State's Data using any AI.

3) Use and Disclosure of AI During the term of the Agreement.

(a) Vendor shall not activate GenAI or AI without the State's written consent and approval.

(b) Vendor must promptly notify the State in writing if Vendor's Services or any work under this Agreement includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors.

4) AI Architecture. If not included in the architectural diagram submitted at offer submission or provided upon request after contract award, the Vendor shall disclose the type(s) of model(s) and/or network(s) used or to be used in the AI model. This includes but is not limited to, generative adversarial networks (GANs) and neural networks.

5) **AI Subcontractors.** The Vendor shall remain responsible for ensuring that Subcontractors comply with all applicable terms and State requirements pertaining to its Solution or Services relating to the use of AI.

6) **AI Autonomy Classification**. Vendor represents that the AI functionality included in the Solution or Service falls into one of the following categories:

(a) Operates automatically with no human intervention;

(b) Operates automatically with occasional retrospective reviews by humans;

(c) System produces recommendations but cannot act without human intervention.

The applicable classification shall be clearly described in the Vendor's submitted documentation.

7) AI Warranties. With respect to all AI described or utilized by the Vendor , Vendor warrants that:

(a) Vendor has accurately identified and fully described all AI ;

(b) Vendor will not use, share, or process State data for any other purpose relating to the use of AI outside of this Agreement.

(c) Where Vendor is providing pre-trained model, the AI will (i) perform with a high degree of accuracy by maintaining a minimum accuracy rate above fifty percent; and (ii) not produce materially inaccurate results when used in accordance with the Documentation by the Vendor. Vendor shall provide documentation to support these performance claims upon request.

(d) Vendor will regularly monitor and validate the performance of the AI to ensure continued accuracy, reliability, and robustness. This includes the Vendor maintaining internal processes and policies for the regular assessment and validation of the AI's outputs for the duration of the Agreement.

(e) Vendor will employ appropriate techniques and technologies to detect and mitigate hallucinations;

(f) Vendor has obtained, and is in compliance with, all rights and licenses necessary to use all AI as described by Vendor;

(g) Vendor has complied with all Laws applicable to Vendor's development and provision of all AI as described by Vendor;

(h) Vendor specifically represents and warrants that Vendor has complied with all applicable data privacy laws, rules, and regulations, including but not limited to, the training of the AI algorithms and the data used in that training.

(i) Vendor will comply with all State policies and procedures relating to the use of AI; the requirements of this section are in addition to and not in lieu of other requirements in this Agreement and its Attachments;

(j) Vendor will notify the State at least sixty (60) days prior to any material changes pertaining to the AI (in whole or in part);

(k) Vendor will cooperate and comply with the State's privacy, security, and proprietary rights questionnaires and assessments concerning all AI and all proposed changes thereto;

(l) Vendor will, upon the State's request, allow the State (or its agent) to audit or review all Software, Deliverables, or Services for usage of AI and will provide the State with all related necessary assistance;

(m) Vendor will disclose any interruptions in use of Vendor's AI in the past six (6) months;

(n) Vendor (i) retains and maintains information in human-readable form that explains or could be used to explain the decisions made or facilitated by the AI, and (ii) maintains such information in a form that can readily be provided to the State upon request;

(o) Vendor maintains or adheres to industry standard policies, frameworks, and procedures relating to the ethical or responsible use of AI at and by Vendor, including policies, protocols and procedures for
   (i) developing and implementing AI in a way that promotes transparency, accountability and human interpretability. Vendor shall provide supporting documentation of their adoption and adherence;
   (ii) In the case where Vendor is providing pre-trained models Vendor must identify and mitigate unintended bias in training data or in the algorithmic model, including without limitation, implicit racial, gender, or ideological bias; and
   (iii) management oversight and approval of employees' use or implementation of AI (collectively, "Vendor AI Policies");
   (iv) auditing the AI's performance, such audits shall ensure the AI operates in alignment with applicable legal and ethical standards.

(p) there has been
   (i) no actual or alleged non-compliance with any such Vendor AI Policies;

(ii) no actual or alleged failure of any AI to satisfy the requirements or guidelines specified in any such Vendor AI Policies;
(iii) no claim alleging that any training data used in the development, training, improvement or testing of any AI was falsified, unintentionally biased, untrustworthy or manipulated in an unethical or unscientific way; and no report, finding or impact assessment by any employee, contractor, or third party that makes any such allegation; and
(iv) no request from any Governmental Authority concerning any Vendor AI.

(q) Vendor shall implement and maintain appropriate safeguards to protect State Data. Such safeguards must include, but are not limited to, the use of de-identification, anonymization, hashing, or other similar processes or privacy enhancing techniques when collecting or processing any State Data, to ensure the privacy, confidentiality, integrity, and security.

8) Use of AI. Reserved.

9) Training & Improving. Vendor may not use Inputs or Outputs to train or otherwise improve the AI, except solely for the benefit of the State. Notwithstanding the foregoing, Vendor may use Inputs or Outputs to train or otherwise improve the AI, but only if (a) such Inputs and Outputs have been (i) de-identified so that they do not identify the State, its Users or any other person; (ii) aggregated with data across Vendor's other customers; and (b) such use is approved in advance by the State Chief Information Officer or the Using Agency. For these purposes (and without limiting other obligations with respect to the State's Data generally), such Data is provided by the State to the Vendor strictly "AS IS".

10) Intellectual Property: **Reserved.**

11) Infringement by Outputs. With respect to infringement or misappropriation of third-party intellectual property rights by Outputs, should any Outputs become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor at its own expense, shall defend any action brought against the State. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. 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.

12) Special Restrictions on Use of AI. **Reserved.**

13) Limitation of Liability Modifications. The Limitation of Vendor's Liability in Section 1 of the NCDIT Terms and Conditions shall not apply to claims for data privacy or intellectual property infringement arising from Vendor's AI.

14) Updates. Vendor's AI has a data cutoff date of _____.

15) Confidentiality. Vendor will ensure that the Services and Software, provided via a third-party cloud ("Cloud Service Provider") and AI environment ("Cloud AI Service Environment"), shall maintain strict confidentiality and security of the State's Data. The State's Data will be securely retained within the specific, dedicated Cloud AI Service Environment allocated for the Vendor, and will not contribute to the training of the Vendor's or the Cloud Service Provider's AI models, nor be utilized by any third party outside of the State's express approval (in writing). Upon receipt of a notice from the State, Vendor will remove all State Data from the Cloud AI Service Environment. Vendor will ensure that the governing contractual terms (e g terms of service) issued by the Cloud Service Provider include provisions materially consistent with this provision and will identify the

forgoing to the State. Vendor will allow Customer to first approve in writing a given Cloud Service Provider and its Cloud AI Service Environment, such approval not to be unreasonably withheld or delayed. If there is any conflict or ambiguity between this provision and the rest of the Agreement, this provision governs and controls.

ATTACHMENT C: 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 and date 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	
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 D: CATEGORY COST FORMS

Note: A separate cost form is required for each bid category.
Remove all non-applicable cost categories

- ☐ **Category A: Security Program Assessment and Consulting Services**
- ☐ **Category B. Application Risk Assessment and Consulting Services**
- ☐ **Category C. Penetration Test and Security Assessment Services**
- ☐ **Category D. Security Incident Readiness and Response Services**
- ☐ **Category E. Vulnerability Management Services**
- ☐ **Category F. Network and Cloud Security Services**
- ☐ **Category G. Security Awareness and Training Services**
- ☐ **Category H. Security Implementation and Integration Services**
- ☐ **Category I. Security Operations Services**
- ☐ **Category J. Governance, Risk, and Compliance Services**
- ☐ **Category K. Application Security Services**
- ☐ **Category L. DevSecOps and Security Automation Services**
- ☐ **Category M. Identity and Access Security Services**
- ☐ **Category N. Data Security Services**
- ☐ **Category O. Cloud Security Services**
- ☐ **Category P. Third-Party Risk Management Services**
- ☐ **Category Q. Mobile Security Services**
- ☐ **Category R. Critical Infrastructure and Operational Technology (OT) Security Services**
- ☐ **Category S. Endpoint Security Services**

#	**CATEGORY SERVICE NAME**	**Public Entity***	**NTE Hourly Rate**	**Additional Information**
1.		**Small**		
		Medium		
		Large		
		X-Large/Enterprise		
2.	**CATEGORY SERVICE NAME**	**Public Entity***	**NTE Hourly Rate**	**Additional Information**
		Small		
		Medium		
		Large		
		X-Large/Enterprise		
3.	**CATEGORY SERVICE NAME**	**Public Entity***	**NTE Hourly Rate**	**Additional Information**
		Small		
		Medium		
		Large		
		X-Large/Enterprise		

*Fixed Price. Travel Must Be Included In Pricing.
Entity Size: Small Entity (50 or Less End Points); Medium Entity (51-500 End Points); Large Entity (501-1500 End Points); X-Large/Enterprise Entity (1500+ End Points).

ATTACHMENT E: 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 F: 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

If yes, Vendor MUST list in what countries the employees are working and in what capacity they are accessing State Data. Specifically, the State must know if the employees are Help Desk support, Technical Support and/or Coders, etc.

ATTACHMENT G: REFERENCES

(The bidding Vendor is required to complete this form to provide their reference information.)

Bidding Vendor Name:	
CATEGORY/SUBCATEGORY	

Vendor shall submit **two (2)** different customer references (**per subcategory**) using this form. Vendor's failure to provide the requested reference(s) will result in Vendor's termination for consideration of contract award. Vendors should copy this form as required to meet the reference submission requirements (one form per reference).

You may use the same reference for more than one subcategory, if appropriate and applicable. If you are using the same reference for more than one subcategory, you must still provide the complete Customer Reference Form for that customer for each subcategory.

References should demonstrate experience providing services the same, or similar to, those specified in the subcategory for which Vendors are submitting them for consideration.

The reference contact provided should have been in a leadership role in the project at the functional and/or technical levels. **References should be for work within three (3) years from the bid posting date.**

The State must be able to directly contact Vendor references. Vendor statements that references cannot be contacted or that contact with references must be initiated through the Vendor will be considered non-responsive.

The State will notify the Vendor if any of the Vendor's customer references do not respond to the State's reference check requests. The Vendor will have only one opportunity to provide replacement reference(s). Vendors will be required to provide a replacement reference(s) within five (5) calendar days from notification by the State. Vendors without two completed and returned references may not be considered for contract award.

SECTION I: CUSTOMER REFERENCE INFORMATION (All information requested below is required.)

Company/Organization Name:	
Customer Address:	
Contact Name and Title:	
Contact Phone Number:	
Contact Email Address:	

SECTION II: CONTRACT DETAILS

Contract Name:	
Value of Contract:	
Term of Contract:	
Date Service Began:	

Date Service Ended: (if applicable)	
If the contract was terminated, please indicate the circumstances.	
Did the project(s) stay on schedule? If not, what was the nature and cause of the delay(s)?	
Did the contract stay on budget? Were any change orders required? If so, how many? Please explain.	
Was training provided? If yes, please describe the length, type, and format.	
Please describe the services provided.	

ATTACHMENT H: 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.**

If you believe that your financial information is confidential. Please follow the requirements for submitting confidential information.

Proposals submitted without the requested financial documentation may be deemed non-responsive.

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 copy of 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 a link to annual reports with financial statements and management discussion 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			
a. Cash and Temporary Investments			
b. Accounts Receivable (beginning of year)			
c. Accounts Receivable (end of year)			
d. Average Account Receivable for the Year (calculated)			
e. Inventory (beginning of year)			
f. Inventory (end of year)			
g. Average Inventory for the Year (calculated)			
h. Current Assets			
i. Current Liabilities			
j. Total Liabilities			
k. Total Stockholders' Equity (beginning of year)			
l. Total Stockholders' Equity (end of year)			
m. Average Stockholders' Equity during the year (calculated)			
INCOME STATEMENT DATA			
a. Net Sales			
b. Cost of Goods Sold (COGS)			
c. Gross Profit (Net Sales minus COGS) (calculated)			
d. Interest Expense for the Year			
e. Net Income after Tax			
f. Earnings for the Year before Interest & Income Tax Expense			
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities			
b. Capital Expenditures (property, plant, equipment)			

ATTACHMENT I: SCOPE OF WORK AND SPECIFICATIONS

I. CATEGORY SPECIFIC SCOPES OF WORK OVERVIEW

Category A: Security Program Assessment and Consulting Services
Category B: Application Risk Assessment and Consulting Services
Category C: Penetration Test and Security Assessment Services
Category D: Security Incident Readiness and Response Services
Category E: Vulnerability Management Services
Category F: Network Security Services
Category G: Security Awareness and Training Services
Category H: Security Implementation and Integration Services
Category I: Security Operations Services
Category J: Governance, Risk, and Compliance Services
Category K: Application Security Services
Category L: DevSecOps and Security Automation Services
Category M: Identity and Access Security Services
Category N: Data Security Services
Category O: Cloud Security Services
Category P: Third-Party Risk Management Services
Category Q: Mobile Security Services
Category R: Critical Infrastructure and Operational Technology (OT) Security Services
Category S: Endpoint Security Services

As previously instructed, Vendors who choose to respond to multiple categories must submit the general proposal response information and the category specific information for each responding bid category.

Refer to the Main RFP Document, RFP category Scopes of Work and the RFP Submittal Checklist, for response instructions and details.

DO NOT MARK YOUR ENTIRE PROPOSAL AS "CONFIDENTIAL" OR "PROPRIETARY."

DO NOT SUBMIT MARKETING MATERIALS IN LIEU OF PROVIDING SPECIFIC ANSWERS TO SPECIFICATIONS.

MARKETING MATERIALS WILL NOT BE ACCEPTED NOR EVALUATED AND YOUR BID RESPONSE MAY BE DEEMED INCOMPLETE AND/OR NON-RESPONSIVE.

II. INFRASTRUCTURE OVERVIEW. The following overview is provided for informational purposes.

The State of North Carolina has adopted a Zero Trust Architecture framework based on NIST SP 800-207 principles.

Core Technologies: The core technologies of North Carolina's Executive State Agencies incorporate: leading industry solutions for operating systems, which may include but are not limited to, Windows 11, legacy Windows systems, MacOS, major Linux and other Unix distributions, iOS, and Android; and networking, which may include but are not limited to, Cisco Systems, Juniper Networks, Fortinet, Dell Technologies, Hewlett Packard Enterprise, Palo Alto Networks, Arista Networks, Gigamon, IBM, VMware, and F5 Networks. The State prioritizes commercial Software as a Service (SaaS) applications and standard development platforms while minimizing support for custom-developed solutions. Core technologies supported by Non-Executive State Agencies may differ from the above.

Operational Scope: The State's Executive State Agencies span multiple departments, supported by a diverse workforce including employees, contractors, volunteers, and interns. The State's Executive Branch Agencies currently have approximately 60,000 laptops and desktops, 3,000 Apple computers and tablets, and 10,000 Android and iOS mobile devices. There are approximately 3,500 Windows Servers and 40 VM Server Farms. State Executive Agencies have adopted a strategic approach towards virtualization.

Non-State Agencies also have computing infrastructures that will require cybersecurity support. Non-State entities utilize a variety of business systems that cater to specialized and general operational needs within data centers and managed cloud hosting environments as well as PaaS, SaaS, and IaaS solutions.

Data Centers: NCDIT operates data centers that are central to the State's IT infrastructure, supporting a wide range of services and applications.

Non-State Executive Agencies may also operate data centers for their own purposes.

Cloud Adoption: A significant portion of the State's primary business systems leverage cloud technology, including but not limited to, organizational tools, customer relationship management, productivity suites, infrastructure services, and specific applications geared towards enhancing operational efficiency and security.

III. CATEGORY SPECIFIC SCOPES OF WORK

CATEGORY A: SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Assessment Methodology:
      i) Describe the service method used to conduct security program assessments.
      ii) Describe how you evaluate the current effectiveness of an organization's security posture.
      iii) Describe the frameworks or standards used for your assessments (e.g., NIST, ISO, CIS).
      iv) Describe tools used to conduct the assessments and any clean up methodology used to remove the tools from the system.
   b) Scope and Depth of Assessments:
      i) Describe the scope and depth of your security program assessments.
      ii) Describe the program areas covered by the assessment (e.g., policies, procedures, technical controls, incident response, training).
      iii) Describe how you ensure that assessments are comprehensive.
   c) Risk Identification and Analysis:
      i) Describe how you identify and analyze risks in an organization's security program.
      ii) Describe how you prioritize risks.
      iii) Describe the criteria used to assess the potential risk impact.
   d) Recommendations and Roadmap Development:
      i) Describe how you provide recommendations and develop roadmaps for improving an organization's security posture.
      ii) Describe how you ensure that recommendations are actionable, prioritized, and aligned with an organization's business objectives.
   e) Stakeholder Engagement and Communication:

i) Describe your approach to engaging stakeholders during the assessment process.
ii) Describe how your findings and recommendations are communicated to both technical and non-technical stakeholders.

3) Capability:
   a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
   b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
   c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
   d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY B: APPLICATION RISK ASSESSMENT AND CONSULTING SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Assessment Scope and Techniques:
      i) Describe the scope of your application risk assessment services.
      ii) Describe the techniques used to identify and assess risks in both web-based, mobile, and client-server applications.
      iii) Describe your approach to assessing both custom-developed and commercial off-the-shelf applications.
   b) Vulnerability Identification and Prioritization:
      i) Describe how your service identifies vulnerabilities within applications.
      ii) Describe how you prioritize vulnerabilities.
      iii) Describe how you correlate multiple vulnerabilities to identify potential attack paths.
   c) Secure Coding Practices and Review:
      i) Describe how your service evaluates the application's adherence to secure coding practices.
      ii) Describe how you perform code reviews.
      iii) Describe how you ensure that developers follow best practices to mitigate security risks.
      iv) Describe your approach to evaluating third-party libraries and dependencies.
   d) Compliance with Security Standards:
      i) How does your service ensure that applications comply with applicable security standards and regulations (e.g., OWASP Top 10, PCI DSS, HIPAA).
      ii) Describe how you evaluate and ensure compliance across the entire application portfolio.
      iii) Describe how, in your application assessments, you address specific regulatory requirements.
   e) Application Security Architecture:
      i) Describe your approach to evaluating and recommending secure application architectures.
      ii) Describe how you assess authentication, authorization, and session management controls.
      iii) Describe how you evaluate both API security and third-party integrations.
3) Capability:

a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services.. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY C: PENETRATION TEST AND SECURITY ASSESSMENT SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Testing Methodologies and Scope:
      i) Describe the penetration testing methods that you employ.
      ii) Describe your process for planning and conducting Penetration Testing ranging from enclaves to enterprise-wide systems.
      iii) Describe the intrusion vectors that you are capable of testing.
      iv) Describe how you determine the boundaries of the testing environment.
      v) Describe your methods used to evaluate the security of various platforms and systems.
      vi) Describe your ability to perform tests of varying scopes and complexities.
      vii) Describe your process from scoping through reporting and remediation support.
      viii) Describe your approach to adversary emulation and threat-based testing.
      ix) Describe how you simulate advanced persistent threats and nation-state actors.
      x) Describe your approach to testing IoT, OT, or specialized systems.
   b) Red Team and Adversary Simulation Services:
      i) Describe your approach to conducting full-scope red team exercises including cyber, physical, and social engineering vectors.
      ii) Describe your ability to perform adversary simulation and emulation of specific threat actors.
      iii) Describe how you conduct purple team exercises to improve defensive capabilities.
      iv) Describe your methodology for campaign-based testing over extended periods.
      v) Describe how you simulate insider threats and advanced persistent threat behaviors.
      vi) Describe your approach to measuring and improving blue team detection and response capabilities.
   c) Compliance with Legal and Ethical Standards:
      i) Describe how your penetration testing services are designed to detect activities that violate (i) NCGS §14-454, Accessing Computers; (ii) the Computer Fraud and Abuse Act, Title 18 U.S.C. §1030; and (iii) the Electronic Communications Privacy Act of 1986 (ECPA), Title 18 U.S.C. §§ 2510-2523.
      ii) Describe how you ensure that testing is conducted without disruption of an organization's normal business activities.
      iii) Describe how you approach risk mitigation during active testing.
   d) Reporting and Debriefing:

i) Describe the reports provided following a security test.
ii) Describe how you debrief an organization on your findings.
iii) Describe how you recommend remediation strategies for discovered vulnerabilities.
iv) Describe validation of remediation efforts after implementation.

e) Tools and Technologies Used:
i) Describe the tools and technologies used during your security testing.
ii) Describe how you stay current with the latest testing tools and techniques.

f) Client Collaboration and Communication:
i) Describe your approach to client collaboration and communication throughout the penetration testing.
ii) Describe how you involve clients in planning, execution, and post-testing activities.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe your qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY D: SECURITY INCIDENT READINESS AND RESPONSE SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) Incident Readiness Assessment:
i) Describe the framework or methods used to assess an organization's incident response readiness.
ii) Describe the evaluation of the current state of an organization's incident response plan, procedures, and capabilities.
iii) Describe how you conduct tabletop exercises and simulations to test readiness.
iv) Describe your approach to developing and maintaining incident response playbooks.
v) Describe how your service ensures that an organization's incident response practices are compliant with NIST SP 800-61 and/or ISO/IEC 27035 best practices.

b) Incident Response Capabilities:
i) Describe your incident response services and capabilities.
ii) Describe how you assist organizations in detecting, investigating, containing, eradicating, and recovering from cybersecurity incidents.
iii) Describe your incident response methodology and process.
iv) Describe your ability to respond to various types of incidents (e.g., ransomware, data breach, insider threat).
v) Describe your approach to digital forensics and evidence collection.

c) Response Time and Availability:

i) Describe your incident response times and provisions for responding to incidents.
ii) Describe how you ensure availability and rapid deployment of resources when an organization requires immediate assistance.
iii) Describe your on-call procedures and escalation processes.

d) Communication and Coordination:
i) Describe your approach to communication and coordination during an incident response.
ii) Describe how you interact with an organization's internal teams, external stakeholders, and law enforcement when required.
iii) Describe your stakeholder management during a crisis.

e) Post-Incident Activities:
i) Describe your post-incident reporting and debriefing process.
ii) Describe the types of reports and documentation provided.
iii) Describe how you facilitate lessons learned and improvement of incident response plans.
iv) Describe your approach to post-incident threat hunting to ensure complete remediation.

f) Malware Analysis and Response:
i) Describe your malware analysis capabilities and methodology.
ii) Describe how you reverse engineer malicious code.
iii) Describe how you extract indicators of compromise from malware.
iv) Describe how you develop custom detection and prevention mechanisms.

g) Breach Management and Notification:
i) Describe your approach to breach investigation and scope determination.
ii) Describe your breach notification planning and execution.
iii) Describe your regulatory compliance assistance to an organization following a breach.
iv) Describe your methodology for stakeholder communication during breaches.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY E: VULNERABILITY MANAGEMENT SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) Vulnerability Assessment and Management Approach:
i) Describe the scope of your vulnerability management services.

ii) Describe your methodology for continuous vulnerability assessment and management.
iii) Describe how you ensure comprehensive coverage across all assets and environments.
iv) Describe your approach to vulnerability, scanning frequency and scheduling.

b) Vulnerability Scanning Tools and Techniques:
i) Describe the tools and techniques your team has experience supporting for vulnerability scanning.
ii) Describe how you ensure that the tools are current with the latest vulnerability signatures and scanning capabilities.
iii) Describe your approach to authenticated versus unauthenticated scanning.
iv) Describe how you minimize performance impact during scanning activities.

c) Vulnerability Prioritization and Remediation:
i) Describe how you prioritize vulnerabilities based on risk and business impact.
ii) Describe your vulnerability scoring methodology and how it aligns with industry standards.
iii) Describe how you develop remediation strategies based on vulnerability findings.
iv) Describe your approach to tracking remediation progress and verifying fixes.

d) Patch Management:
i) Describe your patch management methodology and approach.
ii) Describe your capabilities for patch prioritization and deployment.
iii) Describe how you handle emergency patching for critical vulnerabilities.
iv) Describe your approach to patch testing and validation.
v) Describe how you manage patching across diverse environments.

e) Reporting and Metrics:
i) Describe the types of reports and metrics provided as part of your vulnerability management services.
ii) Describe how you track vulnerability trends and remediation effectiveness over time.
iii) Describe how you communicate findings to different organizational stakeholders.
iv) Describe how you measure the effectiveness of the vulnerability management program.

f) Integration with Security Operations:
i) Describe how your vulnerability management services integrate with other security operations.
ii) Describe how you correlate vulnerability data with threat intelligence and security events.
iii) Describe your approach to identifying and addressing threats targeting known vulnerabilities.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY F: NETWORK SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
    a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
    a) Network Security Assessment and Design:
        i) Describe the methods used to assess network security architecture.
        ii) Describe how you evaluate the current network design for potential vulnerabilities and compliance with best practices.
        iii) Describe your approach to network segmentation design and implementation.
        iv) Describe your process for developing secure network architectures.
    b) Network Security Implementation:
        i) Describe your capabilities for implementing network security controls.
        ii) Describe your approach to firewall management and optimization.
        iii) Describe how you implement secure remote access solutions.
        iv) Describe how you implement network monitoring and visibility solutions.
    c) DNS Security:
        i) Describe your approach to DNS security and filtering.
        ii) Describe your capabilities for DNS monitoring and threat detection.
        iii) Describe how you implement DNS-based security controls.
        iv) Describe your methodology for protecting against DNS-based attacks.
    d) Zero Trust Implementation:
        i) Describe how you design and implement zero trust architectures.
        ii) Describe your approach to transition organizations from traditional perimeter-based security to zero trust.
        iii) Describe how you implement least-privilege access controls.
        iv) Describe how you integrate identity and network security in zero trust implementations.
    e) Email Security Services:
        i) Describe your approach to comprehensive email security.
        ii) Describe your ability to protect an organization against phishing, malware, and other email-borne threats.
        iii) Describe how you implement data loss prevention for email communications.
        iv) Describe your methodology for email authentication and anti-spoofing.
        v) Describe how you secure cloud-based email platforms.
        vi) Describe your capabilities for email encryption and secure messaging.
    f) Web Security Services:
        i) Describe your approach to implementing and managing web security gateways and proxy services.
        ii) Describe your capabilities for SSL/TLS inspection and certificate management.
        iii) Describe how you implement web content filtering, URL categorization, and malicious site blocking.
        iv) Describe your methodology for protecting against web-based malware and phishing.
        v) Describe your approach to browser isolation and remote browser technologies.
        vi) Describe how you integrate web security with existing SIEM and security operations.
3) Capability:
    a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
    b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
    c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
    d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
    a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly

demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).

b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY G: SECURITY AWARENESS AND TRAINING SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Program Content and Structure:
      i) Describe the content and structure of your security awareness and training programs.
      ii) Describe the topics covered in the training and how they align with current threats.
      iii) Describe how you ensure that the material is relevant and effective for different audience types.
      iv) Describe how you customize content for different organizational roles and responsibilities.
   b) Training Delivery Methods:
      i) Describe the various delivery methods available for your training programs.
      ii) Describe how you determine the most effective delivery method for an organization.
      iii) Describe your in-person, virtual, and self-paced training options.
      iv) Describe your simulation capabilities such as phishing simulations or attack scenarios.
   c) Engagement and Effectiveness:
      i) Describe your methods used to engage users and ensure interactivity during the training.
      ii) Describe how you ensure that your training is engaging and memorable to maximize retention.
      iii) Describe how you measure training effectiveness and knowledge retention.
      iv) Describe your approach to making learning about cybersecurity more engaging, memorable, and effective.
   d) Program Measurement and Improvement:
      i) Describe how you measure the effectiveness of security awareness programs.
      ii) Describe the metrics you use to track improvements in security behavior.
      iii) Describe your approach to continuous program improvement based on results.
      iv) Describe how you benchmark awareness program effectiveness against industry standards.
   e) Specialized Training Programs:
      i) Describe any specialized training programs you offer for specific audiences.
      ii) Describe how you deliver role-based security training.
      iii) Describe how you address compliance requirements in your training programs.
      iv) Describe your security training for developers and technical staff.
3) Capability:
   a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
   b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
   c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
   d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly

demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY H: SECURITY IMPLEMENTATION AND INTEGRATION SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Security Technology Implementation:
      i) Describe how you implement and integrate key security technologies including but not limited to SIEM, EDR, XDR, DLP, and email security platforms.
      ii) Describe how you select security technologies to address specific requirements.
      iii) Describe how you ensure interoperability between security technologies.
      iv) Describe how you optimize and tune security technologies post-implementation.
      v) Describe how you develop use cases and detection rules for security monitoring technologies.
   b) Security Architecture Design:
      i) Describe how you design a security architecture.
      ii) Describe how you develop a security reference architecture.
      iii) Describe how you translate business requirements into a security architecture.
      iv) Describe how you incorporate scalability into security designs.
   c) Technology Selection and Evaluation:
      i) Describe your approach to security technology selection and evaluation.
      ii) Describe the criteria you use to evaluate security products and Vendors.
      iii) Describe how you conduct proof of concept testing for security technologies.
      iv) Describe your approach to total cost of ownership analysis for security solutions.
   d) Implementation Quality Assurance:
      i) Describe your quality assurance process for security implementations.
      ii) Describe how you validate whether implementations meet design specifications.
      iii) Describe your approach to security testing after implementation.
      iv) Describe how you measure the effectiveness of implemented security controls.
3) Capability:
   a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
   b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
   c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
   d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:

a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY I: SECURITY OPERATIONS CENTER (SOC) SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your SOC Services address the specifications listed below.
2) Technical Qualifications:
   a) Security Operations Center (SOC) Services:
      i) Describe your SOC services.
      ii) Describe how you establish, manage, and operate SOC services.
      iii) Describe the technology stack, staffing, and processes supported in your SOC operations.
      iv) Describe your continuous monitoring capabilities and coverage hours.
      v) Describe and provide the service level agreements (SLAs) related to response times and support availability
   b) Threat Detection and Analysis:
      i) Describe your approach to threat intelligence collection and analysis.
      ii) Describe your capabilities for dark web monitoring and analysis.
      iii) Describe the methodologies and tools supported for threat detection and analysis.
      iv) Describe how you leverage threat intelligence to identify and mitigate threats.
      v) Describe your process for analyzing security events and correlating data from various sources.
      vi) Describe your approach to threat hunting and proactive threat detection.
   c) Threat Intelligence Services:
      i) Describe your standalone threat intelligence services separate from SOC operations.
      ii) Describe your threat intelligence platform implementation and management.
      iii) Describe how you aggregate, normalize, and operationalize multiple threat intelligence feeds.
      iv) Describe how you provide threat intelligence analysis, contextualization, and actionable reporting.
   d) Alert Management and Response:
      i) Describe your alert management process and triage procedures.
      ii) Describe how you prioritize and escalate security alerts.
      iii) Describe your mean time to detect (MTTD) and mean time to respond (MTTR) metrics.
      iv) Describe your alert investigation and remediation procedures.
   e) Integration:
      i) Describe how you provide managed detection and response (MDR) services.
      ii) Describe your extended detection and response (XDR) across multiple security domains.
      iii) Describe how you incorporate automation and orchestration into security operations.
      iv) Describe your threat intelligence integration and operationalization.
   f) Training and Knowledge Transfer:
      i) Describe the training programs available for client staff to ensure they are proficient in working with SOC services.
      ii) Describe your knowledge transfer process to ensure clients can maintain and optimize their security operations post-deployment.
   g) Reporting and Metrics:
      i) Describe the reporting and metrics provided as part of your security operations services.
      ii) Describe your measurement and reporting on security operations effectiveness.
      iii) Describe your approach to security posture reporting for different stakeholders.
      iv) Describe how you demonstrate return on investment for security operations.
   h) Insider Threat Management:

i) Describe your approach to insider threat program development.
ii) Describe how you detect and investigate insider threats.
iii) Describe how you balance security with privacy when monitoring insider threats.
iv) Describe your methodology for insider threat risk assessment.

i) Standalone SIEM and Security Analytics Services:
i) Describe how you implement and manage SIEM platforms without full SOC services.
ii) Describe your approach to security log aggregation, normalization, and correlation.
iii) Describe how you develop and tune SIEM use cases and detection rules.
iv) Describe your methodology for security analytics platform implementation and optimization.
v) Describe how you provide SIEM-as-a-Service for organizations not requiring 24x7 SOC.
vi) Describe your approach to SIEM sizing, architecture, and performance optimization.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY J: GOVERNANCE, RISK, AND COMPLIANCE SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) Security Policy Development:
i) Describe your approach to developing comprehensive security policies.
ii) Describe how you ensure that policies are aligned with business objectives and risk tolerance.
iii) Describe your methodology for policy lifecycle management.
iv) Describe how you ensure policies remain current with evolving threats and regulations.

b) Regulatory Compliance:
i) Describe your expertise in cybersecurity regulatory compliance.
ii) Describe how you help organizations comply with relevant regulations and standards.
iii) Describe your approach to compliance gap assessment and remediation.
iv) Describe how you stay current with evolving regulatory requirements.

c) Risk Management:
i) Describe your approach to cybersecurity risk management.
ii) Describe the risk assessment methodologies you employ.
iii) Describe how you quantify and communicate risk to business stakeholders.
iv) Describe your approach to developing and implementing risk treatment plans.

d) Security Metrics and Reporting:
    i) Describe how you develop and track security metrics.
    ii) Describe how you align metrics with business objectives and risk priorities.
    iii) Describe your reports and dashboards.
    iv) Describe how you use metrics to drive continuous security improvement.
e) Security Program Governance:
    i) Describe your approach to security program governance.
    ii) Describe how you establish and maintain effective security committees and oversight functions.
    iii) Describe your methodology for security strategy development and execution.
    iv) Describe how you measure and report on security program effectiveness.

3) Capability:
    a) Describe the scalability, interoperability, customization, and integration capabilities of your services.
    b) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
    c) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
    a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
    b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
    a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY K: APPLICATION SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
    a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
    a) Secure Development Lifecycle Integration:
        i) Describe how you integrate security into all phases of the software development lifecycle.
        ii) Describe how you implement and optimize DevSecOps practices.
        iii) Describe how you ensure security is considered from initial design through deployment and maintenance.
        iv) Describe your methodology for secure requirements gathering and threat modeling.
    b) Application Security Testing:
        i) Describe your capabilities for application security testing.
        ii) Describe your approach to static application security testing (SAST).
        iii) Describe your approach to dynamic application security testing (DAST).
        iv) Describe your capabilities for interactive application security testing (IAST) and runtime application self-protection (RASP).
        v) Describe your approach to application programming interface (API) security testing.
    c) Secure Coding Practices:
        i) Describe your approach to promoting and implementing secure coding practices.
        ii) Describe how you provide secure coding training and guidance to development teams.
        iii) Describe your code review methodology and tools.
        iv) Describe how you assess and improve secure coding knowledge and practices.

d) Software Composition Analysis:
    i) Describe your approach to software composition analysis and open-source security.
    ii) Describe how you identify and manage vulnerabilities in third-party components.
    iii) Describe how you maintain software bills of materials (SBOMs).
    iv) Describe how you assess and manage license compliance risks.
e) Application Security Governance:
    i) Describe your approach to application security governance.
    ii) Describe how you establish and enforce application security standards and policies.
    iii) Describe your methodology for security architecture reviews.
    iv) Describe how you measure and report on application security program effectiveness.

3) Capability:
    a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
    b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
    c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
    d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
    a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
    b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
    a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY L: DEVSECOPS AND SECURITY AUTOMATION SERVICES

SPECIFICATIONS:

1) Overview:
    a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
    a) DevSecOps Strategy and Implementation:
        i) Describe your approach to developing and implementing DevSecOps strategies.
        ii) Describe how you integrate security practices into DevOps workflows.
        iii) Describe your methodology for DevSecOps maturity assessment and improvement.
        iv) Describe how you measure the effectiveness of DevSecOps practices.
    b) Security Automation:
        i) Describe your capabilities for security automation.
        ii) Describe your approach to automating security testing within CI/CD pipelines.
        iii) Describe how you implement security orchestration and automated response.
        iv) Describe your methodology for identifying and prioritizing security automation opportunities.
    c) Security as Code:
        i) Describe your approach to implementing security as code.
        ii) Describe how you develop and maintain infrastructure as code (IaC) security.
        iii) Describe your approach to policy as code implementation.
        iv) Describe how you ensure the security of containerized environments.
    d) Security Tool Integration:

i) Describe your capabilities for integrating security tools into DevOps toolchains.
ii) Describe your approach to API-based integration between security and development tools.
iii) Describe how you implement and maintain security tool automation.
iv) Describe your methodology for security tool selection and evaluation.

e) DevSecOps Culture and Collaboration:
i) Describe how you foster DevSecOps culture and collaboration.
ii) Describe how you promote shared responsibility for security across development, operations, and security teams.
iii) Describe your methodology for DevSecOps training and skills development.
iv) Describe how you measure and improve security collaboration effectiveness.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY M: IDENTITY AND ACCESS SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) Identity Governance and Administration:
i) Describe your approach to identity governance and administration.
ii) Describe your capabilities for implementing and optimizing identity lifecycle management.
iii) Describe your methodology for identity attestation and recertification.
iv) Describe how you implement role-based access control and attribute-based access control models.

b) Access Management:
i) Describe your capabilities for implementing and managing access management solutions.
ii) Describe your approach to single sign-on implementation across diverse environments.
iii) Describe how you implement and manage multi-factor authentication solutions.
iv) Describe your methodology for access policy design and enforcement.

c) Privileged Access Management:
i) Describe your approach to privileged access management.
ii) Describe how you implement privileged account discovery and management.
iii) Describe how you implement and manage session monitoring and recording.
iv) Describe your methodology for privileged access governance and compliance.

d) Identity Security Operations:

i) Describe your approach to identity security monitoring and analytics.
ii) Describe how you detect and respond to identity-based threats.
iii) Describe your capabilities for user and entity behavior analytics (UEBA).
iv) Describe your methodology for identity threat hunting and investigation.

e) Authentication Security:
i) Describe your approach to multi-factor authentication implementation.
ii) Describe how you manage diverse authentication methods.
iii) Describe how you implement risk-based authentication.
iv) Describe your methodology for secure authentication across environments.

f) Zero Trust Identity Architecture:
i) Describe how you implement zero trust identity architectures.
ii) Describe how you integrate identity security with network and application security.
iii) Describe your methodology for continuous authentication and authorization.
iv) Describe how you implement least privilege access across diverse environments.

g) User Behavior Analytics:
i) Describe your approach to user and entity behavior analytics.
ii) Describe how you detect anomalous user behavior.
iii) Describe how you integrate behavior analytics with access controls.
iv) Describe your you reduce false positives in behavior monitoring.

h) Directory Security:
i) Describe your approach to directory services security.
ii) Describe how you secure Active Directory and other directory services.
iii) Describe how you manage directory privilege escalation risks.
iv) Describe your methodology for directory security monitoring and cleanup.

i) PKI and Certificate Management Services:
i) Describe how you design and implement Public Key Infrastructure (PKI) solutions.
ii) Describe your capabilities for enterprise certificate lifecycle management.
iii) Describe how you manage SSL/TLS certificates across diverse environments.
iv) Describe your methodology for certificate discovery, inventory, and compliance monitoring.
v) Describe your approach to code signing certificate management and security.
vi) Describe how you implement certificate-based authentication and encryption solutions.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY N: DATA SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Data Security Architecture and Consulting:
      i) Describe your approach to designing enterprise data security architectures.
      ii) Describe how you assess current data security postures and identify gaps.
      iii) Describe your methodology for developing data security roadmaps and strategic plans.
      iv) Describe how you align data security architecture with Zero Trust principles.
   b) Data Discovery and Classification Services:
      i) Describe your methodology for conducting data discovery assessments across diverse environments.
      ii) Describe how you design and implement data classification frameworks and schemas.
      iii) Describe your approach to developing automated classification rules and policies.
      iv) Describe how you help organizations establish and maintain data inventories and catalogs.
   c) Data Loss Prevention Program Development:
      i) Describe your approach to designing comprehensive DLP programs and strategies.
      ii) Describe how you assess and recommend DLP solutions for various environments.
      iii) Describe your methodology for developing DLP policies and use cases.
   d) Data Privacy and Compliance Services:
      i) Describe your approach to conducting Privacy Impact Assessments (PIAs).
      ii) Describe how you develop privacy programs and governance frameworks.
      iii) Describe your methodology for implementing privacy by design principles.
      iv) Describe how you assist with cross-border data transfer assessments and solutions.
   e) Information Protection and Rights Management (IRM) Consulting:
      i) Describe your approach to designing information rights management programs.
      ii) Describe how you secure data across its lifecycle.
      iii) Describe how you implement access controls at the document level.
      iv) Describe how you integrate IRM with existing security infrastructure.
3) Capability:
   a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
   b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
   c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
   d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY O: CLOUD SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Cloud Security Posture Management:
      i) Describe your approach to cloud security posture management.

ii) Describe how you assess and improve cloud security configurations.
iii) Describe your methodology for continuous cloud compliance monitoring.
iv) Describe how you implement and manage cloud security baselines.

b) Cloud Access Security:
i) Describe your approach to cloud access security.
ii) Describe your methodology for securing access to SaaS applications.
iii) Describe how you monitor and control cloud application usage.

c) Cloud Workload Protection:
i) Describe your approach to cloud workload protection.
ii) Describe how you secure virtual machines, containers, and serverless functions.
iii) Describe your methodology for implementing cloud workload security controls.
iv) Describe how you integrate cloud workload security with application security.

d) Cloud Security Architecture:
i) Describe your approach to secure cloud architecture design.
ii) Describe how you develop and implement cloud security reference architectures.
iii) Describe your methodology for secure cloud migration.
iv) Describe how you implement security across multi-cloud and hybrid environments.

e) Cloud Security Operations:
i) Describe your approach to cloud security monitoring and operations.
ii) Describe your capabilities for cloud-native security monitoring and response.
iii) Describe your methodology for cloud security incident management.
iv) Describe how you implement and manage cloud security automation.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY P: THIRD-PARTY RISK MANAGEMENT SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) Third-Party Risk Assessment:
i) Describe your approach to third-party risk assessment.
ii) Describe how you evaluate third-party security postures.
iii) Describe your methodology for third-party risk tiering and prioritization.

iv) Describe how you assess third-party compliance with security requirements.

b) Third-Party Risk Monitoring:
   i) Describe your approach for continuous third-party risk monitoring.
   ii) Describe how you detect changes in third-party security postures.
   iii) Describe your methodology for monitoring third-party security incidents.
   iv) Describe how you implement and manage third-party risk monitoring solutions.

c) Supply Chain Security:
   i) Describe your approach to supply chain security.
   ii) Describe how you secure software supply chains.
   iii) Describe your methodology for evaluating and managing supply chain risks.
   iv) Describe how you implement and manage software bill of materials (SBOM) solutions.

d) Third-Party Security Requirements:
   i) Describe your approach to developing third-party security requirements.
   ii) Describe how you implement and manage third-party security contracts.
   iii) Describe your methodology for incorporating security requirements into procurement processes.
   iv) Describe how you verify third-party compliance with security requirements.

e) Third-Party Incident Response:
   i) Describe your approach to managing third-party security incidents.
   ii) Describe how you coordinate incident response with third parties.
   iii) Describe your methodology for assessing third-party incident impact.
   iv) Describe how you manage remediation of third-party security incidents.

3) Capability:
   a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
   b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
   c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
   d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.
4) Experience and Key Personnel:
   a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
   b) Describe the Vendor's qualifications to perform the services specified in the category.
5) Support and Maintenance:
   a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY Q: MOBILE SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
   a) Describe how your Services address the specifications listed below.
2) Technical Qualifications:
   a) Mobile Device Security Assessment:
      i) Describe your approach to assessing mobile device security across various platforms (iOS, Android, etc.).
      ii) Describe how you evaluate mobile device configuration and security controls.
      iii) Describe how you identify vulnerabilities and security gaps in mobile device deployments.
      iv) Describe your approach to evaluating the effectiveness of existing mobile security solutions.
   b) Mobile Application Security:
      i) Describe your capabilities for mobile application security testing.

ii) Describe how you identify vulnerabilities in mobile applications.
iii) Describe your methodology for testing both internally developed and third-party mobile applications.
iv) Describe how you evaluate the security of mobile application data storage, transmission, and processing.

c) Mobile Device Management (MDM) or Mobile Application Management (MAM) Implementation:
i) Describe how you implement and optimize MDM/MAM solutions.
ii) Describe your ability to configure and deploy mobile device security policies.
iii) Describe how you integrate MDM/MAM with existing identity and access management systems.
iv) Describe how you implement containerization and application management on mobile devices.

d) Mobile Threat Detection and Response:
i) Describe how you implement mobile threat detection and response capabilities.
ii) Describe how you monitor and identify threats to mobile devices.
iii) Describe how you respond to mobile security incidents.
iv) Describe how you integrate mobile security monitoring with broader security operations.

e) Bring Your Own Device (BYOD) and Corporate-Owned Device Security:
i) Describe how you secure both BYOD and corporate-owned mobile devices.
ii) Describe how you implement separation of personal and corporate data.
iii) Describe how you enforce security policies while respecting user privacy.
iv) Describe how you address the unique challenges of BYOD environments.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY R: CRITICAL INFRASTRUCTURE AND OPERATIONAL TECHNOLOGY (OT) SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your Services address the specifications listed below.

2) Technical Qualifications:
a) OT Security Assessment and Monitoring:
i) Describe how you assess and monitor security in OT environments.
ii) Describe how you secure industrial control systems (ICS), SCADA, and other OT assets.

b) Critical Infrastructure Protection:
i) Describe your approach to critical infrastructure security and resilience.
ii) Describe how you implement sector-specific security controls.

c) OT/IT Convergence Security:
i) Describe how you securing environments where IT and OT systems converge.
ii) Describe how you implement security that respects operational requirements.

d) Industrial Network Security:

i) Describe how you secure industrial networks and protocols.
ii) Describe how you implement segmentation in OT environments.

e) OT Threat Intelligence and Response:
i) Describe how you provide specialized threat intelligence for critical infrastructure.
ii) Describe your methodology for incident response in OT environments.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:
a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

CATEGORY S: ENDPOINT SECURITY SERVICES

SPECIFICATIONS:

1) Overview:
a) Describe how your endpoint security professional Services address the specifications listed below.

2) Technical Qualifications:
a) Endpoint Security Architecture and Design:
i) Describe your approach to designing enterprise endpoint security architectures.
ii) Describe how you assess current endpoint security posture and identify gaps.
iii) Describe your methodology for developing endpoint security roadmaps aligned with Zero Trust principles.
iv) Describe how you design endpoint security strategies for diverse device types.

b) Endpoint Security Assessment Services:
i) Describe your methodology for conducting comprehensive endpoint security assessments.
ii) Describe how you evaluate endpoint protection coverage and effectiveness.
iii) Describe your approach to endpoint vulnerability assessment and prioritization.

c) Endpoint Hardening and Configuration Services:
i) Describe your approach to developing endpoint hardening standards.
ii) Describe how you design secure baseline configurations for various operating systems.
iii) Describe your methodology for implementing least-privilege access on endpoints.
iv) Describe how you develop and implement application control and whitelisting strategies.

3) Capability:
a) Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based.
b) Describe the scalability, interoperability, customization, and integration capabilities of your services.
c) Describe how your services can adapt to and grow with the needs of the State of North Carolina.
d) Describe the solution roadmap including a vision for the solution, high-level timeline, and description of how customer feedback is collected and incorporated into solution enhancements.

4) Experience and Key Personnel:
a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly

demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).

b) Describe the Vendor's qualifications to perform the services specified in the category.

5) Support and Maintenance:

a) Describe any ongoing support, warranty and/or training services provided to ensure effective and sustained use of your services.

ATTACHMENT J: SUBMITTAL CHECKLIST

The original proposal response should be organized and uploaded to Ariba Section 5.1 as *one consolidated document* as specified below:

Attachment J: Submittal Checklist		
Cover Letter		Optional
Table of Contents		Organize as specified below and **include page numbers**.
SECTION 1: General Response		
	☐ Signed Bid Execution Page	
	☐ Executed Addenda	
	☐ Attachment C: Description of Offeror (*Include NC HUB Certification Letter, if applicable*)	See Page 41
	☐ Attachment E: Vendor Certification Form (Include Proof of NC Secretary of State License to do Business in North Carolina)	See Page 44
	☐ Attachment F: Location of Workers Utilized by Vendors	See Page 45
	☐ Attachment H: Financial Review Forms	See Page 48
SECTION 2: Category Specific Responses		See Page 50
	Attachment I: Vendor's Responses to Category-Specific Specifications Sections ☐ **Category A: Security Program Assessment and Consulting Services** ☐ **Category B: Application Risk Assessment and Consulting Services** ☐ **Category C: Penetration Test and Security Assessment Services** ☐ **Category D: Security Incident Readiness and Response Services** ☐ **Category E: Vulnerability Management Services** ☐ **Category F: Network Security Services** ☐ **Category G: Security Awareness and Training Services** ☐ **Category H: Security Implementation and Integration Services** ☐ **Category I: Security Operations Services** ☐ **Category J: Governance, Risk, and Compliance Services** ☐ **Category K: Application Security Services** ☐ **Category L: DevSecOps and Security Automation Services** ☐ **Category M: Identity and Access Security Services** ☐ **Category N: Data Security Services** ☐ **Category O: Cloud Security Services** ☐ **Category P: Third-Party Risk Management Services** ☐ **Category Q: Mobile Security Services** ☐ **Category R: Critical Infrastructure and Operational Technology (OT) Security Services** ☐ **Category S: Endpoint Security Services**	

	(Specify the category letter and title for each category for which you are providing a response.) ***Each category proposal should be labeled as its own section and identified sequentially as indicated above.*** ***Organize each category proposal to include category specific responses to Attachment I, Attachment D and Attachment G.***	
	☐ **Attachment D: Cost Proposal Form(s) (subcategory-specific)** (Include the cost form for each category for which you are providing a response. You must complete all lines on the cost form for the category.	See Page 43
	☐ **Attachment G**: **References** (For each category - **Two (2)** Customer reference forms are required.	See Page 46
SECTION 3: VRARs and Original Bid Copy.		
	☐ **Vendor Readiness Assessment Reports (VRARs).**	See Page 10
	☐ All pages of the original bid document**.**	
SECTION 4: Redacted Bid, if applicable.		
The REDACTED proposal response should be organized in the same manner as the original proposal and uploaded to Ariba Section 5.5 as one consolidated document.		
	☐ **Redacted Bid Copy Upload to Ariba:** If Vendor answered Yes to the Ariba Confidential Information question then a bid copy with all confidential information, identified in the original bid, redacted, must be separately uploaded to **Ariba Section 5.5.**	