STATE OF NORTH CAROLINA **Department of Information Technology** **Statewide IT Procurement**	**REQUEST FOR PROPOSAL NO. ITS-500874-000**
	Offers will be publicly opened: **8/29/2024**
	Issue Date: **07/2/2024**
Refer ALL inquiries regarding this RFP to: Allison.howard@nc.gov	Commodity Number: **801015; 432332 & 432225**
	Description: Cybersecurity Products & Services
	Purchasing Agency: Department of Information Technology
	Requisition No.: **NA**

OFFER

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

EXECUTION

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

Failure to execute/sign offer prior to submittal shall render offer invalid. ***Late offers will not be accepted.***

OFFEROR:		
STREET ADDRESS/ P.O. BOX:		
CITY, STATE & ZIP:		TELEPHONE NUMBER:
PRINT NAME & TITLE OF PERSON SIGNING:		
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 Department of Information Technology 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	**7/2/2024**
Written Questions Deadline	Potential Vendors	**7/23/2024**
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	**8/6/2024**
Offer Opening Deadline	Vendors	**8/29/2024**
Contract Award	Agency	**TBD**
Protest Deadline	Responding Vendors	**15 days after award**

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The Department of Information Technology (NCDIT) is soliciting proposals for Cybersecurity Products and Services. This contract will consolidate the End Point Protection (208M), Tanium (208T), and Security Assessments (918A) contracts. Vendors currently awarded on those contracts **must** bid on this contract to continue providing cybersecurity services to the State of North Carolina.

Vendors currently on the 204X IT Infrastructure Solutions contract that offer products listed in this bid **must** submit proposals for those products.

NCDIT intends to move all cybersecurity products from the 204X IT Infrastructure Solutions contract to the new Cybersecurity contract to consolidate all security products into one contract.

This contract will also consolidate security assessment and testing professional services. This is not a staffing contract. Services procured using this contract must be Scope of Work (SOW) based.

Only time-limited, fixed priced, SOWs for professional services are allowed to be procured using this contract.

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

NCDIT may make multiple awards by subcategory of this RFP.

Interested vendors may submit proposals for one or more of the following bid categories. The North Carolina Department of Information Technology "NCDIT" will review and evaluate responses by category.

Contract award will be rolling by category.

CATEGORY SPECIFIC SCOPES OF WORK

Category A: Endpoint and Network Security Products

1. ANTI-VIRUS/MALWARE/ADWARE SOFTWARE
2. ENCRYPTION SOFTWARE AND HARDWARE
3. DATA LOSS PREVENTION (DLP) SOFTWARE
4. CLOUD SECURITY SOFTWARE AND TOOLS INCLUDING CLOUD ACCESS SECURITY BROKER (CASB) SOLUTIONS
5. VIRTUAL PRIVATE NETWORK (VPN) SOLUTIONS
6. MOBILE DEVICE MANAGEMENT (MDM)/ENTERPRISE MOBILITY MANAGEMENT (EMM) SOLUTIONS
7. ENDPOINT DETECTION AND RESPONSE (EDR), EXTENDED DETECTION AND RESPONSE (XDR), AND MANAGED DETECTION AND RESPONSE (MDR)

8. WEB APPLICATION FIREWALLS (WAF) AND EDGE PROXIES

Category B: Identity and Access Management Products

1. IDENTITY AND ACCESS MANAGEMENT (IAM) SOFTWARE SOLUTIONS AND HARDWARE DEVICES

Category C: Security Management and Analytics Products

1. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOFTWARE AND APPLIANCES
2. THREAT INTELLIGENCE SOFTWARE PLATFORMS AND HARDWARE SOLUTIONS
3. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)
4. SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM (SCADA) SOLUTIONS
5. SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) SOLUTIONS
6. BREACH AND ATTACK SIMULATION (BAS) SOLUTIONS
7. VULNERABILITY MANAGEMENT SOLUTIONS

Category D: Email Security Products

1. EMAIL SECURITY SOFTWARE SOLUTIONS AND APPLIANCES

Category E: Software Development Security Products

1. APPLICATION, CODE, AND SOFTWARE DEVELOPMENT SECURITY TESTING TOOLS

Category F: Security Assessment, Testing and Consulting Services

1. SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES
2. APPLICATION RISK ASSESSMENT AND CONSULTING SERVICES
3. PENETRATION TEST AND EMAIL SECURITY ASSESSMENT AND CONSULTING SERVICES
4. SECURITY INCIDENT READINESS ASSESSMENT AND CONSULTING SERVICES
5. INTERNAL VULNERABILITY ASSESSMENT AND CONSULTING SERVICES
6. NETWORK ARCHITECTURE ASSESSMENT AND CONSULTING SERVICES
7. CYBERSECURITY USER TRAINING AND AWARENESS PROGRAM
8. CYBERSECURITY SYSTEM IMPLEMENTATION AND INTEGRATION SERVICES
9. SECURITY INCIDENT RESPONSE CONSULTING SERVICES
10. SECURITY OPERATIONS CENTER AS A SERVICE (SOCaaS)
11. SECURITY POLICY DEVELOPMENT AND COMPLIANCE CONSULTING SERVICES
12. SECURE SOFTWARE DEVELOPMENT CONSULTING SERVICES
13. SECURE DEVOPS (DEVSECOPS) INTEGRATION SERVICES

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

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 this RFP response, NCDIT reserves the right to amend the Agreements awarded under this RFP to include new technologies or 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 SPECIFICATIONS. MARKETING MATERIALS WILL NOT BE ACCEPTED NOR EVALUATED.

2.2 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The initial contract term will be for five (5) years unless terminated earlier. The State retains the option to extend the Agreement for five (5) one (1) year periods at its sole discretion.

2.2.1 EFFECTIVE DATE

This solicitation, including any Exhibits, or any resulting contract or amendment(s) shall not become effective nor bind the State until the appropriate State purchasing authority, official or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for goods provided nor Services rendered prior to the appropriate signatures and

the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.3 CONTRACT TYPE

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; and 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 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 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.

Vendor shall be the Original Equipment Manufacturer of the product proposed in its offer, or the Original Equipment Manufacturer's single authorized representative of the equipment proposed in its offer, ***for all categories with the exception of the Category F: Security Assessment Testing and Consulting category***.

Original Equipment Manufacturer vendors are permitted to include third parties, subcontractors, and partners to deliver the goods and services of this RFP to Agencies during the contract period.

However, the Original Equipment Manufacturer's single authorized representative will not be allowed to include third parties, subcontractors, and partners to further deliver the goods and services of this RFP.

2.4 MINIMUM SALES VOLUME

Vendor shall provide in its offer evidence of recent sales of cybersecurity products and/or services, as applicable, that are within the scope of this RFP.

Original Equipment Manufacturers (OEM) or the OEM's Single Authorized Representative bidding in Categories A through E, shall provide evidence of a minimum sales volume of $50,000,000.00 (USD) of cybersecurity products and/or services within the scope of this RFP to customers in the United States for each of the past two (2), 2022 and 2023, calendar years.

Vendors submitting offer for services in Category F: Security Assessment, Testing and Consulting Services shall provide evidence of a minimum sales volume of $2,000,000.00 (USD) of cybersecurity services within the scope of this RFP to customers in the United States for each of the past two (2), 2022 and 2023, calendar years.

Vendor shall provide their yearly sales data for each of the past two (2), 2022 and 2023, calendar years) in the space provided in **Attachment C** along with supporting sales documentation.

2.5 AGENCY BACKGROUND

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 projects 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.

2.6 PROBLEM STATEMENT

NCDIT recognizes the critical importance of robust cybersecurity measures to protect the state's digital infrastructure and the sensitive data of the state's citizens. Currently, state agencies and entities require a diverse range of cybersecurity products and services to address their unique security challenges. The objective of this RFP is to establish a single, flexible procurement source that can comprehensively meet the evolving cybersecurity needs of the state by encompassing and providing a variety of cybersecurity products and services. Vendors are not required to provide offers for every product or service category.

To ensure the contract remains current and inclusive of the latest cybersecurity advancements, the state may, in its discretion, periodically conduct open enrollment of the contract for the consideration of new vendors and the expansion of offerings by existing vendors.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.1.1 REQUIREMENTS

Means, as used herein, a function, feature, or performance that the system must provide.

3.1.2 SPECIFICATIONS

Means, as used herein, a specification 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

Vendors offering both solutions hosted and not hosted on state infrastructure will be required to provide both types of VRARs.

The state reserves the right to request VRARs from Vendors at offer submittal and during the contract term as the state deems necessary.

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**

The Cybersecurity Products and Services contract will be required to receive and securely manage data that is classified up to and including High Risk**.** 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.

3.2.2 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

Vendors shall provide a completed VRAR - Vendor Readiness Assessment Report Not State Hosted Solutions at offer submission, which includes cloud. This report is located at the following website: **https://it.nc.gov/documents/vendor-readiness-assessment-report.**

Cybersecurity Products and Services may be required to receive and securely manage data that is classified as Statewide Critical. 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 policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls.

This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, or ISO 27001 are required for any cloud service providing support for data classified as Restricted or Highly Restricted.

The Cybersecurity Products and Services contract will be required to receive and securely manage data that is classified as up to and including High Risk. Refer to the North Carolina Statewide Data Classification and Handling policy for more information regarding 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. This requirement additionally applies to all Vendor-provided, agency-managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted) data.

(a) Vendors shall provide a completed Vendor Readiness Assessment Report Non-State Hosted Solutions ("VRAR") at offer submission. This report is located at the following website: **https://it.nc.gov/documents/vendor-readiness-assessment-report**

(b) Upon request, Vendors shall provide a current independent 3rd party assessment report in accordance with the following subparagraphs (i)-(iii) prior to contract award. However, Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(iii) at the time of offer submission.

(i) Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, ISO 27001, or HITRUST are the preferred assessment reports for any Vendor solutions which will handle data classified as Medium Risk (Restricted) or High Risk (Highly Restricted).

(ii) A Vendor that cannot provide a preferred independent 3rd party assessment report as described above may submit an alternative assessment, such as a SOC 2 Type 1 assessment report. The Vendor shall provide an explanation for submitting the alternative assessment report. *The State reserves the right to determine if an alternative 3rd party assessment is acceptable*. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract. Timely submission of this preferred assessment report shall be a material requirement of the contract.

(iii) An IaaS vendor cannot provide a certification or assessment report for a SaaS provider UNLESS permitted by the terms of a written agreement between the two vendors and the scope of the IaaS certification or assessment report clearly includes the SaaS solution.

(c) Additional Security Documentation. Prior to contract award, the State may in its discretion require the Vendor to provide additional security documentation, including but not limited to vulnerability assessment reports and penetration test reports. The awarded Vendor shall provide such additional security documentation upon request by the State during the term of the contract.

3.3 ENTERPRISE REQUIREMENTS AND SPECIFICATIONS

3.3.1 ARCHITECTURE DIAGRAMS

The State utilizes Network Architecture and Technology Stack diagrams to better understand the design and technologies of a proposed solution. Details on these diagrams can be found at the following link: **https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192**

If Vendor is providing software or SaaS products, describe or diagram, both the Network Architecture and Technology Stack for the offered Software or SaaS products.

Additional architectural diagrams may be requested after contract award.

See Attachment I: Scope of Work and Specifications for applicable categories.

3.3.2 SOLUTION ROADMAP

A Solution Roadmap defines the vision and strategic elements of the solution. The Solution Roadmap is a plan of action for how a Solution will evolve over time. The minimum content should include:

- Vision for the solution;
- High-level functionality expected for each solution release into production environment;
- High-level timeline; and
- Description of how customer feedback is collected and incorporated into solution enhancements.

Describe the solution roadmap for your product. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned.

See Attachment I: Scope of Work and Specifications for applicable categories.

3.3.3 IDENTITY AND ACCESS MANAGEMENT

The proposed solution must externalize identity and access management. The protocols describing the State's Identity and Access Management can be found at the following link: **https://it.nc.gov/services/vendor-engagement-resources#Tab-IdentityAccessManagement-1241**

The state reserves the right to request additional information at the time of award or thereafter.

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

If Vendor is providing SaaS products, describe how the proposed products comply with industry accessibility standards.

Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

Standards include:

- W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: **https://www.w3.org/TR/WCAG21/**
- Section 508: **https://www.section508.gov/**
- Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

See Attachment I: Scope of Work and Specifications for applicable categories.

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 Vendors providing the Best Value and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when 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 the 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 of any specification may be grounds for rejection.
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 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 Order of Importance.

1) How well the Vendor's offer conforms with the specifications.
2) How each Vendor's offer compares with other Vendors' offers.
3) Total Cost of Ownership.
4) Strength of references (Category F: Security Assessment, Testing and Consulting Services**)**
5) Maturity of Product or the Company.

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 Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of Vendors' respective offers to determine Vendor awards.

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

5.5 PAST PERFORMANCE

The Vendor may be disqualified from any evaluation or award if the Vendor or any key personnel proposed, has 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 their ability that the recommended approach is not

short lived. Several approaches may exist for hardware configurations, other products and any software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

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

a) waive any formality;

b) amend the solicitation;

c) cancel or terminate this RFP;

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

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

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

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

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

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

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

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. 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 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 NC E-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.

Vendor is and shall remain responsible for paying the transaction fee on behalf of its authorized reseller in the event that the authorized reseller defaults.

6.1.6 ELECTRONIC VENDOR PORTAL (EVP)

The State has implemented the electronic Vendor Portal (eVP) that allow the public to retrieve award notices and information on the Internet at **https://evp.nc.gov**. Results may be found by searching the Solicitation Number or 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 SITE VISIT OR PRE-OFFER CONFERENCE RESERVED.

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 provided email address. 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 the Vendor's offer.

Written questions concerning this Solicitation will be received until **July 23, 2024 at 2:00 pm** Eastern Time.

They must be submitted to the contact person listed on Page One of this Solicitation via **allison.howard@nc.gov**. Please enter "Questions Solicitation XXXX" 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 Ariba Sourcing Tool.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State's Ariba Sourcing Tool for 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

Any errata or exceptions to the State's requirements and specifications may be presented on a separate page labeled "Exceptions to Requirements and Specifications". Include references to the corresponding requirements and specifications of the Solicitation. Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.** If a vendor materially deviates from RFP requirements or specifications, its offer may be determined to be non-responsive by the State.

Exceptions taken to Attachment B: Department of Information Technology Terms and Conditions, Section 3: Terms and Conditions Applicable to Personnel and Personal Services will make your offer non-responsive.

Offers conditioned upon acceptance of Vendor Errata or Exceptions will be determined to be non-responsive by the State.

If negotiations are required, Vendors must provide all license agreement documents in Microsoft Word format.

Vendors must also provide the name, title, email address and telephone number of the attorney that will be directly involved in the negotiations. The state will not negotiate license agreements with non-legal Vendor staff.

A contract award under this RFP is subject to successful license agreement(s) and state contract terms and conditions negotiations.

NCDIT, at its sole discretion, will determine when negotiations with a Vendor have become unproductive and when unproductive negotiations will result in discontinuance of the Vendor being considered for contract award.

6.2.6 ALTERNATE OFFERS

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

Alternate offers must be submitted in a separate document and clearly marked "Alternate Offer for 'name of Vendor'" and numbered sequentially with the first offer if separate offers are submitted.

6.2.7 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.8 BASIS FOR REJECTION

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

6.2.9 NON-RESPONSIVE OFFERS

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

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

6.2.10 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. 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.**

6.2.12 VENDOR POINTS OF CONTACT

CONTACTS AFTER CONTRACT AWARD:

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

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

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

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

a) Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.

b) Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.

c) Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.

d) Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.

e) Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.

f) Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.

g) **Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not 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 or 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 K: RFP Submittal.

6.3.3 OFFER SUBMITTAL

Due Date: **August 29, 2024**

Time: **2:00 PM** Eastern Time

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

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

Sealed offers, subject to the conditions made a part hereof, will be received until 2:00pm 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 SHALL 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: **WS1121785836**.
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, .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 shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (Attachment I), and 2) copies of Financial Statements as further described hereinbelow. **As used herein, Financial Statements shall exclude tax returns and compiled statements.**

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

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

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

Complete ATTACHMENT H – Financial Review Form.

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

7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS

Vendor should provide its license or support agreements for review and evaluation. Terms offered for Vendors' proprietary assets, such as software licensing/access grants and use restrictions, maintenance and support for licensed products or software, intellectual property rights, and warranties will be considered for acceptance by the State.

A Single Authorized Representative bidding for an Original Equipment Manufacturer should provide the OEM's license or support agreements referenced in the above paragraph, as well as the name, phone number, and email address for the OEM's legal contact authorized to negotiate the End User License and support agreements.

Other terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP as determined by the State. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees, interest, audit costs or other similar costs. Vendor provisions on these topics, as well as Vendor provisions excluding from liability damages such as, but not limited to, indirect, incidental, special, punitive, or consequential damages, shall have no force or effect.

7.5 ORIGINAL EQUIPMENT MANUFACTURER'S ("OEM") USE OF A SINGLE AUTHORIZED REPRESENTATIVE

An Original Equipment Manufacturer ("OEM") of the product line(s) offered herein can elect to have its Single Authorized Representative ("Representative") bid in its stead.

a. If an OEM elects to have a Representative submit an offer to this RFP, then the Representative submitting the offer shall include with its offer a written, dated, within thirty (30) dates of original bid opening, statement on the OEM's letterhead, addressed to the State of North Carolina Department of Information Technology, and signed by an individual authorized to bind the OEM, that stipulates:

    1. That the Representative submitting the offer is the OEM's Single Authorized Representative of the product lines within the scope of this RFP.

    2. That the OEM will support the specifications and requirements of the contract for the duration of the contract, acknowledging that the Representative submitting the offer bears sole performance responsibility as established by the Prime Vendor concept in Attachment B: Department of Information Technology Terms and Conditions, Section 3: Terms and Conditions Applicable to Personnel and Personal Services, Paragraph 1, Vendor's Representation of this RFP. This includes the OEM's commitment to supporting the Representative submitting the offer if successful by providing the OEM's products in a timely manner and in quantities necessary for the Representative submitting the offer to fulfill the requirements of the contract.

    3. That the warranty services will be provided to Agencies on OEM's product lines included in Representative's offer.

    4. That the OEM intends to maintain and publish the established method of pricing (U.S. MSRP or Price List) for the duration of this contract and will make such information available to NCDIT and Agencies, if requested.

    5. That the OEM agrees to negotiate its license or support agreements with the State since the Representative lacks the authority to negotiate the OEM's agreements and/or to bind the OEM.

b. If an OEM's Single Authorized Representative is selected for award, then the contract resulting from this RFP will be an Agreement between the Single Authorized Representative and the State. The Single Authorized Representative is prohibited from adding resellers to this Agreement.

7.6 USE OF RESELLERS/DISTRIBUTORS

The State will allow awarded OEMs to utilize approved, designated Resellers to participate as alternate distribution sources for the Vendor(s). Such participation is subject to the following conditions:

a. Order Placement: Vendor shall specify whether orders must be placed directly with the Vendor or may be placed directly with designated Reseller(s). If Resellers are designated to fulfill orders, Vendor shall provide the State with all necessary ordering and contact information and ensure that the Reseller(s). Reseller(s) shall be registered to receive purchase orders through the State E-Procurement system and be current on all E-Procurement fees.

b. Conditions of Participation: Reseller(s) shall be approved in advance by the State as a condition of eligibility under this section. The State also reserves the right to rescind any such participation or request additional Resellers be named at the State's discretion.

c. Number of Designated Resellers: The State reserves the right to limit the number of Resellers per Original Equipment Manufacturer who are authorized under the awarded contract. At this time, the State will accept a maximum of five (5) authorized Resellers per Original Equipment Manufacturer. The Original Equipment Manufacturer may also be on the statewide term contract in addition to their five (5) authorized Resellers.

d. Responsibility for Performance and Reporting: Vendor shall be fully liable for Reseller's performance and compliance with all contract terms and conditions. Products purchased through Reseller(s) must be consolidated and reported **by Vendor** in the required format below.

e. Product: Product ordered directly through Reseller(s) shall be only products previously approved under this contract and shall be subject to all terms and conditions of this contract. At no time can a Reseller's price exceed the published contract price.

7.7 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; delivery, condition of delivered goods, specification compliance of delivered goods or 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 the framework of 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.

Vendor 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. Report shall include the following data elements at a minimum:

Sale Date	PO #	Distributor/ Reseller	Agency Type	Agency Name	Manu Name	Item Desc.	Quantity	Unit List Price	Unit Sales Price	Total Sales Price

In the future Vendors may be required to provide sales reports electronically using an accessible state portal.

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

7.8 ABNORMAL QUANTITY REQUESTS

During the term of the contract, the State reserves the right to request additional discounts (beyond the awarded contract discount percentage) from Vendors for any order or combined orders that exceed the Abnormal Quantity Threshold Amount for this contract. The State will determine the Abnormal Quantity Threshold Amount after award. The State reserves the right to adjust the Abnormal Quantity Threshold Amount at any time during the contract. Further, the State, at its sole discretion, may choose to issue a Request for Quote to awarded Vendors or to issue a separate Invitation for Bid for the order.

7.9 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.

7.10 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a twenty five percent (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.

7.11 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.

7.12 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.

7.13 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.

7.14 PROJECT MANAGEMENT RESERVED.

7.15 MEETINGS RESERVED.

7.16 RECYCLING AND SOURCE REDUCTION

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

7.17 SPECIAL TERMS AND CONDITIONS RESERVED.

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, SaaS 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) **Original Equipment Manufacturer (OEM)**: Original Equipment Manufacturer means a company that, as its primary business function, designs, assembles, owns the trademark/patent and markets cybersecurity hardware, software or SaaS products. The Original Equipment Manufacturer's name shall appear on the cybersecurity products.

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

9) **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.

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

11) **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.

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

13) Small as used in Attachment D: Category Cost Forms, Category F: **Security Assessment, Testing and Consulting Services** means an entity with less than fifty (50) endpoints.

14) Medium as used in Attachment D: Category Cost Forms, Category F: **Security Assessment, Testing and Consulting Services** means an entity with fifty-one (51) to five hundred (500) endpoints.

15) Large as used in Attachment D: Category Cost Forms, Category F: **Security Assessment, Testing and Consulting Services** means an entity with five hundred one (501) to fifteen hundred (1,500) endpoints.

16) Enterprise as used in Attachment D: Category Cost Forms, Category F: **Security Assessment, Testing and Consulting Services** 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, or Section 7(c) of the Software as a Service terms, 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. With respect to Software as a Service (SaaS), Services shall also include, without limitation, providing web browser access by authorized users to Vendor online software applications identified herein, and to related services, such as vendor hosted computer storage, databases, Support, documentation, and other functionalities.

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

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

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

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

5) **TRAVEL EXPENSES: All travel expenses should be included in the Vendor's proposed 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 7) Acceptance Process (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. Payments are subject to any retainage requirements in the Agreement. 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.

a) Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:

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

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

iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.

b) For any third-party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.

c) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software, Deliverables, or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services and Deliverables provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.

d) The Purchasing State Agency shall release any amounts held as retainages for Services or Deliverables completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services or Deliverables identified or associated with such invoices.

e) **Supplemental Payment Terms Applicable to Software as a Service**. Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Initial payments are to be made after

final acceptance of the Services. Subscription fees for term years after the initial year shall be as quoted under State options herein but shall not increase more that 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing.

f) **Supplemental Invoicing and Payment Terms Applicable to Software and Software Support Service:** The total License Fee and the Support Service or Maintenance Fee (if applicable and provided the State subscribes or purchases such Services) for the first year shall be invoiced upon delivery of the Software. The Support Service or Maintenance Fee for subsequent contract years, if any, will be invoiced annually sixty (60) days prior to the anniversary date beginning each subsequent year. Increases in pricing for Support Services or Maintenance shall not exceed five percent (5%) per year following the first Contract year. Payment terms for Support Services are due and payable the month following the month for which charges accrue, or in accordance with the contract payment schedule.

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 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;

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);

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;

d) **Cyber Insurance Errors & Omission** - The Vendor shall provide and maintain Cyber Insurance for Cloud and SaaS product offerings which shall include but is not limited to the following: (i) Coverage for unauthorized access to and unauthorized use of computer systems. (ii) Coverage for regulatory proceedings alleging violation of privacy laws, whether common law or statutory law. (iii) Coverage for business interruption and extra expense caused by a cyber event. This may be met through a standalone policy or included as a component in a Commercial General Liability Policy. Not less than $2,000,000 for each occurrence. The State reserves the right to request higher minimum limits for cybersecurity insurance for procurement requests or SOWs that may interact with sensitive data such as personally identifiable information (PII); and

e) 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) consecutively 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/Services 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/Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables/Services. 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/Services, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.

b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract. The value of the contract is defined as two times the value of the purchase order for the equipment, software, SaaS or two times the value of Statement of Work (SOW), whichever is applicable.

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, 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 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. Vendor is and shall remain responsible for paying the transaction fee(s) on behalf of its authorized reseller in the event that the authorized reseller or sole authorized representative of an original equipment manufacturer defaults.

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 noninfringing and continue to meet

procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.

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

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

40) <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 or Software 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 the Software or for access to the Services. All terms and conditions of any clickwrap agreement provided with any Software or 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 Software or Services.

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

1) **SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:** Deliverables comprising goods, equipment or products (hardware) may contain software for internal operation, or as embedded software or firmware that is generally not sold or licensed as a severable software product. Software may be provided on separate media, such as a CD-ROM or other media, or may be included within the hardware at or prior to delivery. Such software is proprietary, copyrighted, and may also contain valuable trade secrets and may be protected by patents. Vendor grants the State a license to use the Code (or any replacement provided) on, or in conjunction with, only the Deliverables purchased, or with any system identified in the solicitation documents. The State shall have a worldwide, nonexclusive, non-sublicensable license to use such software and/or documentation for its internal use. The State may make and install copies of the software to support the authorized level of use. Provided, however that if the hardware is inoperable, the software may be copied for temporary use on other hardware. The State shall promptly affix to any such copy the same proprietary and copyright notices affixed to the original. The State may make one copy of the software for archival, back-up or disaster recovery purposes. The license set forth in this Paragraph shall terminate immediately upon the State's discontinuance of the use of all equipment on which the software is installed. The software may be transferred to another party only with the transfer of the hardware. If the hardware is transferred, the State shall i) destroy all software copies made by the State, ii) deliver the original or any replacement copies of the software to the transferee, and iii) notify the transferee that title and ownership of the software and the applicable patent, trademark, copyright, and other intellectual property rights shall remain with Vendor, or Vendor's licensors. The State shall not disassemble, decompile, reverse engineer, modify, or prepare derivative works of the embedded software, unless permitted under the solicitation documents.
2) **LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):** This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:
   a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Statement of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful customers. This license shall be perpetual or for the term of the contract (pick one, delete the other), unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.
   b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.
   c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.
   d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.
3) **WARRANTY TERMS:** Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.

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

b) Vendor warrants to the best of its knowledge that:
   i) The licensed Software and associated materials do not infringe any intellectual property rights of any third-party;
   ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third-party;
   iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
   iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.

c) UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.

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

a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.

b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.

c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.

d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

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

a) **Error Correction:** If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.

b) **Other Agreement**: This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein

c) **Temporary Extension of License**: If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
   i) Return of the inoperative CPU to full operation, or
   ii) Termination of the license.

d) **Encryption Code:** Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.

e) **Updates:** Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.

f) **Telephone Assistance:** Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 8:00 AM - 5:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) hours or eight (8) hours or next business day, etc. for calls made at any time

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

SECTION 3: TERMS AND CONDITIONS APPLICABLE TO PERSONNEL AND PERSONAL SERVICES

Exceptions taken to this section's terms and conditions applicable to personnel and personal services will make your offer non-responsive.

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 Services as specified in a Statement of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's Category F: Security Assessment, Testing and Consulting Services and/or use of one or more Software or SaaS Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement").
3) **PERSONNEL:** Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be noticed to the Agency's Contract Administrator in writing accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.
   a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment,

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

b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular workdays and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.

c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
   i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
   ii) Such use does not conflict with any procurement law, regulation or policy, or
   iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.

d) 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: The State shall have and retain the right to obtain personal Services of any individuals providing Services under the Agreement. This right may be exercised at the State's discretion in the event of any transfer of the person providing personal Services, termination, default, merger, acquisition, bankruptcy or receivership of the Vendor to ensure continuity of Services provided under the Agreement. Provided, however, that the Agency shall not retain or solicit any Vendor employee for purposes other than completion of personal Services due as all or part of any performance due under the Agreement.

a) Vendor personnel shall perform any 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.

b) The State has and reserves the right to disapprove the continuing assignment of Vendor personnel provided by Vendor under the Agreement. If this right is exercised and the Vendor is not able to replace the disapproved personnel as required by the State, the parties agree to employ best commercial efforts to informally resolve such failure equitably by adjustment of other duties, set-off, or modification to other terms that may be affected by Vendor's failure.

c) Vendor will make every reasonable effort consistent with prevailing business practices to honor the specific requests of the State regarding assignment of Vendor's employees. Vendor reserves the sole right to determine the assignment of its employees. If one of Vendor's employees is unable to perform due to illness, resignation, or other factors beyond Vendor's control, Vendor will provide suitable personnel at no additional cost to the State.

d) 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.

SECTION 4: TERMS AND CONDITIONS APPLICABLE TO SOFTWARE AS A SERVICE

1) DEFINITIONS:

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

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

2) ACCESS AND USE OF SAAS SERVICES:

a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so- called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq*.

b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.

c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.

e) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.

f) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.

g) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.

h) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.

3) <u>WARRANTY OF NON-INFRINGEMENT; REMEDIES</u>:

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

b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become non-infringing. If neither of these options can reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

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 supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. 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.

d) 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 results from the State's material alteration of any Vendor-

branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) <u>ACCESS AVAILABILITY; REMEDIES</u>:

a) The Vendor warrants that the Services will be in good working order and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.

b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State.

If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:

1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve- month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10% service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) <u>EXCLUSIONS</u>:

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

b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:

i) Actions of non-Vendor personnel;
ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
iii) Force Majeure conditions set forth hereinbelow.
iv) The State's sole misuse of, or its own inability to use, the Services.

6) <u>PERFORMANCE REVIEW AND ACCOUNTABILITY</u>: **RESERVED.**

7) <u>MODIFICATION OF SERVICES</u>: If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to

receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.

8) TRANSITION PERIOD:

a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").

b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.

c) During the Transition Period, Services access shall continue to be made available to the State without alteration.

d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.

e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.

f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.

9) ACCEPTANCE CRITERIA:

a) Initial acceptance testing is required for all Vendor supplied Services before going live, 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 technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.

b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

10) SECURITY OF STATE DATA:

a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at the State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance

with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.

c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy **https://it.nc.gov/documents/statewide-data-classification-and-handling-policy** that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.

d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.

e) The Vendor shall certify to the State:
   i) The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
   ii) That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security control appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4The State reserves the right to independently evaluate, audit, and verify such requirements.
   iii) That the Services will comply with the following;
      (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
         (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
         (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;

(2) Privacy provisions of the Federal Privacy Act of 1974;
(3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75- 65 and -66);
(4) The North Carolina Public Records Act, N.C.G.S. Chapter 132;
(5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA); and
(6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.

f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60 et. seq.) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.

g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.

h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6)

costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.

j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.

k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.

l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.

m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:

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

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

n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n), Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

o) Secure Data Disposal. When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

11) **ACCESS TO PERSONS AND RECORDS**: The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.

SECTION 5: Supplemental TERMS AND CONDITIONS APPLICABLE TO ARTIFICAL INTELLIGENCE ("AI")

The following terms ("**AI Terms**") are hereby added to and become part of the Agreement as Additional Terms. Capitalized terms not defined in these AI Terms have the meanings given in the Agreement.

Definitions:

"AI Features" means large language models (LLMs) or other machine learning (ML) or artificial intelligence (AI) features of the Software or Service. AI Features may include or be in addition to AI Tools.

"AI Tools" means any and all deep learning, machine learning, and other artificial intelligence technologies, including any and all (i) algorithms, heuristics, models, and methodologies, whether in source code, object code, human readable form or other form, (ii) proprietary algorithms, software or other IT Systems that make use of or employ expert systems, natural language processing, computer vision, automated speech recognition, automated planning and scheduling, neural networks, statistical learning algorithms (like linear and logistic regression, support vector machines, random forests, k-means clustering), or reinforcement learning, and (iii) proprietary embodied artificial intelligence and related hardware or equipment.

1) 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 Features or AI Tools (or depends in any way upon any AI Features or AI Tools), including without limitation, any collection or processing of any the State's Data using any AI Features or AI Tools.

2) AI Warranties. With respect to all AI Features or AI Tools (collectively "AI") described by the Vendor and approved for use by the State, Vendor warrants that:

(a) Vendor has accurately identified and fully described all AI for use by the State;
(b) the AI will (i) perform with a high degree of accuracy in accordance with the Specifications and (ii) not produce materially inaccurate results when used in accordance with the Documentation.
(c) Vendor will monitor the performance of the AI to ensure continued accuracy in accordance with the Specifications, including processes and policies for the regular assessment and validation of the AI's outputs.
(d) Vendor has obtained, and is in compliance with, all rights and licenses necessary to use all AI as described in Vendor's proposal;
(e) Vendor has complied with all the Laws and industry standards applicable to (i) Vendor's development and provision of all AI as described in Vendor's proposal and (ii) the State's use of all AI as described in the Vendor's proposal;
(f) 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.
(g) Vendor will comply with all State policies and procedures relating to the use of AI;
(h) Vendor will notify Customer at least sixty (60) days prior to any material changes pertaining to the AI (in whole or in part);
(i) 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;
(j) 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;
(k) there have been no interruptions in use of Vendor's AI in the past six (6) months;
(l) 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;

(m) Vendor maintains or adheres to industry standard policies 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;

(ii) identifying and mitigating bias in training data or in the algorithmic model used in AI Tools, 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");

(n) 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, 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.

3) Use of AI. The State may submit Data (including in the form of prompts or queries) to the AI ("Inputs") and receive outputs from the AI ("Outputs").

4) Training. Vendor may not use Inputs or Outputs to train or otherwise improve AI Features, except solely for the benefit of the State. Notwithstanding the foregoing, Vendor may use Inputs or Outputs to train or otherwise improve the AI Features, 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".

5) Intellectual Property:

(a) Inputs**.** Except for Vendor's express rights in the Agreement, as between the parties, the State owns Inputs as the State's Data and retains all intellectual property and other rights in the Inputs.

(b) Outputs. Outputs are deemed to be State Data, subject to these AI Terms.

6) 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.

7) Special Restrictions on Use of AI Features. The State will not and will not permit anyone else to:

(a) use the AI Features or any Output to infringe any third-party rights,

(b) use the AI Features or any Output to develop, train or improve any AI or ML models (separate from authorized use of the Software or Services under this Agreement),

(c) represent any Output as being approved or vetted by Vendor,
(d) represent any Output as being an original work or a wholly human-generated work,
(e) use the AI Features for automated decision-making that has legal or similarly significant effects on individuals, unless it does so with adequate human review and in compliance with laws applicable to the State, or
(f) use the AI Features for purposes or with effects that are discriminatory, harassing, harmful or unethical.

8) 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.

9) Updates. Vendor's AI has a data cutoff date of _____ **[Fill in date]**. The State has the right to receive updates to the dataset, notification of those updates, and delivery of those updates made generally available to Vendor's Customers receiving similar AI Services.

10) 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 information about the offeror.

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

Title Email address and Telephone Number	
2022 Sales Volume **(Attach supporting sales documentation)**	$
2023 Sales Volume **(Attach supporting sales documentation)**	$

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 Yes, state HUB classification and provide a copy of Vendor's North Carolina HUB Certification Letter:

_____

ATTACHMENT D: CATEGORY COST FORMS

Category A: Endpoint and Network Security Products

			% Discount off List	Unit of Measure	Additional Information	
1.	ANTI-VIRUS/MALWARE/ ADWARE SOFTWARE	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
2.	ENCRYPTION SOFTWARE AND HARDWARE	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
3.	DATA LOSS PREVENTION (DLP) SOFTWARE	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
4.	CLOUD SECURITY SOFTWARE AND TOOLS INCLUDING CLOUD ACCESS SECURITY BROKER CASB) SOLUTIONS	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
5.	VIRTUAL PRIVATE NETWORK (VPN) SOLUTIONS	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
6.	MOBILE DEVICE MANAGEMENT (MDM)/ ENTERPRISE MOBILITY MANAGEMENT (EMM) SOLUTIONS	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				
7.	ENDPOINT DETECTION AND RESPONSE (EDR), EXTENDED DETECTION AND RESPONSE (XDR), AND MANAGED DETECTION AND RESPONSE (MDR)	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				

ATTACHMENT D: CATEGORY COST FORMS

Category A: Endpoint and Network Security Products						
			% Discount off List	**Unit of Measure**	**Additional Information**	
8.	**WEB APPLICATION FIREWALLS (WAF) AND EDGE PROXIES**	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				

ATTACHMENT D: CATEGORY COST FORMS

Category B: Identity and Access Management Products

			% Discount off List	Unit of Measure	Additional Information	
1.	**IDENTITY AND ACCESS MANAGEMENT (IAM) SOFTWARE SOLUTIONS AND HARDWARE DEVICES**	Cloud Subscription/License Fee				
		Customization/Installation/Transition				
		Technical & User Documentation				
		Training				
		Maintenance				
		Technical Support/Customer Service				
		Hardware				
		Other Costs (Describe)				

ATTACHMENT D: CATEGORY COST FORMS

Category C: Security Management and Analytics Products

			% Discount off List	Unit of Measure	Additional Information
1.	**SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOFTWARE AND APPLIANCES**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
2.	**THREAT INTELLIGENCE SOFTWARE PLATFORMS AND HARDWARE SOLUTIONS**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
3.	**INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
4.	**SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM (SCADA) SOLUTIONS**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
5.	**SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) SOLUTIONS**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
6.	**BREACH AND ATTACK**	Cloud Subscription/License Fee			
	SIMULATION (BAS) SOLUTIONS	Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			
7.	**VULNERABILITY MANAGEMENT**	Cloud Subscription/License Fee			
	SOLUTIONS	Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			

ATTACHMENT D: CATEGORY COST FORMS

Category D: Email Security Products

			% Discount off List	Unit of Measure	Additional Information
1.	**EMAIL SECURITY SOFTWARE SOLUTIONS AND APPLIANCES**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			

ATTACHMENT D: CATEGORY COST FORMS

Category E: Software Development Security Products

			% Discount off List	Unit of Measure	Additional Information
1.	**APPLICATION CODE, AND SOFTWARE DEVELOPMENT SECURITY TESTING TOOLS**	Cloud Subscription/License Fee			
		Customization/Installation/Transition			
		Technical & User Documentation			
		Training			
		Maintenance			
		Technical Support/Customer Service			
		Hardware			
		Other Costs (Describe)			

ATTACHMENT D: CATEGORY COST FORMS

Category F: Security Assessment, Testing and Consulting Services

		Public Entity*	NTE Hourly Rate	Additional Information		
1.	SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
2.	APPLICATION RISK ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
3.	PENETRATION TEST AND EMAIL SECURITY ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
4.	SECURITY INCIDENT READINESS ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
5.	INTERNAL VULNERABILITY ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
6.	NETWORK ARCHITECTURE ASSESSMENT AND CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
7.	CYBERSECURITY USER TRAINING AND AWARENESS PROGRAM					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
8.	CYBERSECURITY SYSTEM IMPLEMENTATION AND INTEGRATION SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				

***Fixed price. Travel must be included in pricing.**

****Entity Size: Small Entity (Less than 50 End Points); Medium Entity (50-500 End Points); Large Entity (501-1500 End Points; Enterprise Entity (1500+ End Points).**

ATTACHMENT D: CATEGORY COST FORMS

Category F: Security Assessment, Testing and Consulting Services

		Public Entity*	NTE Hourly Rate	Additional Information		
9	SECURITY INCIDENT RESPONSE CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
10.	SECURITY OPERATIONS CENTER AS A SERVICE (SOCaaS)					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
11.	SECURITY POLICY DEVELOPMENT AND COMPLIANCE CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
12.	SECURE SOFTWARE DEVELOPMENT CONSULTING SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				
13.	SECURE DEVOPS (DEVSECOPS) INTEGRATION SERVICES					
		Small				
		Medium				
		Large				
		X-Large/Enterprise				

***Fixed price. Travel must be included in pricing.**

****Entity Size: Small Entity (Less than 50 End Points); Medium Entity (50-500 End Points); Large Entity (501-1500 End Points; 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, Vendor must register with the North Carolina Secretary of State before contract award and Vendor must 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, please list the countries: _____

For each country, please list and describe the type of work performed and who is performing the work (i.e., Vendor's employees, subcontractors, or other persons)(use additional lines as necessary):

_____

_____

_____

ATTACHMENT G: REFERENCES

CUSTOMER REFERENCE FORM
(CATEGORY F: SECURITY ASSESSMENT, TESTING AND CONSULTING SERVICES)

Vendor Name:	
CATEGORY/SUBCATEGORY	

Vendor shall submit **two (2)** different customer references (**per subcategory**) using this form. Vendors should copy this form as required to meet the reference submission requirements (one form per reference).

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 provided reference contact should have been in a leadership role in the project at the functional and/or technical levels. References should be recent, i.e. for work performed within the past three (3) years.

You may use the same reference for more than one subcategory, if appropriate and applicable, but *do not use a reference more than once within the same subcategory*. 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.

Note: References will initially be evaluated based solely on the information provided in this form and will be part of the "Experience and Qualifications" evaluation criteria. Responses should be detailed and are not limited in size. Use additional pages if necessary to provide a complete and detailed response.

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.

Vendor evaluations will not be considered complete until two (2) complete references are returned to the state by the named references. Vendors without two completed and returned references will not be considered for contract award.

The state will notify the Vendor if any of the Vendor's customer references do not respond to the state's reference check request. 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.

Failure of Vendor to provide the requested reference(s) or failure of Vendor's customer to complete and return the reference form will result in the termination of Vendor's consideration 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 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 change orders required? If so, how many? Please explain.	
Was training provided? If yes, please describe the length, type, and format.	
Did you provide any software tools to the customer? If so, what?	
List all subcontractors, if any, who participated in the project(s), including the extent of their participation.	

Please provide a detailed description of all service provided, including any hardware or software that may have been involved.	

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**.

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. INTRODUCTION

The Department of Information Technology (NCDIT) is soliciting proposals for cybersecurity products and services.

This contract will consolidate the End Point Protection (208M), Tanium (208T), Security Assessments (918A) contracts. Vendors currently awarded on those contracts should bid on this contract to continue providing cybersecurity services to the State of North Carolina.

Vendors currently on the 204X IT Infrastructure Solutions contract that offer products listed in this bid **must** submit proposals for those products.

NCDIT intends to move all cybersecurity products from the 204X IT Infrastructure Solutions contract to the new Cybersecurity contract to consolidate all security products into one contract.

This contract will also consolidate security assessment and testing professional services. This is not a staffing contract. Services procured using this contract must be Scope of Work (SOW) based.

Only time-limited, fixed priced, SOWs for professional services are allowed to be procured using this contract.

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

NCDIT may make multiple awards by subcategory of this RFP.

Interested vendors may submit proposals for one or more of the following bid categories. The North Carolina Department of Information Technology "NCDIT" will review and evaluate responses by category. Contract award will be rolling by category:

CATEGORY SPECIFIC SCOPES OF WORK

Category A: Endpoint and Network Security Products

1. ANTI-VIRUS/MALWARE/ADWARE SOFTWARE
2. ENCRYPTION SOFTWARE AND HARDWARE
3. DATA LOSS PREVENTION (DLP) SOFTWARE
4. CLOUD SECURITY SOFTWARE AND TOOLS INCLUDING CLOUD ACCESS SECURITY BROKER (CASB) SOLUTIONS
5. VIRTUAL PRIVATE NETWORK (VPN) SOLUTIONS
6. MOBILE DEVICE MANAGEMENT (MDM)/ENTERPRISE MOBILITY MANAGEMENT (EMM) SOLUTIONS
7. ENDPOINT DETECTION AND RESPONSE (EDR), EXTENDED DETECTION AND RESPONSE (XDR), AND MANAGED DETECTION AND RESPONSE (MDR)
8. WEB APPLICATION FIREWALLS (WAF) AND EDGE PROXIES

Category B: Identity and Access Management Products

1. IDENTITY AND ACCESS MANAGEMENT (IAM) SOFTWARE SOLUTIONS AND HARDWARE DEVICES

Category C: Security Management and Analytics Products

1. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOFTWARE AND APPLIANCES
2. THREAT INTELLIGENCE SOFTWARE PLATFORMS AND HARDWARE SOLUTIONS
3. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS)
4. SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM (SCADA) SOLUTIONS
5. SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) SOLUTIONS
6. BREACH AND ATTACK SIMULATION (BAS) SOLUTIONS
7. VULNERABILITY MANAGEMENT SOLUTIONS

Category D: Email Security Products

1. EMAIL SECURITY SOFTWARE SOLUTIONS AND APPLIANCES

Category E: Software Development Security Products

1. APPLICATION CODE, AND SOFTWARE DEVELOPMENT SECURITY TESTING TOOLS

Category F: Security Assessment, Testing and Consulting Services

1. SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES
2. APPLICATION RISK ASSESSMENT AND CONSULTING SERVICES
3. PENETRATION TEST AND EMAIL SECURITY ASSESSMENT AND CONSULTING SERVICES
4. SECURITY INCIDENT READINESS ASSESSMENT AND CONSULTING SERVICES
5. INTERNAL VULNERABILITY ASSESSMENT AND CONSULTING SERVICES
6. NETWORK ARCHITECTURE ASSESSMENT AND CONSULTING SERVICES
7. CYBERSECURITY USER TRAINING AND AWARENESS PROGRAM
8. CYBERSECURITY SYSTEM IMPLEMENTATION AND INTEGRATION SERVICES
9. SECURITY INCIDENT RESPONSE CONSULTING SERVICES
10. SECURITY OPERATIONS CENTER AS A SERVICES (SOCaaS)
11. SECURITY POLICY DEVELOPMENT AND COMPLIANCE CONSULTING SERVICES
12. SECURE SOFTWARE DEVELOPMENT CONSULTING SERVICES
13. SECURE DEVOPS (DEVSECOPS) INTEGRATION SERVICES

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

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

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

Core Technologies: The core technologies of North Carolina's Executive State Agencies incorporates 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. We prioritize 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: Our 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 Executive Agencies also have computing infrastructures that will require cybersecurity support. 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 our 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: ENDPOINT AND NETWORK SECURITY PRODUCTS

1. ANTI-VIRUS/MALWARE/ADWARE SOFTWARE

SCOPE OF WORK

Protect endpoints from malicious software, including viruses, malware, and adware, through detection, quarantine, and removal processes.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Detection Efficacy:

(a) Describe the detection methods utilized by your anti-virus/malware/adware software.
(b) Describe how the solution minimizes false positives and false negatives.
(c) Describe the average detection rate for new and emerging threats as verified by the AV-TEST Institute, AV Comparatives or SE Labs.
(d) Describe the workflow from detection to resolution.

2. Update Frequency and Process:

(a) Describe the frequency of your virus, malware, and adware definitions updates.
(b) Describe the process for pushing updates to endpoints.
(c) Describe the average time from threat identification to definition deployment.
(d) Describe how the solution ensures minimal disruption to endpoint operations during updates.
(e) Describe how endpoint updates are managed.

3. System Impact:

(a) Describe the standard system resource consumption when running a full system scan with the software.
(b) Describe the metrics on CPU, memory, disk I/O usage and any network bandwidth implications.

4. Integration and Compatibility:

(a) Describe how your anti-virus/malware/adware software integrates with existing security information and event management (SIEM) systems and other security tools currently in use by the state.
(b) Describe how you support a multi-tenant environment.
(c) Describe how your management console supports centralized management.
(d) Describe which operating systems are supported by your management console and your client for an on-prem solution.
(e) Describe which operating systems are supported at the agent level.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how the products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1:**

https://www.w3.org/TR/WCAG21/; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

2. ENCRYPTION SOFTWARE AND HARDWARE:

SCOPE OF WORK

Secure sensitive data by converting it into unreadable code that can only be deciphered with the correct key or password, both in software and hardware formats.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Encryption Standards and Compliance:

(a) Describe the encryption standards supported by your encryption software and hardware.
(b) Describe how the software aligns with the SCIO System and Communications Protection Policy (SCIO-SEC-316). **https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment**

2. Key Management Process:

(a) Describe your key management process, including key generation, distribution, storage, rotation, and destruction.
(b) Describe how the software prevents unauthorized access to encryption keys. Describe how your software ensures that key management practices are secure and auditable.

3. Performance Impact and Scalability:

(a) Describe the performance impact of implementing your encryption solution on system resources.
(b) Describe the expected throughput and latency metrics when encrypting/decrypting data.
(c) Describe how the software scales to accommodate large volumes of data and high transaction rates.
(d) Describe how the software scales to accommodate large volumes of data and high transaction rates.

4. Recovery and Access Controls:

(a) Describe the procedures for data recovery in the event of key loss or corruption.
(b) Describe how the software ensures that only authorized users can access encrypted data.

5. Integration with Existing Infrastructure:

(a) Describe how the encryption software integrates with the state's existing IT infrastructure, including cloud services, databases, and legacy systems.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.

4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

3. DATA LOSS PREVENTION (DLP) SOFTWARE:

SCOPE OF WORK

Prevent unauthorized access to or sharing of sensitive information, ensuring that data remains within the control of the state.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Data Identification and Classification:

(a) Describe how the Data Loss Prevention software identifies and classes sensitive data across the organization.
(b) Describe the methods used for data discovery.

2. Policy Management and Enforcement:

(a) Describe how the Data Loss Prevention software enables the creation and management of data protection policies.
(b) Describe the policy enforcement capabilities, such as blocking, alerting, and encryption.
(c) Describe how the policies can be customized.
(d) Describe any obfuscation techniques used to ensure that DLP alerting complies with privacy policies and regulation as defined by the Statewide Information Security Manual**.**
https://it.nc.gov/documents/statewide-policies/statewide-information-security-manual/open

3. Incident Management and Reporting:

(a) Describe the incident management and reporting features of your Data Loss Prevention software.
(b) Describe how potential data loss incidents are detected, logged, and reported to administrators.
(c) Describe the workflows available for incident response and remediation.

4. Integration with Existing Systems:

(a) Describe how the Data Loss Prevention software integrates with other security and IT systems, such as email gateways, cloud storage, and endpoint protection platforms.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how the products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

4. CLOUD SECURITY SOFTWARE AND TOOLS INCLUDING CLOUD ACCESS SECURITY BROKER (CASB) SOLUTIONS:

SCOPE OF WORK

Security for cloud-based infrastructure and applications, including access controls, threat monitoring, and data encryption.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Cloud Environment Protection:

(a) Describe the security measures the cloud security software provides for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) environments.
(b) Describe how the software addresses access control, threat detection, and data protection in SaaS, IaaS and PaaS cloud environments.
(c) Describe how the software supports implementation of the zero-trust network access (ZTNA) model.
(d) Describe how the product enforces policies based on user roles, device compliance, location, and other contextual factors.

2. Integration:

(a) Describe the product's integration with AWS, Azure, and Google Cloud Platforms.
(b) Describe how the software ensures consistent security policies across multiple cloud environments.
(c) Describe how the product supports multi-tenancy.
(d) Describe how the product integrates with on-prem security solutions.

3. CASB Capabilities:

(a) Describe the CASB solution's visibility, compliance, data security, and threat protection capabilities.
(b) Describe how the CASB Solution manages and enforces cloud application policies.

4. **Real-time Monitoring and Threat Detection:**
   (a) Describe how the cloud security software conducts real-time monitoring and threat detection.
   (b) Describe the analytics and machine learning capabilities the software employs to identify and respond to potential threats.
5. **Data Loss Prevention (DLP) in the Cloud:**
   (a) Describe the DLP features of your cloud security solution.
   (b) Describe how the solution prevents sensitive data from being uploaded to unauthorized cloud services.
   (c) Describe how the solution protects data residing in the cloud.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

5. VIRTUAL PRIVATE NETWORK (VPN) SOLUTIONS:

SCOPE OF WORK

Securely connect end users directly to a remote private network and its assets.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1.Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. **Encryption and Security Protocols:**
   (a) Describe the encryption standards and security protocols used by the VPN solution.
   (b) Describe how the VPN ensures the confidentiality, integrity, and authenticity of data transmissions over public networks.
2. **Remote Access and Site-to-Site Connectivity:**
   (a) Describe how the VPN solution supports both remote access for individual users and site-to-site connections.
   (b) Describe the features available to manage and secure the different types of VPN connections mentioned above.

3. Compatibility and Integration:

(a) Describe the compatibility of the VPN solution with various operating systems, devices, and network equipment.
(b) Describe how the VPN integrates with existing network infrastructure and authentication services.
(c) Describe how the product supports multi-tenancy.
(d) Describe how the VPN product supports Multi-Factor Authentication (MFA) and Single Sign-On (SSO).
(e) Describe how the product supports and implements the ZTNA model.

4. Scalability and Performance:

(a) Describe how the VPN maintains high throughput and low latency as the number of concurrent users and the volume of data traffic increase.

5. User Experience and Connectivity:

(a) Describe the user interface of your VPN solution.
(b) Describe how the VPN ensures a seamless connection.
(c) Describe the features to handle automatic reconnection and failover connectivity issues.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

6. MOBILE DEVICE MANAGEMENT (MDM)/ENTERPRISE MOBILITY MANAGEMENT (EMM) SOLUTIONS:

SCOPE OF WORK

Safeguard all devices that employees use for work.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Device Enrollment and Management:

(a) Describe the process for enrolling devices into the MDM/EMM solution.
(b) Describe how the solution manages various device types and operating systems.
(c) Describe the solution's capabilities for ongoing device management.

2. Policy Enforcement and Compliance:

(a) Describe how the MDM/EMM solution ensures that devices are compliant with the state's Mobile Device Management Policy (SCIO-SEC-321-00). **https://it.nc.gov/documents/statewide-policies/mobile-device-management-policy/download?attachment**

3. Application Management:

(a) Describe the application management capabilities of the MDM/EMM solution.
(b) Describe how the solution secures applications, manages application distribution, and handles the separation of personal and state data.

4. Remote Wipe and Device Security Features:

(a) Describe the remote wipe and other security features of the MDM/EMM solution.
(b) Describe how the solution protects state data in the event of device loss or theft.

5. User Experience and Support:

(a) Describe the user interface of the MDM/EMM solution.
(b) Describe how the solution minimizes user impact while maintaining security.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

7. ENDPOINT DETECTION AND RESPONSE (EDR), EXTENDED DETECTION AND RESPONSE (XDR), AND MANAGED DETECTION AND RESPONSE (MDR):

SCOPE OF WORK

Provide advanced threat detection, investigation, and response capabilities through Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR) services. The solution should offer a comprehensive approach to identifying and mitigating sophisticated threats across endpoints and the broader IT environment.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Threat Detection and Response Capabilities:

(a) Describe how the EDR solution detects, investigates, and responds to threats on endpoints.
(b) Describe how the XDR solution integrates data from multiple security layers (e.g., endpoints, network, email, cloud) to provide a holistic view of security threats.
(c) Describe the MDR services provided, including the scope of monitoring, threat hunting, and incident response support.

2. Detection Methods and Efficacy:

(a) Describe the detection techniques utilized by your EDR/XDR/MDR solutions (e.g., behavioral analysis, machine learning, threat intelligence).
(b) Describe how your solutions minimize false positives and false negatives.
(c) Describe the average detection rates for new and emerging threats as verified by industry-standard testing organizations such as AV-TEST Institute, AV Comparatives, or SE Labs.

3. Incident Response Workflow:

(a) Describe the workflow from threat detection to resolution for EDR, XDR, and MDR solutions.
(b) Describe the integration of automated and manual response actions.
(c) Describe the tools and processes used for threat investigation and remediation.

4. Threat Intelligence Integration:

(a) Describe how threat intelligence feeds are integrated into your EDR, XDR, and MDR solutions.
(b) Describe how real-time threat intelligence enhances detection and response capabilities.
(c) Describe the threat intelligence sources utilized by your solutions.

5. System Impact and Performance:

(a) Describe the standard system resource consumption when running EDR/XDR/MDR solutions.
(b) Provide metrics on CPU, memory, disk I/O usage, and any network bandwidth implications.
(c) Describe how the product ensures minimal impact on endpoint performance while providing comprehensive protection.

6. Update Frequency and Process:

(a) Describe the frequency of updates for detection algorithms, threat intelligence, and software components.
(b) Describe the process for pushing updates to endpoints and ensuring synchronization across all components.
(c) Describe the average time from threat identification to definition deployment and how updates are managed with minimal disruption to endpoint operations.

7. Integration and Compatibility:

(a) Describe how the EDR, XDR, and MDR products integrate with existing security information and event management (SIEM) systems and other security tools.
(b) Describe how the EDR, XDR, and MDR products support a multi-tenant environment.
(c) Describe the compatibility of the EDR, XDR, and MDR product with various operating systems at both the management console and agent levels.

8. Scalability and Flexibility:

(a) Describe how the EDR, XDR, and MDR products scale to accommodate different size organizations, including small public entities to large agencies.
(b) Describe the deployment options available, on-premises, cloud, hybrid, and how each option supports scalability.
(c) Describe the customization and flexibility of the products to meet specific security requirements and policies of different organizations.

9. Service and Support:

(a) Describe the support services included with the EDR, XDR, and MDR offerings.
(b) Describe the MDR product's availability of 24/7 monitoring and support, including response times and service level agreements (SLAs).

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

8. WEB APPLICATION FIREWALLS (WAF) AND EDGE PROXIES:

SCOPE OF WORK

Protect web applications and edge networks from a wide range of cyber threats through the deployment of Web Application Firewalls (WAF) and Edge Proxies. The solution should provide robust security measures to detect, block, and mitigate attacks while ensuring optimal performance and availability of web services.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Threat Detection and Mitigation:

(a) Describe how the WAF detects and mitigates common web application threats, including SQL injection, cross-site scripting (XSS), and remote file inclusion (RFI).
(b) Describe the methods used to identify and block zero-day vulnerabilities and advanced persistent threats (APTs).
(c) Describe the integration of threat intelligence feeds and real-time security updates.

2. Traffic Management and Performance:

(a) Describe how the Edge Proxy optimizes web traffic, including load balancing, caching, and compression techniques.
(b) Describe the impact of the product on web application performance and how it ensures minimal latency.

3. Configuration and Customization:

(a) Describe the configuration options available for tailoring WAF and Edge Proxy rules to specific application requirements.
(b) Describe the user interface and ease of use for configuring and managing security policies.
(c) Describe the automation features that assist in the dynamic adjustment of security settings based on real-time threat analysis.

4. Compliance and Reporting:

(a) Describe how the product's help organizations comply with industry standards and regulations (e.g., PCI DSS, HIPAA).
(b) Describe the product's reports. and how the reports assist in demonstrating compliance and security posture.
(c) Describe the product's report customization options.

5. Integration and Compatibility:

(a) Describe how the WAF and Edge Proxy integrate with existing security infrastructure, including SIEM systems, identity and access management (IAM) solutions, and other security tools.
(b) Describe how the product supports deployment in various environments, including on-premises, cloud, and hybrid setups.
(c) Describe the product's compatibility with different web server technologies and content management systems (CMS).

6. Scalability and High Availability:

(a) Describe how the product handles varying levels of web traffic.
(b) Describe the product's high availability features, including failover mechanisms and redundancy, to ensure continuous protection and uptime.
(c) Describe the performance benchmarks and scalability testing results of the product.

7. System Impact and Resource Consumption:

(a) Describe the standard system resource consumption for the WAF and Edge Proxy products.
(b) Describe the metrics on CPU, memory, and network bandwidth usage during peak operation.
(c) Describe how the product ensures minimal impact on web application performance while providing robust security.

8. Update Frequency and Process:

(a) Describe the frequency of updates for security rules, threat intelligence, and software components.
(b) Describe the process for pushing updates to the WAF and Edge Proxy components and ensuring minimal disruption to web services.
(c) Describe the average time from threat identification to deployment of security updates.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

CATEGORY B*:* IDENTITY AND ACCESS MANAGEMENT PRODUCTS

1. IDENTITY AND ACCESS MANAGEMENT (IAM) SOFTWARE SOLUTIONS AND HARDWARE DEVICES:

SCOPE OF WORK

Systems that manage digital identities and control user access to resources within an organization, ensuring that the right individuals have access to the appropriate resources at the right times.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Authentication and Authorization Capabilities:

(a) Describe the authentication methods supported by your IAM solutions.
(b) Describe how those methods ensure secure access control, including support for MFA and adaptive authentication methods.
(c) Describe the product's ability to support Privileged Account Management (PAM), Privileged User Management (PUM), and Privileged Identity Management (PIM).
(d) Describe the PIM/PAM/PUM ability to support local accounts and domain accounts.
(e) Describe how the product supports user accounts, privileged user accounts, and administrator accounts.
(f) Describe how the product conducts user access and authentication attestation.
(g) Describe how the product supports non-password-based authentication.
(h) Describe the product's encryption technologies used to maintain the security of stored Application Programming Interface (API) keys, database credentials, Identity and Access Management (IAM) permissions, Secure Shell (SSH) keys, certificates, etc.
(i) Describe how the product supports stored media in a password vault.
(j) Describe how the product supports a role-based access model.

2. Identity Lifecycle Management:

(a) Describe how the IAM solution manages the identity lifecycle, including provisioning, modification, and de-provisioning of user access.
(b) Describe the process for onboarding new users, managing changes in user roles, and offboarding users.

3. Self-Service and User Experience:

(a) Describe how the IAM solution provides self-service capabilities for users, such as password resets and access requests.
(b) Describe how the solution balances user convenience with security requirements.
(c) Describe how the product supports SSO.

4. Reporting and Monitoring:

(a) Describe the solution's reporting and monitoring features.
(b) Describe how the solution provides visibility into access patterns and potential security risks, such as orphaned accounts or excessive permissions.

5. Integration:

(a) Describe how the IAM solution integrates with existing enterprise systems, directories, and applications at a workstation, server, and in the cloud.
(b) Describe how the product supports multi-tenant environments.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

CATEGORY C: SECURITY MANAGEMENT AND ANALYTICS PRODUCTS

1. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SOFTWARE AND APPLIANCES:

SCOPE OF WORK

Real-time analysis of security alerts generated by applications and network hardware, offering insights into potential security incidents.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Event Collection and Correlation:

(a) Describe the event collection capabilities of your SIEM product.
(b) Describe how the solution aggregates and correlates data from various sources, such as network devices, servers, applications, and security systems.
(c) Describe the volume of events that the product can process.
(d) Describe how the product handles peak loads.
(e) Describe how the product supports workloads above 250,000 events per second.
(f) Describe how the product handles archiving.
(g) Describe how the product handles the search of archived data.
(h) Describe how the product incorporates and leverages behavioral analytics.

2. Real-time Analysis and Alerting:

(a) Describe the real-time analysis and alerting methods within your SIEM.
(b) Describe how the software detects anomalies and potential security incidents.

(c) Describe the provided alerting thresholds and notification systems.

3. Compliance and Reporting:

(a) Describe the reporting features of your SIEM solution and its ability to assess compliance with organizational policies or regulatory requirements.
(b) Describe how the software supports compliance with the state's System and Information Integrity Policy (SCIO-SEC-316). **https://it.nc.gov/documents/statewide-policies/scio-system-and-communications-protection/download?attachment**
(c) Describe the reports that can be generated, and how they can be customized for different stakeholders.

4. Forensic Capabilities and Incident Response:

(a) Describe how the SIEM's forensic capabilities support incident response.
(b) Describe how the SIEM facilitates the investigation of security incidents and the collection of evidence for potential legal actions.

5. User Interface and Usability:

(a) Describe the SIEM product user interface.
(b) Describe how the SIEM product presents data to security analysts and the features available to aid in the interpretation and investigation of security events.
(c) Describe how the product promotes single pane of glass visibility.
(d) Describe how the product supports multi-tenancy and role-based access control.

6. Integration:

(a) Describe how the SIEM product integrates with switches and firewalls, operating systems like Windows, Linux, and macOS, and log collection and analysis software such as Splunk, LogRhythm, and Elastic Stack (ELK).
(b) Describe how the product supports or integrates with cybersecurity case management solutions.
(c) Describe how the SIEM product integrates with playbooks such as those provided through a SOAR.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

2. THREAT INTELLIGENCE SOFTWARE PLATFORMS AND HARDWARE SOLUTIONS:

SCOPE OF WORK

Collect and analyze data on emerging threats, helping organizations to understand and prepare for potential cyber-attacks.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Threat Intelligence Collection and Analysis:

(a) Describe the sources of threat intelligence your platform utilizes.
(b) Describe how the solution collects, analyzes, and validates threat data.
(c) Describe the process for ensuring the relevance and accuracy of the intelligence provided.

2. Integration with Security Infrastructure:

(a) Describe how the threat intelligence platform integrates with an organization's existing security infrastructure, such as firewalls, SIEMs, and endpoint protection systems.
(b) Describe how the product enhances the capabilities of these systems to respond to new threats.
(c) Describe how your platform supports role-based access control.

3. Actionable Insights and Customization:

(a) Describe how the platform provides proactive defense strategies and actionable insights tailored to the organization.
(b) Describe the product's customization options for filtering and prioritizing threat intelligence.

4. Collaboration and Information Sharing:

(a) Describe how the product supports collaboration and information sharing within the organization and with external entities.
(b) Describe how the product facilitates the exchange of threat intelligence.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

3. INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS):

SCOPE OF WORK

Monitors the network for threats and take action to stop threats that are detected.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Detection Capabilities:

(a) Describe the detection methods used by the IDPS.
(b) Describe how the IDPS differentiates between normal network behavior and potential threats.
(c) Describe the IDPS' signature-based, anomaly-based, and behavior-based detection methods.
(d) Describe the IDPS' ability to capture network traffic.
(e) Describe how hardware devices connect to the network (i.e., TAP, inline, fail open or close, etc.)

2. Preventive Actions and Response:

(a) Describe the preventive actions the IDPS takes when a threat is detected.
(b) Describe how the IDPS ensures minimal false positives and false negatives.
(c) Describe the IDPS' options available for automated and manual responses.

3. Integration with Existing Security Infrastructure:

(a) Describe how the IDPS integrates with firewalls, SIEM systems, and endpoint protection platforms.
(b) Describe how the IDPS enhances overall security posture.
(c) Describe how the IDPS can enhance organizational capabilities for analysis and incident investigation.

4. Threat Intelligence Integration:

(a) Describe how the IDPS utilizes threat intelligence to improve detection and prevention capabilities.
(b) Describe how the IDPS integrates with external threat intelligence feeds.

5. Forensic Analysis and Incident Investigation:

(a) Describe the IDPS' forensic analysis and incident investigation features.
(b) Describe how the IDPS assists in the post-incident review process.
(c) Describe how the IDPS assists in the identification of the root cause of security breaches.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.

2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

4. SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM (SCADA) SOLUTIONS:

SCOPE OF WORK

Control and manage high-level industrial processes without human intervention.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Operational Technology (OT)-Specific Threat Protection:

(a) Describe how the SCADA protects against OT-specific threats.
(b) Describe the types of threats addressed by the SCADA.
(c) Describe how the SCADA accounts for the unique protocols and devices used in Industrial Control System (ICS) environments.
(d) Describe how the SCADA protects, monitors, and integrates with human-machine interface (HMI) systems.

2. Network Segmentation and Access Controls:

(a) Describe the product's approach to network segmentation and access control within SCADA environments.
(b) Describe how the product prevents unauthorized access to and contains potential incidents within segmented zones.

3. Intrusion Detection for ICS:

(a) Describe how the product detects intrusions.
(b) Describe how the product monitors ICS network traffic for suspicious activities.
(c) Describe the methods used by the product to detect anomalies that may indicate a cyber threat.

4. Integration with ICS and SCADA Systems:

(a) Describe how the product integrates with existing ICS and SCADA systems.
(b) Describe the product's compatibility with legacy systems.
(c) Describe the product's compatibility with Modbus, Distributed Network Protocol 3 (DNP3), or BACnet industrial protocols.
(d) Describe how the product integrates with and supports the Purdue Enterprise Reference Architecture (PERA).

5. Security Monitoring and Incident Response:

(a) Describe the product's security monitoring and incident response features.
(b) Describe how the product supports the detection, analysis, and response to incidents in real-time within an Operational Technology environment.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into

production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

5. SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) SOLUTIONS:

SCOPE OF WORK

Automate cyberattack prevention and response.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your products or services address the scope of work.

b. Technical Qualifications:

1. Orchestration and Integration:

(a) Describe the orchestration capabilities of the SOAR solution.
(b) Describe how the SOAR solution integrates with SIEM, endpoint protection, and threat intelligence platforms to streamline workflows and data sharing.

2. Automation of Workflows:

(a) Describe how the SOAR solution automates security workflows.
(b) Describe the types of processes that can be automated.
(c) Describe how the solution ensures that automation does not compromise the Security Operations Center analyst's decision-making.
(d) Describe how the solution prevents the introduction of new risks.

3. Incident Response Management:

(a) Describe the incident response management features of the SOAR solution.
(b) Describe how the solution supports the entire incident lifecycle from detection to remediation, including case management and collaboration.

4. Playbook Customization and Development:

(a) Describe the SOAR solution's playbook customization and development capabilities.
(b) Describe how organizations can create and tailor playbooks to specific security processes and incident response plans.

5. Machine Learning (ML) and Artificial Intelligence ("AI") Capabilities:

(a) Describe the SOAR solution's machine learning ("ML") and AI capabilities.
(b) Describe how machine learning and AI technologies enhance threat detection, decision-making, and response actions.
(c) Describe the training process for AI and ML capabilities, including customer data used for training sets.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

6. BREACH AND ATTACK SIMULATION (BAS) SOLUTIONS:

SCOPE OF WORK

Enhance security posture through continuous testing, validation, and improvement of security defenses using Breach and Attack Simulation (BAS) tools.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the product offering with a focus on how your product addresses the scope of work.

b. Technical Qualifications:

1. Simulation Capabilities:

(a) Describe the range and complexity of attack scenarios that your BAS tool can simulate, including common tactics, techniques, and procedures (TTPs) used by threat actors.
(b) Describe how the BAS tool continuously updates its attack simulations to reflect the latest threat landscape.
(c) Describe the customized options available for tailoring simulations to specific organizational environments and threat profiles.

2. Continuous Testing and Validation:

(a) Describe the continuous testing capabilities of the BAS tool, including frequency and automation of simulations.
(b) Describe how the BAS tool validates the effectiveness of security controls and provides actionable insights for improvement.
(c) Describe the reporting and visualization features that help organizations track and measure security posture over time.

3. Integration and Compatibility:

(a) Describe how your BAS tool integrates with existing security infrastructure, including SIEM systems, endpoint protection platforms, and network security tools.

(b) Describe how the BAS tool supports deployment in various environments, including on-premises, cloud, and hybrid setups.
(c) Describe the BAS tool's compatibility with different operating systems, applications, and network architectures.

4. System Impact and Performance:

(a) Describe the standard system resource consumption when running BAS simulations.
(b) Describe the BAS tool's metrics on CPU, memory, and network bandwidth usage during simulation activities.
(c) Describe how the BAS tool ensures minimal impact on production systems and business operations while conducting simulations.

5. Update Frequency and Process:

(a) Describe the tool's frequency of updates for attack scenarios, threat intelligence, and software components.
(b) Describe the tool's process for pushing updates to the BAS tool and ensuring synchronization with the latest threat data.
(c) Describe the tool's average time from threat identification to deployment of new simulation scenarios.

6. Scalability and Flexibility:

(a) Describe how the BAS tool scales to accommodate different sizes of organizations.
(b) Describe the tool's deployment options, on-premises, cloud, hybrid.
(c) Describe how each tool option supports scalability.
(d) Describe the tools customization and flexibility of the tool to meet specific security requirements and policies of different organizations.

7. Reporting:

(a) Describe the tool's reporting capabilities, including the types of reports and how the reports assist in demonstrating compliance and security posture.
(b) Describe the customizable reporting options and dashboard views, including screenshots of different dashboards to illustrate the descriptions.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. **Support and Maintenance:**

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

7. VULNERABILITY MANAGEMENT SOLUTIONS:

SCOPE OF WORK

Provide comprehensive identification, assessment, prioritization, and remediation of vulnerabilities across the entire IT environment using advanced Vulnerability Management tools.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product addresses the scope of work.

b. Technical Qualifications:

1. Vulnerability Detection and Assessment:

(a) Describe the methods used to detect and assess vulnerabilities across various assets, including servers, endpoints, networks, and applications.
(b) Describe how your solution identifies and categorizes vulnerabilities, provide details on the use of threat intelligence and vulnerability databases (e.g., CVE, NVD).

2. Risk Prioritization and Management:

(a) Describe how your solution prioritizes vulnerabilities based on risk, including factors such as exploitability, impact, and asset criticality.
(b) Describe the algorithms or methodologies used to assess and rank vulnerabilities.

3. Remediation and Mitigation:

(a) Describe the remediation guidance and support provided by the solution, including automated and manual remediation options.
(b) Describe the solution's integration with patch management systems and other security tools to streamline the remediation process.

4. Continuous Monitoring and Reporting:

(a) Describe the continuous monitoring capabilities of the Vulnerability Management tool, including the frequency and scope of scans.
(b) Describe the reporting features, including customizable reports and dashboards that provide visibility into the organization's vulnerability landscape.

5. Integration and Compatibility:

(a) Describe the continuous monitoring ability of the Vulnerability Management tool, including the frequency and scope of scans.
(b) Describe the reporting features, including customizable reports and dashboards that provide visibility into the organization's vulnerability landscape.

6. Scalability and Flexibility:

(a) Describe how the Vulnerability Management solution scales to accommodate different sizes of organizations, from small businesses to large enterprises.
(b) Describe the deployment options available, on-premises, cloud, hybrid, and how each option supports scalability.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

CATEGORY D: EMAIL SECURITY PRODUCTS

1. EMAIL SECURITY SOFTWARE SOLUTIONS AND APPLIANCES:

SCOPE OF WORK

Protect email communications from threats such as spam, phishing, and malware, often including content filtering and encryption capabilities.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Threat Detection and Prevention:

(a) Describe the methods your email security solution uses to detect and prevent threats such as spam, phishing, and malware.
(b) Describe how your software stays current with evolving email-based attack techniques.
(c) Describe the software's accuracy rate for threat detection.
(d) Describe how the solution handles user flags for suspicious email.
(e) Describe how the product incorporates and leverages email authentication protocols such as DKIM, DMARC, and SPF.

2. Content Filtering and Data Protection:

(a) Describe the content filtering capabilities of your software.
(b) Describe how the software enforces data protection policies.
(c) Describe the measures used to prevent data exfiltration via email.
(d) Describe the encryption features that protect email data both in transit and at rest.

3. Integration with Existing Email Infrastructure:

(a) Describe how the email security solution integrates with the state's existing email infrastructure, including on-premises and cloud-based email systems.

4. Incident Response and Remediation:

(a) Describe the incident response capabilities of your email security software.
(b) Describe how the software handles the detection of security incidents.
(c) Describe the tools available for end users to investigate and remediate issues.

5. Reporting and Analytics:

(a) Describe the reporting and analytics features of your email security solution.

(b) Describe how the software provides insight into email traffic patterns, detected threats, and policy enforcement effectiveness.

c. Capability:

1. Describe the solution's ability to support e-discovery and other investigation or legal requests.
2. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
3. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
4. Describe or diagram both the Network Architecture and Technology Stack for offered Software or SaaS products.
5. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.
6. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

CATEGORY E: SOFTWARE DEVELOPMENT SECURITY PRODUCTS

1. APPLICATION, CODE, AND SOFTWARE DEVELOPMENT SECURITY TESTING TOOLS:

SCOPE OF WORK

Full-spectrum software security tools: scanning application code for vulnerabilities, static application security testing (SAST), dynamic application security testing (DAST), and interactive application security testing (IAST) tools; Reviewing source code for security flaws, ensuring adherence to secure coding standards, identifying open-source components within codebases and checking for known vulnerabilities and licensing issues.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Testing Capabilities and Methodologies:

(a) Describe the Application Security Testing Tools' methods, including SAST, DAST, and IAST.
(b) Describe how the tools identify vulnerabilities.
(c) Describe the security flaws that the application can detect.
(d) Describe the operating systems that the tool is designed to work with.
(e) Describe how the platform automates the detection of security flaws.
(f) Describe the types of vulnerabilities that the platform can identify.
(g) Describe the programming languages and frameworks supported by the platform.

(h) Describe how the Software Component Analysis (SCA) tool detects and identifies open-source components within a codebase,
(i) Describe how the SCA checks for known vulnerabilities.
(j) Describe how the SCA tracks new vulnerabilities.
(k) Describe the ability to generate software bill of materials.

2. Accuracy and False Positive Management:

(a) Describe the accuracy rate of your application security testing tools.
(b) Describe how the tools minimize false positives.
(c) Describe the processes for validating findings and refining the testing algorithms.

3. Reporting and Remediation Guidance:

(a) Describe the reporting capabilities of the tools.
(b) Describe how the tools presents vulnerability findings.
(c) Describe the remediation guidance offered by the tools.
(d) Describe the integration with issue tracking systems or collaboration platforms.

4. Compliance and Standards:

(a) Describe how the Application Security Testing Tools support compliance with Open Worldwide Application Security Project (OWASP) Top 10, Common Weakness Enumeration (CWE),SANS Institute Top 25, and PCI DSS security standards and frameworks.
(b) Describe how the secure code review platform ensures adherence to OWASP and Computer Emergency Response Team (CERT) secure coding standards as well as custom organizational standards.
(c) Describe how the platform can be configured to enforce specific security policies and compliance requirements.

5. Collaboration and Integration

(a) Describe the collaboration features of your platform.
(b) Describe how the platform supports peer reviews, annotations, and discussions within the code review process.
(c) Describe how the platform tracks decisions and code changes made by different team members.
(d) Describe how the platform integrates with integrated development environments (IDEs) and other developer tools.
(e) Describe how the tool integrates with source code repositories, and which are supported.
(f) Describe how the tool supports Single Sign On (SSO) capabilities.

6. License Compliance Management:

(a) Describe how the SCA tool manages licensing issues associated with open-source components.
(b) Describe how the SCA tool identifies licensing conflicts and ensures compliance with open-source licenses (commercial, GPL, MIT, etc.).

7. Remediation and Mitigation Guidance:

(a) Describe the remediation and mitigation guidance the SCA tool provides when vulnerabilities or licensing issues are identified.
(b) Describe the recommendations for alternative libraries or versions.
(c) Describe how the tool mitigates risks when software is updated.

c. Capability:

1. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe how your products or services can adapt to and grow with the needs of the State of North Carolina.
3. Describe or diagram, both the Network Architecture and Technology Stack for offered Software or SaaS products.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

5. Describe how offered SaaS products comply with the following industry accessibility standards: a) **W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/**; b) Section 508: **https://www.section508.gov/**; and c) Voluntary Product Accessibility Template (VPAT®): **https://www.itic.org/policy/accessibility/vpat**

   Describe how the proposed solution is digitally accessible or if not fully accessible, describe the roadmap with timeline for remediation.

d. Experience:

1. Summarize vendor's experience providing the specified category products or services.
2. Include any external recognition or awards received in the past two years that indicate vendor's marketplace position relative to its competitors.

e. Support and Maintenance:

1. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.

CATEGORY F: SECURITY ASSESSMENT, TESTING AND CONSULTING SERVICES

1. SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Evaluate and improve the effectiveness of an organization's overall security posture.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Assessment Methodology:

(a) Describe the service method used to conduct security program assessments.
(b) Describe the evaluation of the current effectiveness of an organization's security posture.
(c) Describe the frameworks or standards used for your assessments (e.g., NIST, ISO, CIS).
(d) Describe tools used to conduct the assessments and any clean up methodology used to remove the tools from the system.

2. Scope and Depth of Assessments:

(a) Describe the scope and depth of your security program assessments.
(b) Describe the program areas covered by the assessment (e.g., policies, procedures, technical controls, incident response, training).
(c) Describe how you ensure that assessments are comprehensive.

3. Risk Identification and Analysis:

(a) Describe how the service identifies and analyzes risks within an organization's security program.
(b) Describe how risks are prioritized.
(c) Describe the criteria used to assess the potential risk impact.

4. Recommendations and Roadmap Development:

(a) Describe how you provide recommendations and develop roadmaps for improving an organization's security posture.
(b) Describe how you ensure that recommendations are actionable, prioritized, and aligned with an organization's business objectives.

5. Stakeholder Engagement and Communication:

(a) Describe the approach to engaging stakeholders during the assessment process.
(b) Describe how findings and recommendations are communicated to both technical and non-technical stakeholders.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned 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).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

2. APPLICATION RISK ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Identify and mitigate potential risks in software applications.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Assessment Scope and Techniques:

(a) Describe the scope of the application risk assessment services.
(b) Describe the techniques used to identify and assess risks in both web-based and client-server applications.

2. Vulnerability Identification and Prioritization:

(a) Describe how the service identifies vulnerabilities within applications.
(b) Describe how vulnerabilities are prioritized based on their severity and potential impact on the organization.

3. Secure Coding Practices and Review:

(a) Describe how the service evaluates the application's adherence to secure coding practices.
(b) Describe how code reviews are performed.
(c) Describe how you ensure that developers follow best practices to mitigate security risks.

4. Compliance with Security Standards:

(a) Describe how the service ensures that applications comply with applicable security standards and regulations (e.g., OWASP Top 10, PCI DSS, HIPAA).

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.

4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

3. PENETRATION TEST AND EMAIL SECURITY ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Simulate cyber-attacks to identify and address security vulnerabilities and evaluate and improve the security of email systems to protect against threats.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Testing Methodologies and Scope:

(a) Describe the penetration testing methods employed (e.g., black box, white box, grey box).
(b) Describe the scope of your penetration tests.
(c) Describe the variety of intrusion vectors that you are capable of testing (including social engineering, spear phishing, media, watering holes, network vulnerabilities, web application attacks, physical security breaches, wireless security, insider threats, and supply chain attacks).
(d) Describe how you determine the boundaries of the testing environment.
(e) Describe the methods used to evaluate the security of email systems.
(f) Describe the identification of potential email vulnerabilities and threats.
(g) Describe pen testing methods your team is capable of employing.
(h) Describe your capabilities in performing tests of varying scopes.
(i) Describe your process (e.g., step 1: scope, step 2: develop plan to conduct assessment, step 3: validate plan, step 4: execute, step 5: clean up, step 6: report, step: 7 training and remediation support).

2. Compliance with Legal and Ethical Standards:

(a) Describe how the penetration testing services are designed to detect activities that violate (i) NCGS §14-454, Accessing Computers; (ii) the Computer Fraud and Abuse Act; and (iii) the Electronic Communications Privacy Act (ECPA).
(b) Describe how you ensure that testing is conducted without disrupting an organization's normal business activities.

3. Reporting and Debriefing:

(a) Describe the types of reports provided following a penetration test.
(b) Describe how you debrief an organization on your penetration testing findings.
(c) Describe the process of recommending remediation strategies for any discovered vulnerabilities.
(d) Describe the assessment of an organization's capabilities to detect and prevent email-based threats, such as phishing, malware, and spam.
(e) Describe the best practices and technologies recommended for threat detection and prevention.

4. Tools and Technologies Used:

(a) Describe the tools and technologies used during penetration testing.
(b) Describe how you stay current with the latest penetration testing tools and techniques.
(c) Describe how you ensure email authentication protocols (e.g., SPF, DKIM, DMARC) and encryption methods are correctly configured and effective.
(d) Describe how you ensure that sensitive information is protected and that content filtering rules are adequate.

5. Client Collaboration and Communication:

(a) Describe the approach to client collaboration and communication throughout the penetration testing and email security assessment processes.
(b) Describe the involvement of clients in planning, execution, and post-testing activities.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

4. SECURITY INCIDENT READINESS ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Assess an organization's preparedness for handling and responding to security incidents, including conducting Table-Top Exercises (TTX).

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Readiness Assessment Framework:

(a) Describe the framework or methods used to assess an organization's incident response readiness.
(b) Describe the evaluation of the current state of an organization's incident response plan, procedures, and capabilities.

2. Tools and Resources:

(a) Describe the software or tools used in the assessment process.
(b) Describe the evaluation of the tools and resources available to the incident response team.
(c) Describe the determination of whether the tools and resources are adequate for effectively detecting, analyzing, and mitigating incidents.

3. Metrics and Measurement:

(a) Discuss the metrics and measurement criteria used to assess incident readiness.
(b) Describe how an organization's ability to respond to and recover from security incidents is measured.

4. Compliance and Best Practices:

(a) Describe how the service ensures that an organization's incident response practices are compliant with NIST SP 800-61 and ISO/IEC 27035 best practices.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

5. INTERNAL VULNERABILITY ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Scan and analyze internal systems for vulnerabilities and recommend remediation strategies.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Assessment Scope and Methodology:

(a) Describe the scope of your internal vulnerability assessment services.
(b) Describe the methods used to identify vulnerabilities within the internal network.
(c) Describe how you ensure all critical assets are covered.

2. Vulnerability Scanning Tools and Techniques:

(a) Describe the tools and techniques employed for vulnerability scanning.
(b) Describe how you ensure that the tools are current with the latest vulnerability signatures and scanning capabilities.

3. Remediation Strategies and Guidance:

(a) Describe the remediation strategies and guidance provided by your service.
(b) Describe how you assist an organization in developing a plan to address identified vulnerabilities effectively.

4. Reporting and Documentation:

(a) Describe the types of reports and documents that Vendor provides following an internal vulnerability assessment.
(b) Describe how you communicate findings and recommendations to both technical staff and executive leadership.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

6. NETWORK ARCHITECTURE ASSESSMENT AND CONSULTING SERVICES:

SCOPE OF WORK

Evaluate network designs, including wireless, for potential vulnerabilities and compliance with best practices.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

Describe the service offering with a focus on how your services address the scope of work.

b. Technical Qualifications:

1. Assessment Methodology:

(a) Describe the methods used to conduct network architecture assessments.
(b) Describe the methods used to conduct wireless network assessments.
(c) Describe how you evaluate the current network design for potential vulnerabilities and compliance with best practices.

2. Best Practices and Frameworks:

(a) Describe the best practices and frameworks (e.g., NIST, CIS, ISO/IEC) referenced when assessing network architecture.
(b) Describe how you ensure that the network aligns with the standards adopted by the organization (e.g., NIST, CIS, ISO/IEC).

3. Risk Identification and Analysis:

(a) Describe the identification and analysis of risks within the network architecture, including specific wireless network attacks such as unauthorized access and rogue access points.
(b) Describe how these risks are prioritized based on their potential impact on an organization's operations and security posture.
(c) Describe the evaluation of the effectiveness of encryption and authentication protocols used in the wireless network.

4. Segmentation and Access Control:

(a) Describe the evaluation of network segmentation and access control strategies.
(b) Describe the assessment of the effectiveness of these controls in limiting the potential spread of a breach.
(c) Describe how you ensure that segmentation is effectively isolating sensitive data and systems from general user access.

5. Security Device and Control Review:

(a) Describe review of the configuration and effectiveness of security devices and controls within the network (e.g., firewalls, intrusion detection/prevention systems, VPNs).

6. Architecture Types:

(a) Describe your ability to assess operational technology network environments.
(b) Describe your ability to assess wireless network environments.

7. Physical Security for Wireless Network Assessments:

(a) Describe how physical security considerations are addressed in your wireless network assessments.
(b) Describe how you evaluate the risks associated with the physical placement of wireless infrastructure.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

7. CYBERSECURITY USER TRAINING AND AWARENESS PROGRAMS:

SCOPE OF WORK

Provide insights into current threats and help organizations develop proactive defense strategies.

SPECIFICATIONS:

Educate users on identifying and responding to cyber security threats.

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Program Content and Structure:

(a) Describe the content and structure of your cyber security training and awareness programs.
(b) Describe the topics covered in the training.
(c) Describe how you ensure that the material is relevant and current with the latest email threat landscape.

2. Customization to Organization's Needs:

(a) Describe how training programs are customized to the specific needs and risks of an organization.
(b) Describe the assessment of an organization's unique vulnerabilities to tailor the training content.

3. Engagement and Interactivity:

(a) Describe the methods used to engage users and to ensure interactivity during the training.
(b) Describe how you make the training engaging and memorable to maximize retention of the information.

4. Delivery Methods:

(a) Describe the various delivery methods available for your training programs (e.g., in-person sessions, webinars, e-learning modules).
(b) Describe how you determine the most effective delivery method for an organization.
(c) Describe any gamification or other engagement-promoting methodologies used.

5. Behavioral Change and Metrics:

(a) Discuss how your programs aim to change user behavior regarding email security.
(b) Describe the metrics used to track changes in user behavior and the program's impact on reducing email-based threats.
(c) Describe your ability to construct and provide reports based on program metrics.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

8. CYBERSECURITY SYSTEM IMPLEMENTATION AND INTEGRATION SERVICES:

SCOPE OF WORK

Deployment, configuration, and integration of comprehensive cybersecurity systems, including SIEM, Extended Detection and Response(XDR), Email Security, and other related solutions, to enhance real-time security monitoring, threat detection, and incident response capabilities.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Implementation Strategy:

(a) Describe the approach to implementing cybersecurity systems such as SIEM, XDR, Email Security Systems, etc.
(b) Describe the project management methodologies used to ensure timely and successful deployment.

2. Integration with Existing Systems:

(a) Describe the process for integrating cybersecurity solutions with existing security tools and IT infrastructure, including switches, firewalls, operating systems, log collection software tools, etc.
(b) Describe how logs and events from various sources are aggregated and normalized to provide comprehensive security insights.

3. Configuration and Customization:

(a) Describe your process for the configuration and customization of cybersecurity systems.
(b) Describe how correlation rules, dashboards, and alerts are set up to provide meaningful and actionable security insights.
(c) Describe the customization options available to tailor the solutions to specific organizational needs.

4. Performance Optimization:

(a) Describe how the performance of cybersecurity solutions are optimized during implementation.
(b) Describe how you ensure that integrated solutions handle large volumes of data and provide timely analysis without impacting network performance.

5. Compliance and Reporting:

(a) Describe how you configure cybersecurity systems to support relevant industry standards and best practices (e.g., NIST 800-137).

6. Incident Response Integration:

(a) Describe the process for the integration of cybersecurity solutions with an organization's incident response processes.
(b) Describe how you configure systems to facilitate rapid detection and response to security incidents.

7. Ongoing Support and Maintenance:

(a) Describe the ongoing support and maintenance services provided to ensure effective and sustained use of cybersecurity solutions.

8. Training and Knowledge Transfer:

(a) Describe the training programs available for client staff to ensure they are proficient in using and managing the implemented security systems.
(b) Describe the knowledge transfer process to ensure clients can maintain and optimize their security systems post-deployment.

9. Vendor and Third-Party Risk Management:

(a) Describe how the solution helps manage and mitigate risks associated with vendors and third parties.
(b) Describe the processes and tools used to assess and monitor third-party security postures.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

9. SECURITY INCIDENT RESPONSE CONSULTING SERVICES:

SCOPE OF WORK

Provide expertise and support to organizations during and after cybersecurity incidents, including investigation, containment, and recovery.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Incident Response Capabilities:

(a) Describe your incident response services.
(b) Describe how you assist organizations in detecting, investigating, containing, eradicating, and recovering from cybersecurity incidents.
(c) Describe your incident response methodology (i.e., the steps you take in a response).

2. Response Time and Availability:

(a) Describe your incident response times and provisions for responding to incidents at a headquarters location and satellite facilities.
(b) Describe how you ensure availability and rapid deployment of resources when an organization requires immediate assistance.

3. Forensic Analysis and Evidence Preservation:

(a) Describe the service's forensic analysis and evidence preservation capabilities.
(b) Describe how you ensure that critical data is collected and handled in a manner that supports potential legal actions.

4. Communication and Coordination:

(a) Describe the approach to communication and coordination during an incident response.
(b) Describe the interaction with an organization's internal teams, external stakeholders, and law enforcement if required.

5. Post-Incident Reporting and Debriefing:

(a) Describe the post-incident reporting and debriefing process.
(b) Describe the types of reports and documentation provided.
(c) Describe how you facilitate lessons learned and improvement of incident response plans.

6. Remediation and Recovery Support:

(a) Describe the assistance with remediation and recovery efforts.
(b) Describe strategies recommended for restoring systems and operations.
(c) Describe how you assist in the prevention of future incidents.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly

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

2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

10. SECURITY OPERATIONS CENTER AS A SERVICE (SOCaaS):

SCOPE OF WORK

Provide comprehensive security operations services, including the management and operation of Security Operations Center as a Service (SOCaaS), continuous monitoring, threat detection, incident response, and overall enhancement of an organization's security posture.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Security Operations Center as a Service (SOCaaS):

(a) Describe your SOCaaS services.
(b) Describe how you establish, manage, and operate SOCaaS, including the technology stack, staffing, and processes involved.
(c) Describe the continuous monitoring capabilities provided by your SOCaaS.

2. Threat Detection and Analysis:

(a) Describe the methodologies and tools used for threat detection and analysis.
(b) Describe how you leverage threat intelligence to identify and mitigate threats in real-time.
(c) Describe your process for analyzing security events and correlating data from various sources to detect potential threats.

3. Incident Response Capabilities:

(a) Describe the incident response services within the SOCaaS framework.
(b) Describe how you assist organizations in detecting, investigating, containing, eradicating, and recovering from cybersecurity incidents.
(c) Describe the processes and technologies used to facilitate rapid incident response.

4. Compliance and Reporting:

(a) Describe how the SOCaaS assists organizations with regulation and standards, , compliance, including PCI DSS, HIPAA.
(b) Describe the reports and dashboards provided to clients.

5. Integration and Customization:

(a) Describe how the SOCaaS integrates with existing security infrastructure and tools, such as SIEM, Endpoint Detection and Response (EDR), XDR, and other cybersecurity solutions.
(b) Describe the customization options available to tailor the SOCaaS to specific organizational needs and security requirements.

6. 24/7 Monitoring and Support:

(a) Describe the 24/7 monitoring and support services provided by the SOCaaS.
(b) Describe the process to ensure continuous coverage and rapid response to security incidents.
(c) Describe the service level agreements (SLAs) related to response times and support availability.

7. Threat Hunting and Proactive Measures:

(a) Describe the threat hunting capabilities and how they are integrated into your SOC services.
(b) Describe the proactive measures taken to identify and mitigate threats before they impact the organization.

(c) Describe the use of advanced analytics, machine learning, and other technologies in threat hunting.

8. Training and Knowledge Transfer:

(a) Describe the training programs available for client staff to ensure they are proficient in working with SOCaaS services.
(b) Describe your knowledge transfer process to ensure clients can maintain and optimize their security operations post-deployment.

9. Scalability and Flexibility:

(a) Describe how the SOCaaS scales to accommodate organizations of different sizes, from small public entities to large agencies.
(b) Describe the deployment options available, on-premises, cloud, hybrid, and how each option supports scalability and flexibility.
(c) Describe the SOCaaS' ability to adapt and grow with the evolving security needs of the organization.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

11. SECURITY POLICY DEVELOPMENT AND COMPLIANCE CONSULTING SERVICES

SCOPE OF WORK

Assist with creating and implementing security policies that comply with regulatory requirements.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Policy Development Expertise:

(a) Describe your expertise in developing security policies.
(b) Describe how you ensure that the policies are comprehensive, clear, and aligned with an organization's business objectives and risk profile.

2. Compliance Assessment and Gap Analysis:

(a) Describe the approach to conducting compliance assessments and gap analyses.
(b) Describe how areas where an organization may not meet regulatory requirements are identified.

3. Regulatory Compliance:

(a) Describe your expertise in cybersecurity regulatory compliance.

(b) Describe how an organization is assisted in complying with relevant cybersecurity regulations and standards (e.g., HIPAA, NIST, ISO/IEC 27001).
(c) Describe how you stay current with evolving regulatory requirements.
(d) Describe the documentation and reporting provided to demonstrate compliance with regulations.
(e) Describe how you ensure that documentation is thorough and audit ready.

4. Stakeholder Engagement:

(a) Describe the approach to engaging stakeholders in the policy development and compliance process.
(b) Describe how you ensure buy-in from various departments and levels within the organization.

5. Customization of Security Policies:

(a) Describe the customization of security policies to fit the specific needs and context of an organization.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the Vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

12. SECURE SOFTWARE DEVELOPMENT CONSULTING SERVICES:

SCOPE OF WORK

Integrate security into the Software Development Life Cycle (SDLC), including threat modeling and secure design, testing of applications to identify vulnerabilities, and conducting thorough reviews of application source code to identify security issues.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. Integration with SDLC:

(a) Describe how you ensure that security is a consideration from initial design through development, testing, deployment, and maintenance.
(b) Describe the testing methodologies for application security, secure code reviews, and software development security.
(c) Describe how you determine which methods to use based on the application's characteristics.

2. Threat Modeling and Risk Assessment:

(a) Describe the approach to threat modeling and risk assessment within the SDLC.
(b) Describe how you identify potential threats and vulnerabilities early in the development process.

3. **Tools and Techniques:**
   (a) Describe the tools and techniques used in software development, secure coding, or software vulnerability testing services.
   (b) Describe how you balance automated tools with manual expertise to ensure comprehensive coverage.
4. **Vulnerability Identification and Analysis:**
   (a) Describe how the service identifies and analyzes vulnerabilities within applications.
   (b) Describe classification of the severity of vulnerabilities.
   (c) Describe the standards used for assessment (e.g., OWASP Top 10, CWE/SANS Top 25).
5. **Secure Coding Practices:**
   (a) Describe the promotion and implementation of secure coding practices.
   (b) Describe the training and resources provided to development teams to enhance their understanding of security issues.
6. **Security Testing and Validation:**
   (a) Describe the security testing and validation strategies that your service recommends.
   (b) Describe how you ensure that security testing is thorough and effective at identifying vulnerabilities.
7. **Secure Architecture and Design Consulting:**
   (a) Describe assistance with secure architecture and design.
   (b) Describe how you ensure that security is built into the architecture of software applications.
8. **Remediation Support:**
   (a) Describe the provision of remediation support.
   (b) Describe assistance provided to developers to understand vulnerabilities and to implement effective remediation strategies.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the Vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

13. SECURE DEVOPS (DEVSECOPS) INTEGRATION SERVICES:

SCOPE OF WORK

Integrate security practices into DevOps workflows to enhance the security of development processes.

SPECIFICATIONS:

Vendors are to submit proposals that provide:

a. Overview:

1. Describe the service offering with a focus on how your product or services address the scope of work.

b. Technical Qualifications:

1. DevSecOps Strategy and Approach:

(a) Describe the strategy and approach for integrating security practices into DevOps workflows.
(b) Describe how you ensure that security is a seamless part of the development and deployment process.

2. Security Automation in Continuous Integration / Continuous Deployment (CI/CD):

(a) Describe the automation of security within the CI/CD pipeline.
(b) Describe the tools and technologies implemented to perform security checks during code commits, builds, and deployments.

3. Collaboration Between Teams:

(a) Describe the facilitation of collaboration between development, operations, and security teams.

4. Security Metrics and KPIs:

(a) Describe the security metrics and key performance indicators (KPIs) established to measure the effectiveness of DevSecOps practices.
(b) Describe the tracking and reporting on these metrics.

c. Capability:

1. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
2. Describe the scalability, interoperability, customization, and integration capabilities of your services.
3. Describe how your services can adapt to and grow with the needs of the State of North Carolina.
4. Describe the solution roadmap for your product or service. Include content on release strategies for functionality, roadmap for technical architecture, how scalability of solution is planned. The minimum content should include: a) Vision for the solution; b) High-level functionality expected for each solution release into production environment; c) High-level timeline; and d) Description of how customer feedback is collected and incorporated into solution enhancements.

d. Experience and Key Personnel:

1. Describe the position title, experience, certifications and educational requirements for the vendor's technical/professional staff who will be assigned to perform the category services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).
2. Describe the Vendor's qualifications to perform the services specified in the category.

e. Support and Maintenance:

1. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

ATTACHMENT J: GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI)

For Vendor solutions incorporating or utilizing GenAI, please respond to the following specifications. Vendors are requested to respond for each subcategory for which Vendor has provided a response.

1. Describe how the Vendor's proposed GenAI solution meets the State's definition of 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)"
2. Describe the Vendor's resources to support risk and compliance during product development.
3. Describe how the Vendor handles development, testing, and management of the product.
4. Describe how the Vendor's AI is being or was trained.
5. Describe what AI training and validation practices the Vendor employs to meet responsible AI objectives.
6. Describe the sources of data used in AI training.
7. Describe how the Vendor's AI practices, training, and testing methods align with U.S. AI frameworks and guidance (e.g., The White House Blueprint for an AI Bill of Rights, NIST AI Risk Management Framework 1.0) to mitigate ethical and moral risks (e.g., bias, algorithmic discrimination protections, data privacy, safe and effective systems, notice and explanation, human alternatives, consideration, and fall back).
8. Describe the options that users have to control the activation of AI capabilities within applications (or within Vendor's proposed solution).
9. Describe the configurable settings for the user to enable or disable AI functionalities within the applications (or within Vendor's proposed solution).
10. Describe how the Vendor integrates data governance into sourcing, managing, and overseeing training data as part of Vendor's AI model development process.
11. Describe how the Vendor safeguards the State's data.
12. Describe the standards the Vendor follows for safeguarding The State's data.
13. Describe how the Vendor operationalizes the standards.
14. Describe Vendor's data governance practices employed in the development and delivery of AI applications.
15. Describe Vendor's approach to responsible use of AI.
16. Describe the ethical principles, guidelines, or requirements that the Vendor has adopted to ensure responsible use of AI and data governance.
17. Describe whether the Vendor or a third-party designed, developed, deployed, and/or maintains the GenAI system.
18. Describe the mechanisms used to test a GenAI solution residing on state infrastructure.
19. Describe how the mechanisms tests how the AI interacts with all systems.
20. Describe the access the Vendor provides system owners to the GenAI/AI.
21. Describe the type of model(s) and/or network(s) (e.g., artificial neural networks, large language models (LLMs) used in the GenAI system. Please reference all and explain their specific applicational use and purpose.
22. Describe the mechanisms that are used to audit the system and its data.
23. Describe who will have access to audit logs.
24. Describe whether access will be role-based and authenticated.
25. Describe the mechanism used to detect and correct an output error (e.g. automated, service support center, etc.).
26. Describe how errors and level or risk of errors are ranked (e.g., high, medium, low).
27. Describe how Vendor's proposed solution accommodates the State of North Carolina's ownership of all rights and intellectual property of data outputs.
28. Describe how Vendor's proposed solution accommodates the following statement concerning ownership: Vendors are to release all ownership of data generated by the AI. Identify the Level of GenAI Autonomy:
    a. ☐ System operates automatically with no human intervention.
    b. ☐ System operates automatically with occasional retrospective reviews by humans.
    c. ☐ System produces recommendations but cannot act without human intervention.
29. Describe how the Vendor will identify and mitigate hallucinations and ensure that GenAI data outputs are accurate and factual.
30. Describe how the Vendor monitors GenAI to ensure continued accurate performance over the lifetime of the contract.
31. Describe whether logs will be available in a non-proprietary format and the process of log ingestion into a Security Information and Event Management (SIEM) tool.

ATTACHMENT K: SUBMITTAL CHECKLIST

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

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 2022 and 2023 Sales Volume Data, NC HUB Certification Letter, if applicable, Letter of Authorization from Original Equipment Manufacturer, if applicable, Proof of eProcurement registration (i.e. Print Screen)*)	See Page 55
	☐ Attachment E: Vendor Certification Form (Include Proof of NC Secretary of State License to do Business in North Carolina)	See Page 65
	☐ Attachment F: Location of Workers Utilized by Vendors	See Page 66
	☐ Attachment H: Financial Review Forms	See Page 70
SECTION 2: Category Specific Response		
	Category A: Endpoint and Network Security Products **Category B: Identity and Access Management Products** **Category C: Security Management and Analytics Products** **Category D: Email Security Products** **Category E: Software Development Security Products** **Category F: Security Assessment, Testing and Consulting Services** (Specify the category letter, title, subcategory number, and title for each subcategory for which you are providing a response.) ***Each subcategory proposal should be labeled as its own section and numbered sequentially as indicated above.*** ***Organize each subcategory proposal to include subcategory specific responses to Attachment I, Attachment D, Attachment G and Attachment J.***	
☐	☐ **Attachment I: Vendor's Responses to Subcategory-Specific Specifications Sections a.-e.:**	See Page 72
	☐ **Attachment D: Cost Proposal Form(s) (subcategory-specific)** (Include the cost form for each subcategory for which you are providing a response. You must complete all lines on the cost form for that subcategory.	See Page 57
	☐ **Attachment G**: **References** (For Each Category F subcategory) **Two (2)** Customer reference forms.	See Page 67
	☐ **Attachment J**: **Generative Artificial Intelligence (GenAI)**	See Page 112

SECTION 3: VRARs, Errata and Exceptions, License Agreements and Bid Copy.		
	☐ **Vendor Readiness Assessment Reports (VRARs).**	
	☐ **Errata and exceptions, if any, excluding Section 3: Terms and Conditions Applicable to Personnel and Personal Services.**	
	☐ Vendor's license agreement(s), maintenance, warranty and service level agreements.	
	☐ All pages of the bid document, excluding the execution page**.**	
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.**	