CYBERSECURITY PRODUCTS & SERVICES WORD ATTACHMENTS C-K

# 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**](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.

1. **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.

1. **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.

1. **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:

1. 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.
2. 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  Yes  No

addressing significant issues? If yes, please explain and provide a copy

of the notification letters.

1. Are the financial figures below based on audited financial statements?  Yes  No
2. Start Date of financial statements:

End Date of financial statements:

1. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years:
2. 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** |  |  |  |
| 1. Cash and Temporary Investments |  |  |  |
| 1. Accounts Receivable (beginning of year) |  |  |  |
| 1. Accounts Receivable (end of year) |  |  |  |
| 1. Average Account Receivable for the Year (calculated) |  |  |  |
| 1. Inventory (beginning of year) |  |  |  |
| 1. Inventory (end of year) |  |  |  |
| 1. Average Inventory for the Year (calculated) |  |  |  |
| 1. Current Assets |  |  |  |
| 1. Current Liabilities |  |  |  |
| 1. Total Liabilities |  |  |  |
| 1. Total Stockholders’ Equity (beginning of year) |  |  |  |
| 1. Total Stockholders’ Equity (end of year) |  |  |  |
| 1. Average Stockholders’ Equity during the year (calculated) |  |  |  |
|  |  |  |  |
| **INCOME STATEMENT DATA** |  |  |  |
| 1. Net Sales |  |  |  |
| 1. Cost of Goods Sold (COGS) |  |  |  |
| 1. Gross Profit (Net Sales minus COGS) (calculated) |  |  |  |
| 1. Interest Expense for the Year |  |  |  |
| 1. Net Income after Tax |  |  |  |
| 1. Earnings for the Year before Interest & Income Tax Expense |  |  |  |
|  |  |  |  |
| **STATEMENT OF CASH FLOWS** |  |  |  |
| 1. Cash Flow provided by Operating Activities |  |  |  |
| 1. 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 Product**s

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:*

1. **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:**

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

**2. Update Frequency and Process:**

1. Describe the frequency of your virus, malware, and adware definitions updates.
2. Describe the process for pushing updates to endpoints.
3. Describe the average time from threat identification to definition deployment.
4. Describe how the solution ensures minimal disruption to endpoint operations during updates.
5. Describe how endpoint updates are managed.

**3. System Impact:**

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

**4. Integration and Compatibility:**

1. 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.
2. Describe how you support a multi-tenant environment.
3. Describe how your management console supports centralized management.
4. Describe which operating systems are supported by your management console and your client for an on-prem solution.
5. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **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:*

1. **Overview:**

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

1. **Technical Qualifications:**

**1. Encryption Standards and Compliance:**

1. Describe the encryption standards supported by your encryption software and hardware.
2. 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:**

1. Describe your key management process, including key generation, distribution, storage, rotation, and destruction.
2. 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:**

1. Describe the performance impact of implementing your encryption solution on system resources.
2. Describe the expected throughput and latency metrics when encrypting/decrypting data.
3. Describe how the software scales to accommodate large volumes of data and high transaction rates.
4. Describe how the software scales to accommodate large volumes of data and high transaction rates.

**4. Recovery and Access Controls:**

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

**5. Integration with Existing Infrastructure:**

1. Describe how the encryption software integrates with the state's existing IT infrastructure, including cloud services, databases, and legacy systems.
2. **Capability:**

Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.

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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **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.
2. **Support and Maintenance:**

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:*

1. **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:**

1. Describe how the Data Loss Prevention software identifies and classes sensitive data across the organization.
2. Describe the methods used for data discovery.

**2. Policy Management and Enforcement:**

1. Describe how the Data Loss Prevention software enables the creation and management of data protection policies.
2. Describe the policy enforcement capabilities, such as blocking, alerting, and encryption.
3. Describe how the policies can be customized.
4. 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**](https://it.nc.gov/documents/statewide-policies/statewide-information-security-manual/open)

**3. Incident Management and Reporting:**

1. Describe the incident management and reporting features of your Data Loss Prevention software.
2. Describe how potential data loss incidents are detected, logged, and reported to administrators.
3. Describe the workflows available for incident response and remediation.

**4. Integration with Existing Systems:**

1. Describe how the Data Loss Prevention software integrates with other security and IT systems, such as email gateways, cloud storage, and endpoint protection platforms.
2. **Capability:**

Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.

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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**

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

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

1. **Support and Maintenance:**

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:*

1. **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:**

1. 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.
2. Describe how the software addresses access control, threat detection, and data protection in SaaS, IaaS and PaaS cloud environments.
3. Describe how the software supports implementation of the zero-trust network access (ZTNA) model.
4. Describe how the product enforces policies based on user roles, device compliance, location, and other contextual factors.

**2. Integration:**

1. Describe the product’s integration with AWS, Azure, and Google Cloud Platforms.
2. Describe how the software ensures consistent security policies across multiple cloud environments.
3. Describe how the product supports multi-tenancy.
4. Describe how the product integrates with on-prem security solutions.

**3. CASB Capabilities:**

1. Describe the CASB solution’s visibility, compliance, data security, and threat protection capabilities.
2. Describe how the CASB Solution manages and enforces cloud application policies.

**4. Real-time Monitoring and Threat Detection:**

1. Describe how the cloud security software conducts real-time monitoring and threat detection.
2. 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:**

1. Describe the DLP features of your cloud security solution.
2. Describe how the solution prevents sensitive data from being uploaded to unauthorized cloud services.
3. Describe how the solution protects data residing in the cloud.
4. **Capability:**

Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.

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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**

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

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

1. **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:*

1. **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:**

1. Describe the encryption standards and security protocols used by the VPN solution.
2. Describe how the VPN ensures the confidentiality, integrity, and authenticity of data transmissions over public networks.

**2. Remote Access and Site-to-Site Connectivity:**

1. Describe how the VPN solution supports both remote access for individual users and site-to-site connections.
2. Describe the features available to manage and secure the different types of VPN connections mentioned above.

**3. Compatibility and Integration:**

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

**4. Scalability and Performance:**

1. 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:**

1. Describe the user interface of your VPN solution.
2. Describe how the VPN ensures a seamless connection.
3. Describe the features to handle automatic reconnection and failover connectivity issues.
4. **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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **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.

1. **Support and Maintenance:**
2. 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:*

1. **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:**

1. Describe the process for enrolling devices into the MDM/EMM solution.
2. Describe how the solution manages various device types and operating systems.
3. Describe the solution’s capabilities for ongoing device management.

**2. Policy Enforcement and Compliance:**

1. 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:**

1. Describe the application management capabilities of the MDM/EMM solution.
2. 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:**

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

**5. User Experience and Support:**

1. Describe the user interface of the MDM/EMM solution.
2. Describe how the solution minimizes user impact while maintaining security.
3. **Capability:**
4. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
5. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **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:**

1. Describe how the EDR solution detects, investigates, and responds to threats on endpoints.
2. 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.
3. Describe the MDR services provided, including the scope of monitoring, threat hunting, and incident response support.

**2. Detection Methods and Efficacy:**

1. Describe the detection techniques utilized by your EDR/XDR/MDR solutions (e.g., behavioral analysis, machine learning, threat intelligence).
2. Describe how your solutions minimize false positives and false negatives.
3. 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:**

1. Describe the workflow from threat detection to resolution for EDR, XDR, and MDR solutions.
2. Describe the integration of automated and manual response actions.
3. Describe the tools and processes used for threat investigation and remediation.

**4. Threat Intelligence Integration:**

1. Describe how threat intelligence feeds are integrated into your EDR, XDR, and MDR solutions.
2. Describe how real-time threat intelligence enhances detection and response capabilities.
3. Describe the threat intelligence sources utilized by your solutions.

**5. System Impact and Performance:**

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

**6. Update Frequency and Process:**

1. Describe the frequency of updates for detection algorithms, threat intelligence, and software components.
2. Describe the process for pushing updates to endpoints and ensuring synchronization across all components.
3. 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:**

1. Describe how the EDR, XDR, and MDR products integrate with existing security information and event management (SIEM) systems and other security tools.
2. Describe how the EDR, XDR, and MDR products support a multi-tenant environment.
3. 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:**

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

**9. Service and Support:**

1. Describe the support services included with the EDR, XDR, and MDR offerings.
2. Describe the MDR product’s availability of 24/7 monitoring and support, including response times and service level agreements (SLAs).
3. **Capability:**
4. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
5. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **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:**

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

**2. Traffic Management and Performance:**

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

**3. Configuration and Customization:**

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

**4. Compliance and Reporting:**

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

**5. Integration and Compatibility:**

1. 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.
2. Describe how the product supports deployment in various environments, including on-premises, cloud, and hybrid setups.
3. Describe the product’s compatibility with different web server technologies and content management systems (CMS).

**6. Scalability and High Availability:**

1. Describe how the product handles varying levels of web traffic.
2. Describe the product’s high availability features, including failover mechanisms and redundancy, to ensure continuous protection and uptime.
3. Describe the performance benchmarks and scalability testing results of the product.

**7. System Impact and Resource Consumption:**

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

**8. Update Frequency and Process:**

1. Describe the frequency of updates for security rules, threat intelligence, and software components.
2. Describe the process for pushing updates to the WAF and Edge Proxy components and ensuring minimal disruption to web services.
3. Describe the average time from threat identification to deployment of security updates.
4. **Capability:**
5. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
6. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **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:**

1. Describe the authentication methods supported by your IAM solutions.
2. Describe how those methods ensure secure access control, including support for MFA and adaptive authentication methods.
3. Describe the product’s ability to support Privileged Account Management (PAM), Privileged User Management (PUM), and Privileged Identity Management (PIM).
4. Describe the PIM/PAM/PUM ability to support local accounts and domain accounts.
5. Describe how the product supports user accounts, privileged user accounts, and administrator accounts.
6. Describe how the product conducts user access and authentication attestation.
7. Describe how the product supports non-password-based authentication.
8. 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.
9. Describe how the product supports stored media in a password vault.
10. Describe how the product supports a role-based access model.
11. **Identity Lifecycle Management:**
12. Describe how the IAM solution manages the identity lifecycle, including provisioning, modification, and de-provisioning of user access.
13. Describe the process for onboarding new users, managing changes in user roles, and offboarding users.
14. **Self-Service and User Experience:**
15. Describe how the IAM solution provides self-service capabilities for users, such as password resets and access requests.
16. Describe how the solution balances user convenience with security requirements.
17. Describe how the product supports SSO.
18. **Reporting and Monitoring:**
19. Describe the solution’s reporting and monitoring features.
20. Describe how the solution provides visibility into access patterns and potential security risks, such as orphaned accounts or excessive permissions.
21. **Integration:**
22. Describe how the IAM solution integrates with existing enterprise systems, directories, and applications at a workstation, server, and in the cloud.
23. Describe how the product supports multi-tenant environments.
24. **Capability:**
25. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
26. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**
2. Describe the product offering with a focus on how your products or services address the scope of work.
3. **Technical Qualifications:**
4. **Event Collection and Correlation:**
5. Describe the event collection capabilities of your SIEM product.
6. Describe how the solution aggregates and correlates data from various sources, such as network devices, servers, applications, and security systems.
7. Describe the volume of events that the product can process.
8. Describe how the product handles peak loads.
9. Describe how the product supports workloads above 250,000 events per second.
10. Describe how the product handles archiving.
11. Describe how the product handles the search of archived data.
12. Describe how the product incorporates and leverages behavioral analytics.
13. **Real-time Analysis and Alerting:**
14. Describe the real-time analysis and alerting methods within your SIEM.
15. Describe how the software detects anomalies and potential security incidents.
16. Describe the provided alerting thresholds and notification systems.
17. **Compliance and Reporting:**
18. Describe the reporting features of your SIEM solution and its ability to assess compliance with organizational policies or regulatory requirements.
19. 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**
20. Describe the reports that can be generated, and how they can be customized for different stakeholders.
21. **Forensic Capabilities and Incident Response:**
22. Describe how the SIEM’s forensic capabilities support incident response.
23. Describe how the SIEM facilitates the investigation of security incidents and the collection of evidence for potential legal actions.
24. **User Interface and Usability:**
25. Describe the SIEM product user interface.
26. Describe how the SIEM product presents data to security analysts and the features available to aid in the interpretation and investigation of security events.
27. Describe how the product promotes single pane of glass visibility.
28. Describe how the product supports multi-tenancy and role-based access control.
29. **Integration:**
30. 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).
31. Describe how the product supports or integrates with cybersecurity case management solutions.
32. Describe how the SIEM product integrates with playbooks such as those provided through a SOAR.
33. **Capability:**
34. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
35. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**
2. Describe the product offering with a focus on how your products or services address the scope of work.
3. **Technical Qualifications:**
4. **Threat Intelligence Collection and Analysis:**
5. Describe the sources of threat intelligence your platform utilizes.
6. Describe how the solution collects, analyzes, and validates threat data.
7. Describe the process for ensuring the relevance and accuracy of the intelligence provided.
8. **Integration with Security Infrastructure:**
9. Describe how the threat intelligence platform integrates with an organization's existing security infrastructure, such as firewalls, SIEMs, and endpoint protection systems.
10. Describe how the product enhances the capabilities of these systems to respond to new threats.
11. Describe how your platform supports role-based access control.
12. **Actionable Insights and Customization:**
13. Describe how the platform provides proactive defense strategies and actionable insights tailored to the organization.
14. Describe the product’s customization options for filtering and prioritizing threat intelligence.
15. **Collaboration and Information Sharing:**
16. Describe how the product supports collaboration and information sharing within the organization and with external entities.
17. Describe how the product facilitates the exchange of threat intelligence.
18. **Capability:**
19. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
20. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.
6. **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:*

1. **Overview:**
2. Describe the product offering with a focus on how your products or services address the scope of work.
3. **Technical Qualifications:**
4. **Detection Capabilities:**
5. Describe the detection methods used by the IDPS.
6. Describe how the IDPS differentiates between normal network behavior and potential threats.
7. Describe the IDPS’ signature-based, anomaly-based, and behavior-based detection methods.
8. Describe the IDPS’ ability to capture network traffic.
9. Describe how hardware devices connect to the network (i.e., TAP, inline, fail open or close, etc.)
10. **Preventive Actions and Response:**
11. Describe the preventive actions the IDPS takes when a threat is detected.
12. Describe how the IDPS ensures minimal false positives and false negatives.
13. Describe the IDPS’ options available for automated and manual responses.
14. **Integration with Existing Security Infrastructure:**
15. Describe how the IDPS integrates with firewalls, SIEM systems, and endpoint protection platforms.
16. Describe how the IDPS enhances overall security posture.
17. Describe how the IDPS can enhance organizational capabilities for analysis and incident investigation.
18. **Threat Intelligence Integration:**
19. Describe how the IDPS utilizes threat intelligence to improve detection and prevention capabilities.
20. Describe how the IDPS integrates with external threat intelligence feeds.
21. **Forensic Analysis and Incident Investigation:**
22. Describe the IDPS’ forensic analysis and incident investigation features.
23. Describe how the IDPS assists in the post-incident review process.
24. Describe how the IDPS assists in the identification of the root cause of security breaches.
25. **Capability:**
26. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
27. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.
6. **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:*

1. **Overview:**
2. Describe the product offering with a focus on how your products or services address the scope of work.
3. **Technical Qualifications:**
4. **Operational Technology (OT)-Specific Threat Protection:**
5. Describe how the SCADA protects against OT-specific threats.
6. Describe the types of threats addressed by the SCADA.
7. Describe how the SCADA accounts for the unique protocols and devices used in Industrial Control System (ICS) environments.
8. Describe how the SCADA protects, monitors, and integrates with human-machine interface (HMI) systems.

**2. Network Segmentation and Access Controls:**

1. Describe the product’s approach to network segmentation and access control within SCADA environments.
2. Describe how the product prevents unauthorized access to and contains potential incidents within segmented zones.
3. **Intrusion Detection for ICS:**
4. Describe how the product detects intrusions.
5. Describe how the product monitors ICS network traffic for suspicious activities.
6. Describe the methods used by the product to detect anomalies that may indicate a cyber threat.
7. **Integration with ICS and SCADA Systems:**
8. Describe how the product integrates with existing ICS and SCADA systems.
9. Describe the product’s compatibility with legacy systems.
10. Describe the product’s compatibility with Modbus, Distributed Network Protocol 3 (DNP3), or BACnet industrial protocols.
11. Describe how the product integrates with and supports the Purdue Enterprise Reference Architecture (PERA).
12. **Security Monitoring and Incident Response:**
13. Describe the product’s security monitoring and incident response features.
14. Describe how the product supports the detection, analysis, and response to incidents in real-time within an Operational Technology environment.
15. **Capability:**
16. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
17. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.
6. **SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) SOLUTIONS:**

**SCOPE OF WORK**

Automate cyberattack prevention and response.

**SPECIFICATIONS:**

*Vendors are to submit proposals that provide:*

1. **Overview:**
2. Describe the product offering with a focus on how your products or services address the scope of work.
3. **Technical Qualifications:**
4. **Orchestration and Integration:**
5. Describe the orchestration capabilities of the SOAR solution.
6. Describe how the SOAR solution integrates with SIEM, endpoint protection, and threat intelligence platforms to streamline workflows and data sharing.
7. **Automation of Workflows:**
8. Describe how the SOAR solution automates security workflows.
9. Describe the types of processes that can be automated.
10. Describe how the solution ensures that automation does not compromise the Security Operations Center analyst’s decision-making.
11. Describe how the solution prevents the introduction of new risks.
12. **Incident Response Management:**
13. Describe the incident response management features of the SOAR solution.
14. Describe how the solution supports the entire incident lifecycle from detection to remediation, including case management and collaboration.
15. **Playbook Customization and Development:**
16. Describe the SOAR solution’s playbook customization and development capabilities.
17. Describe how organizations can create and tailor playbooks to specific security processes and incident response plans.
18. **Machine Learning (ML) and Artificial Intelligence (“AI”) Capabilities:**
19. Describe the SOAR solution’s machine learning (“ML”) and AI capabilities.
20. Describe how machine learning and AI technologies enhance threat detection, decision-making, and response actions.
21. Describe the training process for AI and ML capabilities, including customer data used for training sets.
22. **Capability:**
23. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
24. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**
2. Describe the product offering with a focus on how your product addresses the scope of work.
3. **Technical Qualifications:**
4. **Simulation Capabilities:**
5. 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.
6. Describe how the BAS tool continuously updates its attack simulations to reflect the latest threat landscape.
7. Describe the customized options available for tailoring simulations to specific organizational environments and threat profiles.
8. **Continuous Testing and Validation:**
9. Describe the continuous testing capabilities of the BAS tool, including frequency and automation of simulations.
10. Describe how the BAS tool validates the effectiveness of security controls and provides actionable insights for improvement.
11. Describe the reporting and visualization features that help organizations track and measure security posture over time.
12. **Integration and Compatibility:**
13. Describe how your BAS tool integrates with existing security infrastructure, including SIEM systems, endpoint protection platforms, and network security tools.
14. Describe how the BAS tool supports deployment in various environments, including on-premises, cloud, and hybrid setups.
15. Describe the BAS tool’s compatibility with different operating systems, applications, and network architectures.
16. **System Impact and Performance:**
17. Describe the standard system resource consumption when running BAS simulations.
18. Describe the BAS tool’s metrics on CPU, memory, and network bandwidth usage during simulation activities.
19. Describe how the BAS tool ensures minimal impact on production systems and business operations while conducting simulations.
20. **Update Frequency and Process:**
21. Describe the tool’s frequency of updates for attack scenarios, threat intelligence, and software components.
22. Describe the tool’s process for pushing updates to the BAS tool and ensuring synchronization with the latest threat data.
23. Describe the tool’s average time from threat identification to deployment of new simulation scenarios.
24. **Scalability and Flexibility:**
25. Describe how the BAS tool scales to accommodate different sizes of organizations.
26. Describe the tool’s deployment options, on-premises, cloud, hybrid.
27. Describe how each tool option supports scalability.
28. Describe the tools customization and flexibility of the tool to meet specific security requirements and policies of different organizations.
29. **Reporting:**
30. Describe the tool’s reporting capabilities, including the types of reports and how the reports assist in demonstrating compliance and security posture.
31. Describe the customizable reporting options and dashboard views, including screenshots of different dashboards to illustrate the descriptions.
32. **Capability:**
33. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
34. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. Describe the ongoing support, maintenance, warranty and any training services provided to ensure effective and sustained use of your products or services.
6. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product addresses the scope of work.
3. **Technical Qualifications:**
4. **Vulnerability Detection and Assessment:**
5. Describe the methods used to detect and assess vulnerabilities across various assets, including servers, endpoints, networks, and applications.
6. Describe how your solution identifies and categorizes vulnerabilities, provide details on the use of threat intelligence and vulnerability databases (e.g., CVE, NVD).
7. **Risk Prioritization and Management:**
8. Describe how your solution prioritizes vulnerabilities based on risk, including factors such as exploitability, impact, and asset criticality.
9. Describe the algorithms or methodologies used to assess and rank vulnerabilities.
10. **Remediation and Mitigation:**
11. Describe the remediation guidance and support provided by the solution, including automated and manual remediation options.
12. Describe the solution’s integration with patch management systems and other security tools to streamline the remediation process.
13. **Continuous Monitoring and Reporting:**
14. Describe the continuous monitoring capabilities of the Vulnerability Management tool, including the frequency and scope of scans.
15. Describe the reporting features, including customizable reports and dashboards that provide visibility into the organization’s vulnerability landscape.
16. **Integration and Compatibility:**
17. Describe the continuous monitoring ability of the Vulnerability Management tool, including the frequency and scope of scans.
18. Describe the reporting features, including customizable reports and dashboards that provide visibility into the organization’s vulnerability landscape.
19. **Scalability and Flexibility:**
20. Describe how the Vulnerability Management solution scales to accommodate different sizes of organizations, from small businesses to large enterprises.
21. Describe the deployment options available, on-premises, cloud, hybrid, and how each option supports scalability.
22. **Capability:**
23. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
24. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Threat Detection and Prevention:**
5. Describe the methods your email security solution uses to detect and prevent threats such as spam, phishing, and malware.
6. Describe how your software stays current with evolving email-based attack techniques.
7. Describe the software’s accuracy rate for threat detection.
8. Describe how the solution handles user flags for suspicious email.
9. Describe how the product incorporates and leverages email authentication protocols such as DKIM, DMARC, and SPF.
10. **Content Filtering and Data Protection:**
11. Describe the content filtering capabilities of your software.
12. Describe how the software enforces data protection policies.
13. Describe the measures used to prevent data exfiltration via email.
14. Describe the encryption features that protect email data both in transit and at rest.
15. **Integration with Existing Email Infrastructure:**
16. Describe how the email security solution integrates with the state's existing email infrastructure, including on-premises and cloud-based email systems.
17. **Incident Response and Remediation:**
18. Describe the incident response capabilities of your email security software.
19. Describe how the software handles the detection of security incidents.
20. Describe the tools available for end users to investigate and remediate issues.
21. **Reporting and Analytics:**
22. Describe the reporting and analytics features of your email security solution.
23. Describe how the software provides insight into email traffic patterns, detected threats, and policy enforcement effectiveness.
24. **Capability:**
25. Describe the solution's ability to support e-discovery and other investigation or legal requests.
26. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
27. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**

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

1. **Technical Qualifications:**
2. **Testing Capabilities and Methodologies:**
3. Describe the Application Security Testing Tools’ methods, including SAST, DAST, and IAST.
4. Describe how the tools identify vulnerabilities.
5. Describe the security flaws that the application can detect.
6. Describe the operating systems that the tool is designed to work with.
7. Describe how the platform automates the detection of security flaws.
8. Describe the types of vulnerabilities that the platform can identify.
9. Describe the programming languages and frameworks supported by the platform.
10. Describe how the Software Component Analysis (SCA) tool detects and identifies open-source components within a codebase,
11. Describe how the SCA checks for known vulnerabilities.
12. Describe how the SCA tracks new vulnerabilities.
13. Describe the ability to generate software bill of materials.
14. **Accuracy and False Positive Management:**
15. Describe the accuracy rate of your application security testing tools.
16. Describe how the tools minimize false positives.
17. Describe the processes for validating findings and refining the testing algorithms.
18. **Reporting and Remediation Guidance:**
19. Describe the reporting capabilities of the tools.
20. Describe how the tools presents vulnerability findings.
21. Describe the remediation guidance offered by the tools.
22. Describe the integration with issue tracking systems or collaboration platforms.

**4. Compliance and Standards:**

1. 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.
2. 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.
3. Describe how the platform can be configured to enforce specific security policies and compliance requirements.
4. **Collaboration and Integration**
5. Describe the collaboration features of your platform.
6. Describe how the platform supports peer reviews, annotations, and discussions within the code review process.
7. Describe how the platform tracks decisions and code changes made by different team members.
8. Describe how the platform integrates with integrated development environments (IDEs) and other developer tools.
9. Describe how the tool integrates with source code repositories, and which are supported.
10. Describe how the tool supports Single Sign On (SSO) capabilities.
11. **License Compliance Management:**
12. Describe how the SCA tool manages licensing issues associated with open-source components.
13. Describe how the SCA tool identifies licensing conflicts and ensures compliance with open-source licenses (commercial, GPL, MIT, etc.).
14. **Remediation and Mitigation Guidance:**
15. Describe the remediation and mitigation guidance the SCA tool provides when vulnerabilities or licensing issues are identified.
16. Describe the recommendations for alternative libraries or versions.
17. Describe how the tool mitigates risks when software is updated.
18. **Capability:**
19. Describe where the products can be implemented e.g. at the endpoint, network based, and/or cloud based.
20. 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/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.w3.org%2FTR%2FWCAG21%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463390497%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=e02p3b8aB5KB1xe2s6LB3ksZyRtoo09MCHTXDzO5E6Q%3D&reserved=0); b) Section 508: [**https://www.section508.gov/**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.section508.gov%2F&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463398992%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=pzgUTV7chyDcngdl6SvQJ3tAIz7RLJvSY02jf8A4SRg%3D&reserved=0); and c) Voluntary Product Accessibility Template (VPAT®): [**https://www.itic.org/policy/accessibility/vpat**](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.itic.org%2Fpolicy%2Faccessibility%2Fvpat&data=05%7C02%7Cstarr.christen%40nc.gov%7C3737b44528934d4e45f508dc3a2fddad%7C7a7681dcb9d0449a85c3ecc26cd7ed19%7C0%7C0%7C638449224463405831%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=5PxuYxDYvzebQ0oJ4qLv%2BXmBS25YhqJa3ms9L3r8c8c%3D&reserved=0)

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

1. **Experience:**
2. Summarize vendor’s experience providing the specified category products or services.
3. Include any external recognition or awards received in the past two years that indicate vendor’s marketplace position relative to its competitors.
4. **Support and Maintenance:**
5. 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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Assessment Methodology:**
5. Describe the service method used to conduct security program assessments.
6. Describe the evaluation of the current effectiveness of an organization's security posture.
7. Describe the frameworks or standards used for your assessments (e.g., NIST, ISO, CIS).
8. Describe tools used to conduct the assessments and any clean up methodology used to remove the tools from the system.
9. **Scope and Depth of Assessments:**
10. Describe the scope and depth of your security program assessments.
11. Describe the program areas covered by the assessment (e.g., policies, procedures, technical controls, incident response, training).
12. Describe how you ensure that assessments are comprehensive.
13. **Risk Identification and Analysis:**
14. Describe how the service identifies and analyzes risks within an organization's security program.
15. Describe how risks are prioritized.
16. Describe the criteria used to assess the potential risk impact.
17. **Recommendations and Roadmap Development:**
18. Describe how you provide recommendations and develop roadmaps for improving an organization’s security posture.
19. Describe how you ensure that recommendations are actionable, prioritized, and aligned with an organization's business objectives.
20. **Stakeholder Engagement and Communication:**
21. Describe the approach to engaging stakeholders during the assessment process.
22. Describe how findings and recommendations are communicated to both technical and non-technical stakeholders.
23. **Capability:**
24. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
25. Describe the scalability, interoperability, customization, and integration capabilities of your services.
26. 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.

1. **Experience and Key Personnel:**
2. 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).
3. Describe the vendor’s qualifications to perform the services specified in the category.
4. **Support and Maintenance:**
5. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.

1. **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:*

1. **Overview:**

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

1. **Technical Qualifications:**
2. **Assessment Scope and Techniques:**
3. Describe the scope of the application risk assessment services.
4. Describe the techniques used to identify and assess risks in both web-based and client-server applications.
5. **Vulnerability Identification and Prioritization:**
6. Describe how the service identifies vulnerabilities within applications.
7. Describe how vulnerabilities are prioritized based on their severity and potential impact on the organization.
8. **Secure Coding Practices and Review:**
9. Describe how the service evaluates the application's adherence to secure coding practices.
10. Describe how code reviews are performed.
11. Describe how you ensure that developers follow best practices to mitigate security risks.
12. **Compliance with Security Standards:**
13. Describe how the service ensures that applications comply with applicable security standards and regulations (e.g., OWASP Top 10, PCI DSS, HIPAA).
14. **Capability:**
15. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
16. Describe the scalability, interoperability, customization, and integration capabilities of your services.
17. 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.

1. **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.

1. **Support and Maintenance:**
2. 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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Testing Methodologies and Scope:**
5. Describe the penetration testing methods employed (e.g., black box, white box, grey box).
6. Describe the scope of your penetration tests.
7. 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).
8. Describe how you determine the boundaries of the testing environment.
9. Describe the methods used to evaluate the security of email systems.
10. Describe the identification of potential email vulnerabilities and threats.
11. Describe pen testing methods your team is capable of employing.
12. Describe your capabilities in performing tests of varying scopes.
13. 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).
14. **Compliance with Legal and Ethical Standards:**
15. 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).
16. Describe how you ensure that testing is conducted without disrupting an organization's normal business activities.
17. **Reporting and Debriefing:**
18. Describe the types of reports provided following a penetration test.
19. Describe how you debrief an organization on your penetration testing findings.
20. Describe the process of recommending remediation strategies for any discovered vulnerabilities.
21. Describe the assessment of an organization's capabilities to detect and prevent email-based threats, such as phishing, malware, and spam.
22. Describe the best practices and technologies recommended for threat detection and prevention.
23. **Tools and Technologies Used:**
24. Describe the tools and technologies used during penetration testing.
25. Describe how you stay current with the latest penetration testing tools and techniques.
26. Describe how you ensure email authentication protocols (e.g., SPF, DKIM, DMARC) and encryption methods are correctly configured and effective.
27. Describe how you ensure that sensitive information is protected and that content filtering rules are adequate.
28. **Client Collaboration and Communication:**
29. Describe the approach to client collaboration and communication throughout the penetration testing and email security assessment processes.
30. Describe the involvement of clients in planning, execution, and post-testing activities.
31. **Capability:**
32. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Readiness Assessment Framework:**
5. Describe the framework or methods used to assess an organization's incident response readiness.
6. Describe the evaluation of the current state of an organization's incident response plan, procedures, and capabilities.
7. **Tools and Resources:**
8. Describe the software or tools used in the assessment process.
9. Describe the evaluation of the tools and resources available to the incident response team.
10. Describe the determination of whether the tools and resources are adequate for effectively detecting, analyzing, and mitigating incidents.
11. **Metrics and Measurement:**
12. Discuss the metrics and measurement criteria used to assess incident readiness.
13. Describe how an organization's ability to respond to and recover from security incidents is measured.
14. **Compliance and Best Practices:**
15. 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.
16. **Capability:**
17. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
18. Describe the scalability, interoperability, customization, and integration capabilities of your services.
19. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Assessment Scope and Methodology:**
5. Describe the scope of your internal vulnerability assessment services.
6. Describe the methods used to identify vulnerabilities within the internal network.
7. Describe how you ensure all critical assets are covered.
8. **Vulnerability Scanning Tools and Techniques:**
9. Describe the tools and techniques employed for vulnerability scanning.
10. Describe how you ensure that the tools are current with the latest vulnerability signatures and scanning capabilities.
11. **Remediation Strategies and Guidance:**
12. Describe the remediation strategies and guidance provided by your service.
13. Describe how you assist an organization in developing a plan to address identified vulnerabilities effectively.
14. **Reporting and Documentation:**
15. Describe the types of reports and documents that Vendor provides following an internal vulnerability assessment.
16. Describe how you communicate findings and recommendations to both technical staff and executive leadership.
17. **Capability:**
18. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
19. Describe the scalability, interoperability, customization, and integration capabilities of your services.
20. 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.

1. **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.

1. **Support and Maintenance:**
2. 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:*

1. **Overview:**

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

1. **Technical Qualifications:**
2. **Assessment Methodology:**
3. Describe the methods used to conduct network architecture assessments.
4. Describe the methods used to conduct wireless network assessments.
5. Describe how you evaluate the current network design for potential vulnerabilities and compliance with best practices.
6. **Best Practices and Frameworks:**
7. Describe the best practices and frameworks (e.g., NIST, CIS, ISO/IEC) referenced when assessing network architecture.
8. Describe how you ensure that the network aligns with the standards adopted by the organization (e.g., NIST, CIS, ISO/IEC).
9. **Risk Identification and Analysis:**
10. Describe the identification and analysis of risks within the network architecture, including specific wireless network attacks such as unauthorized access and rogue access points.
11. Describe how these risks are prioritized based on their potential impact on an organization's operations and security posture.
12. Describe the evaluation of the effectiveness of encryption and authentication protocols used in the wireless network.
13. **Segmentation and Access Control:**
14. Describe the evaluation of network segmentation and access control strategies.
15. Describe the assessment of the effectiveness of these controls in limiting the potential spread of a breach.
16. Describe how you ensure that segmentation is effectively isolating sensitive data and systems from general user access.
17. **Security Device and Control Review:**
18. Describe review of the configuration and effectiveness of security devices and controls within the network (e.g., firewalls, intrusion detection/prevention systems, VPNs).
19. **Architecture Types:**
20. Describe your ability to assess operational technology network environments.
21. Describe your ability to assess wireless network environments.
22. **Physical Security for Wireless Network Assessments:**
23. Describe how physical security considerations are addressed in your wireless network assessments.
24. Describe how you evaluate the risks associated with the physical placement of wireless infrastructure.
25. **Capability:**
26. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
27. Describe the scalability, interoperability, customization, and integration capabilities of your services.
28. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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.

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Program Content and Structure:**
5. Describe the content and structure of your cyber security training and awareness programs.
6. Describe the topics covered in the training.
7. Describe how you ensure that the material is relevant and current with the latest email threat landscape.
8. **Customization to Organization's Needs:**
9. Describe how training programs are customized to the specific needs and risks of an organization.
10. Describe the assessment of an organization's unique vulnerabilities to tailor the training content.
11. **Engagement and Interactivity:**
12. Describe the methods used to engage users and to ensure interactivity during the training.
13. Describe how you make the training engaging and memorable to maximize retention of the information.
14. **Delivery Methods:**
15. Describe the various delivery methods available for your training programs (e.g., in-person sessions, webinars, e-learning modules).
16. Describe how you determine the most effective delivery method for an organization.
17. Describe any gamification or other engagement-promoting methodologies used.
18. **Behavioral Change and Metrics:**
19. Discuss how your programs aim to change user behavior regarding email security.
20. Describe the metrics used to track changes in user behavior and the program's impact on reducing email-based threats.
21. Describe your ability to construct and provide reports based on program metrics.
22. **Capability:**
23. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
24. Describe the scalability, interoperability, customization, and integration capabilities of your services.
25. 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.

1. **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.

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

1. **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:*

1. **Overview:**

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

1. **Technical Qualifications:**
2. **Implementation Strategy:**
3. Describe the approach to implementing cybersecurity systems such as SIEM, XDR, Email Security Systems, etc.
4. Describe the project management methodologies used to ensure timely and successful deployment.
5. **Integration with Existing Systems:**
6. Describe the process for integrating cybersecurity solutions with existing security tools and IT infrastructure, including switches, firewalls, operating systems, log collection software tools, etc.
7. Describe how logs and events from various sources are aggregated and normalized to provide comprehensive security insights.
8. **Configuration and Customization:**
9. Describe your process for the configuration and customization of cybersecurity systems.
10. Describe how correlation rules, dashboards, and alerts are set up to provide meaningful and actionable security insights.
11. Describe the customization options available to tailor the solutions to specific organizational needs.
12. **Performance Optimization:**
13. Describe how the performance of cybersecurity solutions are optimized during implementation.
14. Describe how you ensure that integrated solutions handle large volumes of data and provide timely analysis without impacting network performance.
15. **Compliance and Reporting:**
16. Describe how you configure cybersecurity systems to support relevant industry standards and best practices (e.g., NIST 800-137).
17. **Incident Response Integration:**
18. Describe the process for the integration of cybersecurity solutions with an organization's incident response processes.
19. Describe how you configure systems to facilitate rapid detection and response to security incidents.
20. **Ongoing Support and Maintenance:**
21. Describe the ongoing support and maintenance services provided to ensure effective and sustained use of cybersecurity solutions.
22. **Training and Knowledge Transfer:**
23. Describe the training programs available for client staff to ensure they are proficient in using and managing the implemented security systems.
24. Describe the knowledge transfer process to ensure clients can maintain and optimize their security systems post-deployment.
25. **Vendor and Third-Party Risk Management:**
26. Describe how the solution helps manage and mitigate risks associated with vendors and third parties.
27. Describe the processes and tools used to assess and monitor third-party security postures.
28. **Capability:**
29. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
30. Describe the scalability, interoperability, customization, and integration capabilities of your services.
31. 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.

1. **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.

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

1. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Incident Response Capabilities:**
5. Describe your incident response services.
6. Describe how you assist organizations in detecting, investigating, containing, eradicating, and recovering from cybersecurity incidents.
7. Describe your incident response methodology (i.e., the steps you take in a response).
8. **Response Time and Availability:**
9. Describe your incident response times and provisions for responding to incidents at a headquarters location and satellite facilities.
10. Describe how you ensure availability and rapid deployment of resources when an organization requires immediate assistance.
11. **Forensic Analysis and Evidence Preservation:**
12. Describe the service’s forensic analysis and evidence preservation capabilities.
13. Describe how you ensure that critical data is collected and handled in a manner that supports potential legal actions.
14. **Communication and Coordination:**
15. Describe the approach to communication and coordination during an incident response.
16. Describe the interaction with an organization's internal teams, external stakeholders, and law enforcement if required.
17. **Post-Incident Reporting and Debriefing:**
18. Describe the post-incident reporting and debriefing process.
19. Describe the types of reports and documentation provided.
20. Describe how you facilitate lessons learned and improvement of incident response plans.
21. **Remediation and Recovery Support:**
22. Describe the assistance with remediation and recovery efforts.
23. Describe strategies recommended for restoring systems and operations.
24. Describe how you assist in the prevention of future incidents.
25. **Capability:**
26. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
27. Describe the scalability, interoperability, customization, and integration capabilities of your services.
28. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Security Operations Center as a Service (SOCaaS):**
5. Describe your SOCaaS services.
6. Describe how you establish, manage, and operate SOCaaS, including the technology stack, staffing, and processes involved.
7. Describe the continuous monitoring capabilities provided by your SOCaaS.
8. **Threat Detection and Analysis:**
9. Describe the methodologies and tools used for threat detection and analysis.
10. Describe how you leverage threat intelligence to identify and mitigate threats in real-time.
11. Describe your process for analyzing security events and correlating data from various sources to detect potential threats.
12. **Incident Response Capabilities:**
13. Describe the incident response services within the SOCaaS framework.
14. Describe how you assist organizations in detecting, investigating, containing, eradicating, and recovering from cybersecurity incidents.
15. Describe the processes and technologies used to facilitate rapid incident response.
16. **Compliance and Reporting:**
17. Describe how the SOCaaS assists organizations with regulation and standards, , compliance, including PCI DSS, HIPAA.
18. Describe the reports and dashboards provided to clients.
19. **Integration and Customization:**
20. Describe how the SOCaaS integrates with existing security infrastructure and tools, such as SIEM, Endpoint Detection and Response (EDR), XDR, and other cybersecurity solutions.
21. Describe the customization options available to tailor the SOCaaS to specific organizational needs and security requirements.
22. **24/7 Monitoring and Support:**
23. Describe the 24/7 monitoring and support services provided by the SOCaaS.
24. Describe the process to ensure continuous coverage and rapid response to security incidents.
25. Describe the service level agreements (SLAs) related to response times and support availability.
26. **Threat Hunting and Proactive Measures:**
27. Describe the threat hunting capabilities and how they are integrated into your SOC services.
28. Describe the proactive measures taken to identify and mitigate threats before they impact the organization.
29. Describe the use of advanced analytics, machine learning, and other technologies in threat hunting.
30. **Training and Knowledge Transfer:**
31. Describe the training programs available for client staff to ensure they are proficient in working with SOCaaS services.
32. Describe your knowledge transfer process to ensure clients can maintain and optimize their security operations post-deployment.
33. **Scalability and Flexibility:**
34. Describe how the SOCaaS scales to accommodate organizations of different sizes, from small public entities to large agencies.
35. Describe the deployment options available, on-premises, cloud, hybrid, and how each option supports scalability and flexibility.
36. Describe the SOCaaS’ ability to adapt and grow with the evolving security needs of the organization.
37. **Capability:**
38. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
39. Describe the scalability, interoperability, customization, and integration capabilities of your services.
40. 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.

1. **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.

1. **Support and Maintenance:**
2. 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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Policy Development Expertise:**
5. Describe your expertise in developing security policies.
6. Describe how you ensure that the policies are comprehensive, clear, and aligned with an organization's business objectives and risk profile.
7. **Compliance Assessment and Gap Analysis:**
8. Describe the approach to conducting compliance assessments and gap analyses.
9. Describe how areas where an organization may not meet regulatory requirements are identified.
10. **Regulatory Compliance:**
11. Describe your expertise in cybersecurity regulatory compliance.
12. Describe how an organization is assisted in complying with relevant cybersecurity regulations and standards (e.g., HIPAA, NIST, ISO/IEC 27001).
13. Describe how you stay current with evolving regulatory requirements.
14. Describe the documentation and reporting provided to demonstrate compliance with regulations.
15. Describe how you ensure that documentation is thorough and audit ready.
16. **Stakeholder Engagement:**
17. Describe the approach to engaging stakeholders in the policy development and compliance process.
18. Describe how you ensure buy-in from various departments and levels within the organization.
19. **Customization of Security Policies:**
20. Describe the customization of security policies to fit the specific needs and context of an organization.
21. **Capability:**
22. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
23. Describe the scalability, interoperability, customization, and integration capabilities of your services.
24. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **Integration with SDLC:**
5. Describe how you ensure that security is a consideration from initial design through development, testing, deployment, and maintenance.
6. Describe the testing methodologies for application security, secure code reviews, and software development security.
7. Describe how you determine which methods to use based on the application's characteristics.
8. **Threat Modeling and Risk Assessment:**
9. Describe the approach to threat modeling and risk assessment within the SDLC.
10. Describe how you identify potential threats and vulnerabilities early in the development process.
11. **Tools and Techniques:**
12. Describe the tools and techniques used in software development, secure coding, or software vulnerability testing services.
13. Describe how you balance automated tools with manual expertise to ensure comprehensive coverage.
14. **Vulnerability Identification and Analysis:**
15. Describe how the service identifies and analyzes vulnerabilities within applications.
16. Describe classification of the severity of vulnerabilities.
17. Describe the standards used for assessment (e.g., OWASP Top 10, CWE/SANS Top 25).
18. **Secure Coding Practices:**
19. Describe the promotion and implementation of secure coding practices.
20. Describe the training and resources provided to development teams to enhance their understanding of security issues.
21. **Security Testing and Validation:**
22. Describe the security testing and validation strategies that your service recommends.
23. Describe how you ensure that security testing is thorough and effective at identifying vulnerabilities.
24. **Secure Architecture and Design Consulting:**
25. Describe assistance with secure architecture and design.
26. Describe how you ensure that security is built into the architecture of software applications.
27. **Remediation Support:**
28. Describe the provision of remediation support.
29. Describe assistance provided to developers to understand vulnerabilities and to implement effective remediation strategies.
30. **Capability:**
31. Describe where the services will be implemented e.g. at the endpoint, network based, and/or cloud based.
32. Describe the scalability, interoperability, customization, and integration capabilities of your services.
33. 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.

1. **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.

1. **Support and Maintenance:**
2. Describe the ongoing support, warranty and any training services provided to ensure effective and sustained use of your services.
3. **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:*

1. **Overview:**
2. Describe the service offering with a focus on how your product or services address the scope of work.
3. **Technical Qualifications:**
4. **DevSecOps Strategy and Approach:**
5. Describe the strategy and approach for integrating security practices into DevOps workflows.
6. Describe how you ensure that security is a seamless part of the development and deployment process.
7. **Security Automation in Continuous Integration / Continuous Deployment (CI/CD):**
8. Describe the automation of security within the CI/CD pipeline.
9. Describe the tools and technologies implemented to perform security checks during code commits, builds, and deployments.
10. **Collaboration Between Teams:**
11. Describe the facilitation of collaboration between development, operations, and security teams.
12. **Security Metrics and KPIs:**
13. Describe the security metrics and key performance indicators (KPIs) established to measure the effectiveness of DevSecOps practices.
14. Describe the tracking and reporting on these metrics.
15. **Capability:**
16. 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.

1. **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.

1. **Support and Maintenance:**
2. 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.

1. Describe how the Vendor will identify and mitigate hallucinations and ensure that GenAI data outputs are accurate and factual.
2. Describe how the Vendor monitors GenAI to ensure continued accurate performance over the lifetime of the contract.
3. 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 Product**s  **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.** |  |