



## Solicitation Addendum

**Solicitation Number:** ITS-500874-001  
**Solicitation Description:** Cybersecurity Professional Services RFP  
**Solicitation Opening Date and Time:** September 9, 2025, 2:00 PM ET  
**Addendum Number:** 1  
**Addendum Date:** August 18, 2025  
**Strategic Sourcing Specialist:** Allison.Howard@nc.gov

- 
1. This addendum must be returned properly executed with the bid prior to the bid opening date and time.
  2. The bid cannot be copyrighted. Do not mark any page as copyrighted etc.
  3. DO NOT MARK THE ENTIRE BID AS CONFIDENTIAL.
  4. Ensure that the contact for receipt of all documents is listed as a contact in Ariba.
  5. **Do not JPEG or lock your bid response.**
  6. A redacted bid copy is required if your bid has confidential information identified and marked as such in your bid response.
  7. All cybersecurity professional services must be based in the United States.
  8. Solicitation Section 5.2 Evaluation Criteria is hereby modified to read as follows:

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

- a. How well the Vendor's offer conforms with the specifications, **(Attachment I)**, ~~including risks associated with the Vendor's proposal (Attachment F)~~ and adherence to the Section 3.2 Security Specifications.

- b. How each Vendor’s offer compares with other Vendors’ offers.
- c. Financial Stability (**Attachment H**)
- d. Strength of references relevant to Specifications and Vendor Past Performance. (**Attachment G**)
- e. Total Cost of Ownership. (**Attachment D**)

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

9. The following are questions about the solicitation received from Vendors and the State’s response to those questions.

Question #	RFP Section	Vendor Question	State’s Response
1	2.1 Introduction, Page Number 4	The State’s RFP states that cybersecurity professional services are being solicited (i.e. implementation, deployment, and configuration type services). Can the State please confirm that offers for products and software (i.e. mobile device management solutions, software, products, etc.) should not be submitted at this time?	Reference bid Section 2.1 Paragraphs 3 & 4.
2	2.1 Introduction - Categories of Work	What types of training models will be sought and/or considered e.g., in person, platform-based delivery, other)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

3	3.2 Security Specifications	Can the state share any NC state-specific cybersecurity regulations that vendors must comply with?	Reference 3.3.9 Enterprise, Services, and Standards.
4	7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.	Are offshore resources permitted for any aspect of the project, such as development, testing, or support?	All resources must be based in the United States.
5	7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.	If so, are there any restrictions related to data handling, security, or compliance that vendors should be aware of?	All resources must be based in the United States.
6	7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.	Can vendors utilize resources outside the State for implementation and ongoing maintenance of the solution?	All resources must be based in the United States.
7	7.2 FINANCIAL STATEMENTS/ Page 19	The instruction states that The Vendor must provide evidence of financial stability by returning with its offer A) completed Financial Review Form (Attachment I), and B) copies of Financial Statements as further described below. Attachment I is submission Checklist, hence it seems it should be Attachment H, not Attachment I. Please confirm if this is a typo.	The Financial Review Form is Attachment H.
8	7.2 FINANCIAL STATEMENTS/ Page 19	The instruction states that The Vendor must provide evidence of financial stability by returning with its offer A) completed Financial Review Form (Attachment I), and B) copies of Financial Statements as further described below. Attachment H needs to be submitted in Excel format. Do we need to include the financial statements as a separate	The Financial Review Form is Attachment <b>H</b> . Reference Attachment J: Submittal Checklist. Your proposal should be in PDF format before uploading it to Ariba.

		documents or can submit as a separate document along with our original electronic offer?	
9	7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY RESERVED.	If a vendor requests modifications to the unlimited liability clause in the standard state contract, would this impact their eligibility for consideration?	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.
10	7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY RESERVED.	Will the State accept redlines or proposed revisions to the standard contract terms as part of the negotiation process?	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.
11	Attachment C- Historically Underutilized Businesses/ Page#42	Does the State have any preference for HUB-certified businesses? If yes, please clarify how such certification will be considered during the evaluation process.	The State invites and encourages participation by HUB Vendors.
12	ATTACHMENT C: DESCRIPTION OF OFFEROR/ Page#41	Vendors are asked to provide their North Carolina Secretary of State Registration Number in this form. Could NCDIT please clarify whether vendors must be registered with the NC Secretary of State at the time of proposal submission, or if registration can be completed upon award?	Reference Section 6.2.10 Vendor Registration with the Secretary of State.
13	ATTACHMENT F: LOCATION OF WORKERS UTILIZED BY VENDOR/ Page# 45	In this attachment, it stated that 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. Does this requirement indicate that offshore and hybrid delivery models are acceptable under this RFP, provided	All resources must be based in the United States.

		that the vendor discloses the relevant details as requested?	
14	ATTACHMENT G: REFERENCES/ Page# 46	Will NCDIT accept past performance references from commercial clients whose projects are of highly relevant and comparable scope, breadth, depth, and complexity of work delivered to what is outlined in the RFP?	Relevant commercial client references are acceptable.
15	Attachment H: Financial Review Forms/ Page 48	The instruction states that 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. As per the submission instructions, we need to submit one consolidated offer, titled as Original Electronic Offer and one redacted copy of Electronic offer. As Excel document cannot be included in the Original Offer, this will make it the third document to be submitted along with- Original Offer, redacted offer, and Attachment H. Please clarify.	Your proposal should be in PDF format before uploading it to Ariba.
16	ATTACHMENT J: SUBMITTAL CHECKLIST	Under SECTION 3: VRARs and Original Bid Copy, are we required to include the entire RFP document within our response? If yes, considering that this could impact the flow and readability of our submission, would it be acceptable to provide the VRARs and the original RFP document as a separate attachment alongside our original offer?	No. The items mentioned are the last items of the original offer and there should be no impact on the flow and/or readability of the submission.
17	ATTACHMENT J: SUBMITTAL CHECKLIST/ Page #72; Under SECTION 3: VRARs and Original Bid Copy,	Are bidders required to include the entire RFP document within one's response file? If yes, considering that this could impact the flow and readability of the submission, would it be acceptable to provide the VRARs	No. The items mentioned are the last items of the original offer and there should be no impact on the flow and/or readability of the submission.

		and original RFP document as a separate attachment alongside one's original offer?	
18	ATTACHMENT J: SUBMITTAL CHECKLIST/ Page#72	One item—Signed Bid Execution Page—is listed under SECTION 1: General Response. We couldn't locate any document with this title. Could you please confirm whether this refers to the cover page of the RFP document?	The RFP cover page is where the proposal must be executed.
19	2.1- Introduction/ Page# 5	It is stated in this section that Vendors currently awarded on Security Assessments and Testing, (918A), contract must bid on this solicitation to continue providing cybersecurity professional services to the State of North Carolina. - Could NCDIT please provide the incumbents details currently on the 918A contract? Additionally, please clarify how many vendors NCDIT intends to award under this new solicitation.	Reference Section 2.5, Paragraph 5 and webpage address <a href="https://it.nc.gov/documents/files/918a-web-summary/open">https://it.nc.gov/documents/files/918a-web-summary/open</a>
20	5.2/ Page# 12	One of the evaluation criteria is - How each Vendor's offer compares with other Vendors' offers and 20 points are assigned to it. Could the NCDIT please elaborate on: 1) Are there any aspects of the response that will be emphasized under this criteria in addition to listed criteria? 2) Can the state provide further guidance to understand better how to best align a proposal response to maximize scoring in this area?	No. The state will not provide additional information regarding this evaluation criteria.
21	6.3.3./Page# 18	It is stated in this section that Vendors must include all the pages of this solicitation in their response. Should vendors include all 73 pages of RFP in our response or do we submit it as a separate document with completed	Reference Attachment J Submittal Checklist.

		RFP Cover Page? Please clarify.	
22	General	<p>Please clarify how the following security services are currently being delivered and/or if the state intends to deliver going forward (e.g., remote, on-site, hybrid; centralized vs. decentralized):</p> <p>Security Program Assessment and Consulting Services, Application Risk Assessment and Consulting Services, Penetration Test and Security Assessment Services, Security Incident Readiness and Response Services, Vulnerability Management Services, Network Security Services, Security Awareness and Training Services, Security Implementation and Integration Services, Security Operations Services, Governance, Risk, and Compliance Services, Application Security Services, DevSecOps and Security Automation Services, Identity and Access Security Services, Data Security Services, Cloud Security Services, Third-Party Risk Management Services, Mobile Security Services, Critical Infrastructure and Operational Technology (OT) Security Services, Endpoint Security Services</p>	The State requires bidding Vendors to provide this information in their proposals.
23	General	What are the strategic outcomes the State expects from security program assessments—maturity benchmarking, roadmap creation, or compliance validation?	The State will not provide this information.
24	General	Can the State provide an estimated budget or funding range allocated for this project and contract?	This information is not available.

25	General	Is the project fully funded, or are there pending legislative approvals that could impact on the procurement timeline?	This RFP is to prequalify vendors for future cybersecurity SOW based professional services.
26	General	If vendors develop custom modules or enhancements, will the State retain full ownership of the source code and intellectual property?	Reference Attachment B, Section 1, Subsection 39 Patent, Copyright, and Trade Secret Protection.
27	General	Are there existing vendors or contractors currently providing these cybersecurity professional services?	This is a new contract.
28	General	If so, will the incumbent vendor(s) be eligible to rebid?	All interested Vendors must bid.
29	General	What are the most pressing cybersecurity challenges/ pain points the State is facing today that vendors should prioritize in their solutioning?	The State will not provide this information.
30	RFP Section 6.2.2	Can the question deadline be extended?	The State does not agree to extend the Vendor question deadline.
31	III. Category Specific Scopes of Work Category A: Security Program Assessment and Consulting Services	Historically how many assessments and their sizes were conducted by the state agencies in the last five (5) years? This is required to gauge the types of assessment required by the agencies.	This information is not available.
32	Attachment D: Category Cost Forms	Cost Proposal Template: The Cost Proposal Template is asking for "hourly rate" for Small, Medium, Large, and X-large enterprises. Can you confirm that you are looking for a blended hourly rate? Please confirm the blended hourly rate can be a range?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
33	Attachment G: References	For references, can we provide names upon request?	References must be provided with the bid.
34	Acceptance of Offer, pg. 1	Will the State agree to Vendor SAAS Licenses as primary in the order of precedence pursuant to Vendor's Offer?	No. This RFP is <b>not</b> for SAAS.

35	Section 2.1, pg. 7	Will the State agree to change 'will make non-responsive' to 'may make non-responsive' with respect to exceptions to terms and conditions in order to provide the State additional flexibility to make an award?	No. Exceptions taken to the terms and conditions will make a vendor's offer non-responsive.
36	Section 7.4 VENDOR'S LICENSE OR SUPPORT AGREEMENTS, pg. 19	Can the State confirm whether this is a placeholder for the incorporation of Vendor SAAS License agreements? Please explain how Vendor licenses will be incorporated into the award.	No. This RFP is <b>not</b> for SAAS.
37	Sec. 2 Standards, pg. 24	Will the State remove "and NC State Chief Information Officer's (CIO) policy or regulation" from this section, with respect to commercial SAAS subscription license services contracts, since there is no basis to tailor delivery of commercial services to NC CIO policy and regulations?	No. This RFP is <b>not</b> for SAAS.
38	Sec. 2 Standards, pg. 24	Since SAAS subscription license vendors' deliverables are per commercial documentation only and they will not be conducting operation, certification, testing and inspection against RFP specifications, will the State agree to make the below language inapplicable to such SAAS subscription license contracts? "Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility	No. This RFP is <b>not</b> for SAAS.

		specifications.”	
39	Section 9, ACCEPTANCE PROCESS, pg. 25	Will the State confirm that this section does not apply to SAAS subscription license services?	Yes. This RFP is <b>not</b> for SAAS.
40	Section 10 Payment Terms, pg. 25	Will the State confirm that payment is net due upon invoice in the case of SAAS subscription license services?	This RFP is <b>not</b> for SAAS.
41	Section 18 Confidentiality, pg. 28	Will the State revise the following language to reflect the fact that the delivery of SAAS subscription license services by a vendor does not result in any derivative works licensed to the state during the term of service? <i>“Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.”</i>	No. This RFP is <b>not</b> for SAAS.
42	Section 19, Default, pg. 28-29	Will the State agree to make this clause inapplicable to SAAS subscription license service vendors in favor of the exclusive warranties, support services and applicable SLAs under a SAAS subscription license agreement?	No. This RFP is <b>not</b> for SAAS.
43	Section 39 PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION, pg. 33	Will the State agree to clarify this section to make clear that, with respect to SAAS subscription license services, in no event will the State acquire any license rights other than a right to use the services during the subscription term?	No. This RFP is <b>not</b> for SAAS.
44	Section 39 PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION, pg. 33	Will the State confirm that, with respect to the following, SAAS subscription license service vendors shall have the limited rights to use data in performance of the services as provided in the vendor’s license	This RFP is <b>not</b> for SAAS.

		agreement? <i>“Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor.”</i>	
45	Section 39 PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION, pg. 34	With respect to SAAS subscription license service vendors, will the State agree to delete the below remedy language as it compromises revrec for such vendors to have independent services subject to termination where such services were not the subject of infringement? <i>“If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.”</i>	No. This RFP is <b>not</b> for SAAS.
46	Section 42 TRANSITION ASSISTANCE, pg. 35	Will the State agree to render this clause N/A to SAAS subscription license vendors since transition assistance will not apply at termination of a subscription license agreement?	No. This RFP is <b>not</b> for SAAS.
47	VENDOR'S REPRESENTATION (a), pg. 35	Will the State agree to delete the IP rights warranty in this section in favor of the IP rights infringement indemnity under Attachment B Section 1,	No.

		subsection 39?	
48	Section 2.1, page 5	<p>In Section 2.1, on page 5 of the RFP, it states that, "...the State is unable to provide user specific architecture, software, hardware, or other specific information across all agencies and other governmental entities that will be eligible to use the Cybersecurity Services Contract."</p> <p>Two paragraphs later, the RFP also states, "Governmental entities using the contract will provide more specific information, using Scopes of Work (SOWs) for procurement of cybersecurity professional services."</p> <p>Since this very important "more specific information," will be unknown to the Offerors on the date that the Proposals are submitted, Governmental entities using the contract will not be able to order services off of the master contract without first supplying, "more specific information," to the down-selected vendors. As a result of the missing information, certain terms and conditions in the proposed master contract will require varying alternate terms at the order level. Therefore, would the State please amend the RFP so that the terms of the individual order-level procurements take precedence over conflicting terms found in the proposed master contract by revising the order of precedence on page 1 of the RFP to list the negotiated purchase order SOW</p>	No. The State will not amend the RFP.

		<p>terms and conditions higher on the order of precedence than the terms presented in the RFP?</p> <p>For clarity, here's an example of what such amended RFP should look like:</p> <p><b>ACCEPTANCE OF OFFER</b>  <i>If any or all parts of this offer are accepted, an authorized representative of the North Carolina Department of information Technology ("NCDIT") shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows:</i></p> <p><u>(1) Scope (or Statement) of Work negotiated between the Government entity using the contract and the Vendor prior to the issuance of any purchase order under the contract,</u>  <u>(2) Best and Final Offers, if any,</u>  <u>(3) Special terms and conditions specific to this RFP,</u>  <u>(4) Specifications of the RFP,</u>  <u>(5) the Department of Information Technology Terms and Conditions,</u>  and  <u>(6) the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).</u></p>	
49	Attachment F: Location of Workers Utilized by Vendor	Are there any functional service areas (Categories) that are precluded from using delivery roles or centers outside the US? If so, which Categories?	All resources must be based in the United States.
50	2.3 Contract Term, page 8	We acknowledge that the contract term will be five years. What	Reference Section 2.4 Effective Date.

		estimated start date (month) should all vendors use in their proposal?	
51	General	A lot of the services described in the provided Categories could also overlap or be included in Category I: SOC Services (for example, Mobile Security Services, OT Security Services, etc). Are vendors to assume that these services/categories would NOT be included in Category I: SOC Services?	Vendors are required to respond to all questions in each of their bid categories.
52	Attachment D: Category Cost Form, Page 43 Attachment A: Definitions, #12, Page 23	Not all of the subcategory entity sizes within the Category D Cost Form, in alignment with Definition #12, can be measured by number of end points to determine the scope and complexity of the engagement. Can NCDIT please provide further metrics and detail on what constitutes a Small, Medium, Large, and X-Large/Enterprise for each of the subcategories in D? Does NCDIT expect that pricing is reduced as the category size increases?	Vendors should provide competitive pricing using the entity sizes provided by the State.
53	Attachment J: Submittal Checklist, Section 3: VRARs and Original Bid Copy, Page 73  3.2 Security Specifications, Page 10	Can NCDIT please clarify that VRARs are not required for vendors replying to this solicitation as this is for services only? No software will be included in this Proposal.	Reference Section 3.2.1 Solutions Hosted on State Infrastructure.
54	2.3 Contract Term, Page 8	Will vendors be given the opportunity to revisit pricing at completion of the initial 5 (five) year term, prior to renewals?	The State will negotiate pricing with Vendors before any contract renewal.
55	RFP Section - PROCUREMENT SCHEDULE	Would the State of North Carolina consider granting an extension to the proposal submission deadline?	The State does not agree to extend the Vendor question deadline.

	Page Number - 4		
56	RFP Section - INSTRUCTIONS FOR OFFER SUBMISSION Page Number - 17	Are the cover page and table of contents excluded from the overall page count limit?	The State did not specify a page limit count.
57	RFP Section - INSTRUCTIONS FOR OFFER SUBMISSION Page Number - 17	May we include additional pages for abbreviations and references, and will those be excluded from the stated page limit?	The State will not accept nor evaluate additional pages.
58	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number - 7	Can any portion of the scope of services be performed offshore, or is the work required to be fully performed onshore (within the U.S.)?	All resources must be based in the United States.
59	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number - 7	Can vendors bid on individual sections of the category (e.g., in Category F- Network and Cloud Security Services only "Cloud Security") or must they cover multiple?	No. Vendors must be able to provide all the services in the category.
60	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number - 7	Will preference be given to vendors offering multiple categories?	No.
61	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number -7	Will a master contract/ IDIQ be issued to the selected vendors or separate SOWs required per engagement?	This is an RFP for SOW based cybersecurity Professional Services.
62	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number -7	What is the turnaround expected for responding to each SOW?	Turnaround of a SOW will depend on the future professional services being performed.
63	RFP Section - SECURITY	For incident response, what is the expected time frame for deploying on-	Vendors are required to provide their response times for these services.

	INCIDENT READINESS AND RESPONSE SERVICES Page Number - 54	site resources?	
64	RFP Section - COST OF VENDOR'S OFFER Page Number- 11	Is this a fixed-price, time-and- materials, or rate card-based contract?	Fixed price.
65	RFP Section - COST OF VENDOR'S OFFER Page Number- 11	Are there budget caps for each category?	No.
66	RFP Section - Penetration Test and Security Assessment Services Page Number - 53	Will the State provide legal safe harbor documentation for offensive testing (e.g., pen tests)?	All resources must be based in the United States.
67	RFP Section - Penetration Test and Security Assessment Services Page Number - 53	Is compliance with NCGS §14-454 and related statutes enforced as a strict liability?	Yes. Vendors must comply with all applicable statutes.
68	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number - 7	Are vendors permitted to use offshore resources (for any part of the work including assessments, development, SOC monitoring, or support services)? If permitted are there any specific countries that are approved? And do this restriction only apply to subcontractors or only prime vendors?	All resources must be based in the United States.
69	RFP Section - CATEGORY SPECIFIC SCOPES OF WORK Page Number - 7	Are vendors allowed to retain data for research or reporting purposes?	Reference Section 18 Confidentiality and Section 4: Supplemental Terms and Conditions Applicable to Artificial Intelligence ("AI").
70	PROCUREMENT SCHEDULE	Can the due date be extended 2 weeks?	The State does not agree to extend the Vendor question deadline.

71	Attachment D Page 43.	Can discount off list be used either in lieu of or in addition to hourly rates?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
72	RFP Section 1.2, Page 4	Please clarify if the State anticipates issuing task orders for each category independently or combining multiple categories under a single task order.	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
73	RFP Section 5.1, Page 27	For categories with a wide range of potential staffing levels (e.g., Security Operations Services, Category I), should NTE rates be calculated as per-labor-hour for a single resource, or should vendors propose rates that anticipate multiple resources working simultaneously under a single task order?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises
74	RFP Section 5.2, Page 28	Will the State provide estimated annual hours or level-of-effort ranges per category to allow vendors to model realistic cost and staffing assumptions in Attachment D?	No.
75	RFP Section 5.6, Page 30	Please clarify whether the RFP's task order process is envisioned to be coordinated through NCDIT or issued directly by individual agencies, as this affects project management planning.	Each governmental entity will individually issue their SOW.
76	RFP Section 6.3, Page 33	Please confirm whether vendors may propose additional in-scope services beyond the minimum listed requirements for each category.	Vendors may only bid on the Cybersecurity professional services listed.
77	RFP Section 5.4, Page 29	Will the State require security clearances for certain categories (e.g., Critical Infrastructure/OT Security) at the time of award, or will clearances be allowed to be obtained post-award for assigned personnel?	Reference Section 7.8 Security and Background Checks.

78	Attachment I, Page 1	For KPI tracking and reporting, does the State have a preferred reporting template or tool to be used by vendors, or may vendors propose their own performance reporting format?	Reference Section 7.16 Contracts Administration.
79	Cybersecurity Products Contract2.0 Purpose of RFP/page 4	Will offerors/awardees on this Services contract be eligible for award of the contemplated products contract?	No. Vendors will be required to submit a bid for the cybersecurity products procurement.
80	Consent to Subcontract Attachment B - Section 1: #4 Subcontracting/page 24	Are Vendors allowed to subcontract services?	Reference Section 4 Subcontracting.
81	General	Can you provide an asset inventory (counts, types, criticality tags) for each entity size (Small / Medium / Large / X-Large) that the State expects us to cover?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
82	General	Will the State furnish a network topology & data-flow diagram (including cloud, OT and on-prem segments) before SOW finalization?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
83	General	Does the State have a preferred control & maturity framework (e.g., NIST CSF vs ISO 27001) that must anchor all findings and road-maps, or should we recommend one for each category?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

84	General	For categories that involve tooling (VA scanners, SAST/DAST, EDR, SIEM, MDM, etc.), do you require us to use your existing licenses, deploy our own stack, or present both options?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
85	General	Should retainer-style services (e.g., IR on-call, third-party risk monitoring) be priced hourly or as fixed monthly retainers?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises
86	General	Does "travel must be included in pricing" mean all work can be performed remotely unless on-site is explicitly requested?	No. That is not what that statement means. However, some work can be performed remotely.
87	Category A – Security Program Assessment	Is the desired output a one-time baseline report or a multi-year maturity roadmap with quarterly re-assessments?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
88	Category A – Security Program Assessment	Will you supply existing policy corpus for gap analysis, or should we conduct document discovery workshops?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
89	Category B – Application Risk Assessment	Approx. how many applications (web, mobile, thick-client) per year; average LOC/codebase size?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

90	Category B – Application Risk Assessment	Do you already run SCA/SAST tools; if so, which and who owns the license?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
91	Category B – Application Risk Assessment	Is grey-box access (source code + running instance) guaranteed, or do we assume black-box only?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
92	Category C – Penetration Testing	Target mix by percentage (external / internal / cloud / OT / IoT / physical / social-engineering)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
93	Category C – Penetration Testing	Acceptable testing windows / freeze periods for critical prod systems?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
94	Category C – Penetration Testing	Is a full-scope red-team with phishing and physical intrusion envisaged, or limited to technical vectors?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

95	Category D – Incident Readiness & Response	Expected SLA for onsite presence once an incident is declared?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
96	Category D – Incident Readiness & Response	Maximum retainer hours per year the State will pre-purchase?	This information is not available.
97	Category E – Vulnerability Management	Preferred scanner engines (Tenable, Qualys, Rapid7) and current license counts?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
98	Category E – Vulnerability Management	Required scan cadence for external vs internal assets?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
99	Category E – Vulnerability Management	Does the State already run patch-management infrastructure, or must we propose one?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
100	Category F – Network Security	Current firewall vendors and policy volumes to be migrated/optimized?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
101	Category F – Network Security	Any mandate to align with the State’s Zero-Trust reference architecture version?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
102	Category G – Security Awareness & Training	Estimated learner population and segmentation (employees, contractors, K-12 staff, etc.)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
103	Category G – Security Awareness & Training	Frequency of phishing simulations per user per year?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
104	Category I – SOC / MDR	Do you already operate a state-run SOC that we will augment, or is this net-new?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
105	Category I – SOC / MDR	Preferred SIEM/XDR stack (Splunk, MS Sentinel, etc.) and daily EPS/GB ingest rate?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

106	Category J – GRC	Which regulations drive highest priority (CJIS, IRS Pub 1075, HIPAA, FERPA, PCI)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
107	Category J – GRC	Is tool-based GRC platform (e.g., Archer, ServiceNow IRM) already in place?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
108	Category K – Application Security	CI/CD platforms in use (Azure DevOps, GitHub Actions, Jenkins, etc.)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
109	Category L – DevSecOps & Automation	Toolchain names for IaC (Terraform, Pulumi, Bicep) and container orchestrators (AKS/EKS)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
110	Category M – Identity & Access	Current IdP(s) (Azure AD, Okta, Ping) and target architecture for Zero-Trust identity.	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

111	Category M – Identity & Access	Are you seeking cloud-hosted PAM or on-prem vault?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
112	Category M – Identity & Access	Directory forest health: any Active Directory consolidation efforts planned?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
113	Category N – Data Security	Is there an existing enterprise data classification schema, or should we build one?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
114	Category N – Data Security	DLP coverage expectation: email + endpoint + cloud SaaS, or phased?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
115	Category N – Data Security	Regulatory drivers for privacy (NC identity-theft statute, GLBA, etc.)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

116	Category O – Cloud Security	Primary cloud providers (Azure Gov, AWS GovCloud, GCP) and subscription count.	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
117	Category O – Cloud Security	Should CSPM tooling be agentless or agent-based?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
118	III. Cat. A, Pg. 51	What is the preferred cybersecurity framework for the state?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
119	III. Cat. A, Pg. 51	Does the state have a pre-existing GRC tool? What are the names of those tools? Should vendor be prepared to provide tools?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
120	III. Cat. B, Pg. 52	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
121	III. Cat E, Pg. 55	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional

			<p>services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
122	III. Cat H 2.a.i, Pg. 59	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
123	III. Cat M, Pg. 64	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
124	III. Cat N, Pg. 65	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
125	III. Cat O, Pg. 66	What cloud platforms does the state use?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
126	III. Cat P, Pg. 67	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional</p>

			<p>services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
127	III. Cat S, Pg. 70	Does the state have pre-existing tools in place? What are the names of those tools? Should vendor be prepared to provide tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
128	Attachment G: References, Pg. 46	Instructions are to provide references "per subcategory" but the response refers to categories not subcategories. In this case is it DITs expectation that respondents provide 2 references per category identified in Attachment I: Scope of Work and Specifications?	Two references per category.
129	Several, All Category descriptions, Section 4 Key Personnel, Pg. Several	Can DIT clarify whether the resumes submitted for key personnel are expected to reflect actual individuals who will be assigned to the engagement upon award, or if representative resumes that illustrate the qualifications of potential staff are acceptable?	The bid requires you to describe the experience, titles etc of your key professional staff expected to perform the services. Resumes of actual individuals will be required at the SOW level.
130	6.3.3 Offer Submittal, page 17.	Will the State of North Carolina consider extending the RFP due date to September 30th?	The State does not agree to extend the Vendor question deadline.
131	Attachment D: Category Cost Forms, page 43.	Must the vendor follow the sample S/M/L/XL model or may the vendor use it's own models? For example, IP ranges 1 – 100 devices, 101-500 devices, etc.	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
132	Attachment D: Category Cost Forms, page 43.	Is the vendor pricing expected to be Not to Exceed pricing?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.

133	Attachment D: Category Cost Forms, page 43.	Are there any prevailing wage rates that need to met in North Carolina?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
134	Attachment D: Category Cost Forms, page 43.	Should the costs only be expressed in a Full Time Equivalent hourly rate? Or may they be expressed as a monthly recurring charge?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
135	Attachment D: Category Cost Forms, page 43.	Will the vendor need to create a separate and unique Cost Form for each category? So, Category A will be its own Cost Form, Category B will its own Cost Form and so on?	Yes. A separate cost form is required for each bid category.
136	Attachment E: Vendor Certification Form, page 44.	If awarded some or all of the responded categories, is the vendor precluded from bidding on the subsequent cybersecurity solution/product RFP? If so, are they only precluded in the categories they were awarded?	No.
137	CATEGORY A: Security Program Assessment and Consulting Services, Page 53	What frameworks would the State like included?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
138	CATEGORY A: Security Program Assessment and Consulting Services, Page 53	Does the State have a particular risk analysis methodology that they prefer the vendor align to?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
139	Category F: Network Security Services, page 56	What are some examples of network security control implementation tasks and deliverables that would support North Carolina's agencies and departments?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
140	Category F: Network Security Services, page 56	What are some examples of firewall management and optimization tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
141	Category F: Network Security Services, page 56	What are some examples secure remote access tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
142	Category F: Network Security Services, page 56	What are some examples of DNS Security tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
143	Category F: Network Security Services, page 56	What are some examples of Email Security tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
144	Category F: Network Security Services, page 56	What are some examples of Web Security Service tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
145	Category F: Network Security Services, page 56	What are some examples of implementing and managing web security gateway and proxy service tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
146	Category F: Network Security Services, page 56	What are some examples of SSL/TLS inspection and certificate management tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
147	Category F: Network Security Services, page 56	Are there any legacy systems or outdated infrastructure that need special attention?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
148	Category F: Network Security Services, page 56	What is the organization's risk tolerance for network vulnerabilities?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
149	Category F: Network Security Services, page 56	Which regulatory frameworks or industry standards must the assessment align with?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
150	Category F: Network Security Services, page 56	Are there specific compliance audits or certifications required as part of this assessment?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
151	Category F: Network Security Services, page 56	How are compliance gaps currently tracked or reported?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
152	Category F: Network Security Services, page 56	What is the organization's strategy for continuous monitoring and threat detection?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
153	Category F: Network Security Services, page 56	Does the organization prefer a phased approach (e.g., initial assessment, design, implementation) or a single comprehensive evaluation?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
154	Category F: Network Security Services, page 56	Are there specific methodologies or frameworks the organization prefers (e.g., NIST, MITRE ATT&CK)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
155	Category F: Network Security Services, page 56	How should the assessment address integration with existing security tools or processes?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
156	Category F: Network Security Services, page 56	What metrics or KPIs will be used to evaluate the effectiveness of the network security assessment?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
157	Category F: Network Security Services, page 56	How will the organization track the implementation of recommendations?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
158	Category F: Network Security Services, page 56	Does the organization have a process for continuous monitoring of network security?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
159	Category F: Network Security Services, page 56	How are changes to the network architecture or security controls tracked and documented?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
160	Category F: Network Security Services, page 56	Are there existing segmentation policies or tools in place (e.g., firewalls, intrusion detection systems, network access control)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
161	Category F: Network Security Services, page 56	How are network zones currently defined (e.g., by function, data sensitivity, user roles)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
162	Category F: Network Security Services, page 56	What tools are used for traffic analysis, log correlation, or monitoring inter-segment communication?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
163	Category F: Network Security Services, page 56	What is the organization's stance on zero trust architecture (ZTA) in segmentation design?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
164	Category F: Network Security Services, page 56	Does the organization have a preference for on-premises, cloud-based, or hybrid segmentation solutions?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
165	Category F: Network Security Services,	How frequently are network vulnerability scans and penetration	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	page 56	tests conducted (e.g., quarterly, annually, continuously)?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
166	Category F: Network Security Services, page 56	How frequently are network vulnerability scans and penetration tests conducted (e.g., quarterly, annually, continuously)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
167	CATEGORY H: SECURITY IMPLEMENTATION AND INTEGRATION SERVICES, page 59	Will the vendor be providing an EDR solution or only staff to operate existing SIEM tech stacks?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
168	CATEGORY H: SECURITY IMPLEMENTATION AND INTEGRATION SERVICES, page 59	How many EDR solutions will the vendor be responsible for operating? What are they?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
169	Category I: Security Operations Center (SOC) Services, page 60	Is the state ok with a remote, US based workforce to support 24x7 SOC monitoring?	All resources must be based in the United States.
170	Category I: Security Operations Center (SOC) Services, page 60	Will the vendor be providing a SIEM or only staff to operate an existing SIEM tech stack?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
171	Category I: Security Operations Center (SOC) Services, page 60	How many SIEM solutions will the vendor be responsible for operating? What are they?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
172	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of Security Operation Center (SOC) Service tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
173	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of Threat Detection and Analysis tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
174	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of Threat Intelligence Services tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
175	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of Alert Management and Response Services tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
176	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of SOC Integration Services tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
177	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of SOC Training and Knowledge Transfer tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
178	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of SOC Reporting and Metrics tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
179	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of SOC Insider Threat Management tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
180	Category I: Security Operations Center (SOC) Services, page 60	What are some examples of SOC Standalone SIEM and Security Analytics tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
181	Category I: Security Operations Center (SOC) Services, page 61	What regulatory requirements must the State adhere to?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
182	Category I: Security Operations Center (SOC) Services, page 61	Does the State or individual agencies have GRC platforms in place?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
183	Category O: Cloud Security Services, page 66	What are some examples of Cloud Security Posture Management tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
184	Category O: Cloud Security Services, page 66	What are some examples of Cloud Access Security tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
185	Category O: Cloud Security Services, page 66	What are some examples of Cloud Workload Protection tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
186	Category O: Cloud Security Services, page 66	What are some examples of Cloud Security Architecture tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
187	Category O: Cloud Security Services, page 66	What are some examples of Cloud Security Operations tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
188	CATEGORY P: Third-Party Risk Management Services , Page 67	Does the State / individual agencies have third party monitoring platforms in place?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
189	Category Q: Mobile Security Services, page 68	What are some examples of Mobile Threat Detection and Response tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
190	Category Q: Mobile Security Services, page 68	What are some examples of BYOD and COU device security tasks and deliverables that would support North Carolina's agencies and departments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
191	Section 2.0 Purpose of RFP, page 4.	To ensure our response aligns with your expectations, could you clarify whether you're seeking purely project-based professional services (e.g. consulting, implementation support), or if you're also open to—or expecting—proposed solutions that include technology components, managed services, or ongoing support?	Reference Attachment I.
192	Section 5.2 Evaluation Criteria, page 12.	Will the vendor be evaluated and awarded based on all of the categories they submitted responses? Or will the vendor be award a category that is best for the State of North Carolina, even if they are not awarded other submitted category responses?	Vendors are evaluated on responded categories.
193	Section 5.2 Evaluation Criteria, page 12.	Will the vendor be evaluated on selected Technical Qualifications in a Category they elect to provide a response? For example, if the vendor only elects to provide a response to Zero Trust Architecture and User Behavior Architecture, would they be negatively evaluated for not responding to the other Technical Qualifications?	Vendors must respond to the entire category.
194	Vendor Readiness Assessment Reports (VRARs)	Do we have to respond to this document, considering there is no solution that we are proposing. It is a capability ask and hence only capability responses with rates will be provided.	Reference Section 3.2.1 Solutions Hosted on State Infrastructure.
195	DM2069_285_4_RFP_Word_Attachments_CJ	Please let us know the roles, years of experience etc., details that you are looking for in the cost forms. The table that is provided has Category names	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.

		and hourly rate column to be filled. But we need to know what roles and what level of experience you are looking at.	
196	Category N_ Data Security Services	What key data protection regulations must be addressed in this engagement?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
197	Category N_ Data Security Services	What geographies does your organization support in or store/process data in?	All resources must be based in the United States.
198	Category N_ Data Security Services	Are there industry-specific compliance requirements to consider?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
199	Category N_ Data Security Services	Do the services require cross-border data transfer assessments or controls?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
200	Category N_ Data Security Services	Are there any preferred or mandated tools for data classification, labeling, or retention being looked for the role?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

201	Category N_ Data Security Services	What are the key outcomes you expect from this advisory engagement?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
202	Category N_ Data Security Services	What types of sensitive data (e.g., PII, PHI, PCI, IP, source code) does your organization collect, process, or store?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
203	Category N_ Data Security Services	What tools or processes are currently in place for data discovery across on-premises, cloud, and SaaS environments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
204	Category N_ Data Security Services	Do you have an enterprise-wide data classification framework? If yes, how is it enforced?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
205	Category N_ Data Security Services	Do you have an internal Public Key Infrastructure (PKI)? If yes, is it self-managed or outsourced?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

206	Category N_ Data Security Services	Which tools are being used for PKI and CLM.	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
207	Category N_ Data Security Services	What is the current certificate lifecycle process – is it manual or automated?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
208	Category N_ Data Security Services	Are you using certificates for device/user authentication, mutual TLS, VPN, Wi-Fi, or code signing?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
209	Category N_ Data Security Services	What challenges are you facing in managing SSL/TLS certificates across hybrid/cloud environments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
210	Category N_ Data Security Services	How do you track, monitor, and renew certificates today? Is there a centralized inventory?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

211	Category N_ Data Security Services	Are you looking to integrate CLM with CI/CD pipelines, DevOps tools, or infrastructure	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
212	Category N_ Data Security Services	What are your current risks or incidents related to expired/misconfigured certificates?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
213	Category N_ Data Security Services	Which privacy regulations are applicable to your organization? (e.g., GDPR, CCPA, HIPAA, DPDPA, ISO 27701)	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
214	Category N_ Data Security Services	Do you currently conduct DPIAs, PIAs, or maintain Records of Processing Activities (ROPA)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
215	Category N_ Data Security Services	How do you manage data subject requests (DSRs), consent, and preferences? Are these automated?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

216	Category N_ Data Security Services	Do you have data flowing across borders? If so, how are transfer risks and legal obligations (e.g., SCCs, BCRs) managed?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
217	Category N_ Data Security Services	Are you looking to integrate Data Protection, PKI, and CLM with existing systems like IAM, SIEM, DLP, CMDB, or cloud security tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
218	Category O: Cloud Security Services	<p>What are the cloud service providers used by the State of North Carolina? Please share the list of current security tools/controls (native and third party) that is implemented which needs is in scope for security support.</p> <p>a) Firewalls:  b) Network &amp; host-based IDS / IPS:  c) Web Application Firewall:  d) Antimalware:  e) SAST/DAST/SCA/Infra Scan, Pentest etc:  f) DLP/CASB: (Data security details data classification, labeling etc.):  g) Encryption: (Data at rest/transit, encryption standard etc):  h) Identity and Access Management (IGA/SSO/MFA/Access Control etc.):  i) Email Security:  j) Container security:  k) Compliance (HIPAA, PCI etc):  l) SIEM monitoring:  m) CWPP tool:  n) CSPM tool:</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

		p) Cloud compliance monitoring tool:	
219	Category O: Cloud Security Services	a) What is the maturity level of your current cloud infrastructure ? b) What is the Supplier's cloud security future roadmap? c) Kindly share insights on security initiatives covering : Technology & strategy roadmaps (Zero Trust, Network transformation (SASE), Cloud).	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
220	Category G :Security Awareness and Training Services	a) Do you have any training platform in place? If yes, please provide the platform name ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
221	Category G :Security Awareness and Training Services	b) What types of training sessions are you expecting to provide (in-person, virtual, e-learning, self-paced)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
222	Category G :Security Awareness and Training Services	c) If any content library subscription is available? If yes, having a defined list of training areas(modules) to be covered part of the training ? Whether training content finalization and its readiness is in scope of the supplier ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
223	Category G :Security Awareness and Training Services	d) Do you currently run phishing simulations? If yes please confirm on this - How often are they conducted(monthly, quarterly) ? Which is the platform used for	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

		Phishing simulation ?	Describe your ability to provide the professional services requested in the bid specifications.
224	Category G :Security Awareness and Training Services	e) Are there any specific compliance standards you need to meet (e.g. ISO 27001, HIPAA, PCI-DSS etc.)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
225	Category G :Security Awareness and Training Services	f) Approx .total no: of employees/contractors in scope for the training ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
226	Category G :Security Awareness and Training Services	g) List of locations in scope for the training ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
227	Category G :Security Awareness and Training Services	h) Whether all the in scope employees/contractors whether having access to the training platform if not please provide a split of users by having access to the online training platform and no: of users do not have access to the training platform to provide class room based trainings ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
228	Category G :Security Awareness and Training Services	i) How often are the class room training sessions conducted(monthly/quarterly)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
229	Category G :Security Awareness and Training Services	j) Whether role based training content is already available ? Whether the supplier is expected to support role based training content readiness ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
230	Category G :Security Awareness and Training Services	k) List of languages to be covered for the training ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
231	Category G :Security Awareness and Training Services	l) Location from where the services to be delivered out - onsite client location remote offshore ? If onsite location name ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
232	Category J. Governance, Risk, and Compliance Services	a) Please clarify on the applicable state / federal / global information security standards / frameworks / regulations needing compliance management support (such as ISO 27001, PCI DSS, NIST CSF, GDPR etc.). Is there existing common security control framework for all compliance requirements?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
233	Category J. Governance, Risk, and Compliance Services	b) Is there a GRC tool/platform currently used for security , governance and reporting , If yes the tool name?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
234	Category J. Governance, Risk, and Compliance Services	c) What is the current level of automation and AI/Gen AI adoption for security, governance and compliance areas?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
235	Category J. Governance, Risk, and Compliance Services	d) What is the approx.no: of cyber security policies currently available?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
236	Category J. Governance, Risk, and Compliance Services	e) Do you have a defined cyber risk management program with control framework, operating model, risk management process, KPIs, metrics with on-going security & compliance reporting ?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
237	Category J. Governance, Risk, and Compliance Services	f) What are the major challenges related to security and compliance? Do you have a risk remediation program with remediation progress reporting?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
238	Category J. Governance, Risk, and Compliance Services	h) What is the current level of cyber security maturity in a scale of 1 to 5?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
239	Category P : Third-party Risk Management Services	a) How many suppliers are in scope for vendor risk assessment ? How are these Vendor Organizations geographically spread and vendor risk category (Critical /High risk/medium risk/low risk)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the bid specifications.
240	Category P : Third-party Risk Management Services	b) Does client have documented vendor risk management methodology with vendor tiering, defined vendor assessment questionnaire for each of the categories, vendor assessment approach (onsite/remote) etc?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the bid specifications.
241	Category P : Third-party Risk Management Services	c) What is the approx number of vendor assessments performed per year ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the bid specifications.
242	Category P : Third-party Risk Management Services	d) What is annual rate of vendor on-boardings and off-boardings?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the bid specifications.
243	Category P : Third-party Risk Management Services	e) Do you have a TPRM platform for performing the assessment? if yes what is the platform name?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the

			bid specifications.
244	Category P : Third-party Risk Management Services	f) What is the level of automation of TPRM activities?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
245	Category F,H,I, DM2069_285_2_FIN AL_Cybersecurity_Professional_Services_DIT_500874001	What is the scope in the Network Security Services, Security Implementation and Integration Services, Security Operations Services & Endpoint Security Services category? Whether the scope is to do implementation of these Security tools or it will be just a Management of these tools is in scope?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
246	Category F, DM2069_285_2_FIN AL_Cybersecurity_Professional_Services_DIT_500874001	What are the network security tools which will be in the scope of the RFP under Category F?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
247	Category F, DM2069_285_2_FIN AL_Cybersecurity_Professional_Services_DIT_500874001	If implementation is the scope of the RFP, will supplier going to bring the tools or will it be provided by North Carolina?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
248	Category F,H,I, DM2069_285_2_FIN AL_Cybersecurity_Professional_Services_	If Implementation of Security tools is in scope, then who will own the licenses of these security tools?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional</p>

	DIT_500874001		<p>services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
249	Category H, DM2069_285_2_FIN AL_Cybersecurity_Pr ofessional_Services_ DIT_500874001	Please let us know whether the tools which include SIEM, EDR, XDR, DLP & Email Security Platform have already been implemented?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
250	Category H, DM2069_285_2_FIN AL_Cybersecurity_Pr ofessional_Services_ DIT_500874001	If implementation of SIEM, EDR, XDR, DLP & Email Security Platform is in the scope of the RFP, then please let us know whether supplier will going to bring the tools or it will be provided by North Carolina itself?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
251	Category I, DM2069_285_2_FIN AL_Cybersecurity_Pr ofessional_Services_ DIT_500874001	Please let us know whether North Carolina already SOC team in place have who is doing the incident management?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
252	Category I, DM2069_285_2_FIN AL_Cybersecurity_Pr ofessional_Services_ DIT_500874001	Is the expectation from supplier is to bring in the Commercial TI feed or North Carolina already have the Threat Intelligence subscription?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
253	Submission Date	Any possible of getting few weeks extension?	The State does not agree to extend the Vendor question deadline.
254	In Section 3: VRAR and Original Bid	You mention: "All pages of the original Bid document." Could you please	A copy of the original bid document must be included with your proposal.

	(page 73)	clarify what specifically we are required to include in our submission of the original Bid? Are you referring to the full document as originally submitted, or just specific sections?	
255	Additionally, in Section 4: Redacted Bid (page 73)	If we have no content that requires redaction, should we omit this section from our submission entirely?	Correct.
256	Section Number: III. Category A: Security Program Assessment and Consulting Services Page: 51-52	Are cross-agency assessments or shared services environments (e.g., identity, networking, or cloud services managed by NCDIT) a component of assessments, or all engagements agency-specific?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
257	Section Number: III. Category A: Security Program Assessment and Consulting Services Page: 51-52	Are there existing deliverable formats, reporting templates, or compliance documentation systems that should be planned for use or integration with proposed deliverables, or are vendors expected to propose their own?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
258	Section Number: III. Category A: Security Program Assessment and Consulting Services Page: 51-52	Are optional post-assessment services expected as a component of the proposal (e.g., roadmap execution, remediation support), or is the scope strictly limited to assessment and recommendations?	No. Only the professional services listed in Attachment I.
259	Section 2.1 Introduction: SCOPES Page Number 07	Can we use the same reference for each category to showcase our experience?	Vendor must have performed the category services for the reference within three years from the date of the bid posting.
260	Section 2.1 Introduction: SCOPES Page Number 07	Can we use commercial clients as a reference?	Relevant commercial client references are acceptable.
261	RFP Section: HISTORICALLY	Is HUB a mandatory requirement?	No.

	UNDERUTILIZED BUSINESSES Page Number 42		
262	RFP Section: General Requirements	What was the annual spend for the previous year on this Project?	New contract.
263	RFP Section: General Requirements	If this is a new Contract, what is the annual Budget for this?	Yes. Annual budget is not applicable.
264	RFP Section: General Requirements	Are you open to a hybrid delivery model with a mix of offshore and onshore resources?	All resources must be based in the United States.
265	RFP Section: General Requirements	Work will be Onsite or Remote ?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
266	Attachment B: Department of IT Terms and Conditions – Section 5 Travel Expenses (p. 24)	The RFP states “All travel expenses should be included in the Vendor’s proposed costs.” Given that each SOW/contract awarded under the master contract will vary in scope and location(s) of work, we are unsure how to estimate travel in order to account for it in our proposed rates. Would the state reimburse pre-approved vendor travel at cost, and will this be specified in the SOWs on a case-by-case basis?	Travel must be included in your proposed cost.
267	Attachment B: Department of IT Terms and Conditions – Section 5 Travel Expenses (p. 24)	Will remote work be allowed when possible, or will all work be performed onsite? If onsite, will contractors be quartered in NC facilities or will they need their own office?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

<p>268</p>	<p>Attachment E: Vendor Certification Form (p. 44)</p>	<p>Item 4 on the VCF states “As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.” Since our company is registered on the State of North Carolina eVP vendor portal, does this mean we are registered with the NC Secretary of State or is that a separate process?</p>	<p>No. Reference Attachment E for NC Secretary of State registration.</p>
<p>269</p>	<p>Section III. CATEGORY SPECIFIC SCOPES OF WORK, beginning on Page 51. All categories: 3) Experience and Key Personnel: a) Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services. Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work</p>	<p>Specific resources are not assigned until a project is planned and dated, is an overview of staff capabilities for each category requested acceptable? if no, how should vendor express compliance and expertise across many resources without providing individual specific resumes.</p>	<p>The bid requires you to describe the experience, titles etc of your key professional staff expected to perform the services. Resumes of actual individuals will be required at the SOW level.</p>

	(SOW).		
270	Attachment B: Department of Information Technology Terms and Conditions. Page 24. Section 1, Item 4. Subcontracting	Can you please clarify whether all subcontractors need to be identified at time of our proposal response or does that occur as individual subcontractors are required to complete a future project.	Reference Section 4 Subcontracting.
271	Section 7.2 Financial Statements, Page 19.  b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.	If a private company provides a written statement per the RFP requirements, is there any other financial data required? If so, please specify.  Additionally, would this letter be provided in lieu of Attachment. H: Financial Review Form?	Audited financial statements are required. Your CPA must certify that those statements were not prepared for b) to apply.  Attachment H must be submitted.
272	Attachment D. Category Cost Forms, Page 43	Is it ok to submit multiple hourly rates for different skillsets required, or is only one hourly rate acceptable?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
273	Attachment G. References, Page 46	Is there a preference or requirement that references be from state and local government?	No.
274	Section 3.2 Security Specifications, Page 10	It states that "Upon request, Vendors shall provide a current independent 3rd party assessment report". Will you execute an NDA in order for the Vendor to submit one of the 3rd Party	Reference Section 18 Confidentiality.

		assessment report options?	
275	CATEGORY A: SECURITY PROGRAM ASSESSMENT AND CONSULTING SERVICES	<p>What is the current security program maturity level? Has a formal assessment been done before?</p> <p>What is driving this engagement (e.g., compliance requirement, cyber incident, grant funding, internal audit)?</p> <p>Are there specific business objectives or pain points the agency wants addressed beyond compliance?</p> <p>Does the agency already follow a specific primary framework, or is it looking to transition to one?</p> <p>Which framework(s) take priority—NIST CSF, NIST 800-53, ISO 27001, CIS Controls—or a hybrid approach?</p> <p>Are there mandated state or federal security requirements (e.g., CJIS, HIPAA, IRS 1075, FedRAMP)?</p> <p>Will current security policies, procedures, and risk registers be provided for review?</p> <p>Does the agency have up-to-date asset inventories, data flow diagrams, and network architecture documentation?</p> <p>What compliance or certification reports (e.g., SOC 2, ISO 27001, state audits) are available for reference?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

		<p>Will interviews be conducted with both technical and business staff?</p> <p>What is the preferred deliverable format—formal report, scorecard, heatmap, roadmap?</p> <p>Should recommendations be prioritized by risk, cost, or compliance alignment?</p> <p>Is a remediation roadmap with timelines and resource estimates required?</p> <p>Will the final deliverable be presented to executive leadership, the board, or public oversight bodies?</p> <p>Does “consulting” mean ongoing advisory after the assessment or only during the engagement?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
<p>276</p>	<p>CATEGORY C: PENETRATION TEST AND SECURITY ASSESSMENT SERVICES</p>	<p>What is the primary goal—compliance validation, real-world attack simulation, control effectiveness testing, incident response evaluation, or executive risk awareness?</p> <p>Is the focus on specific threat actors (e.g., nation-state, ransomware gangs, insider threats)?</p> <p>Is the engagement intended to meet a regulatory requirement (e.g., CJIS, PCI DSS, HIPAA, IRS 1075)?</p> <p>Should the test measure detection, response, and containment (purple team focus) or purely exploitability?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

		<p>Are there strict limitations on exploit attempts in production systems?</p> <p>Is a “stop on impact” protocol required if service degradation is detected?</p> <p>Should the red team operate with full stealth (covert) or partial coordination with defenders (purple team)?</p> <p>Are there hours of operation restrictions (e.g., business hours only, nights/weekends allowed)?</p> <p>Will live malware, ransomware simulants, or C2 infrastructure be permitted?</p> <p>Should the exercise include initial access + lateral movement + exfiltration, or just initial compromise?</p> <p>Should the red team test incident detection and response by remaining undetected for a period of time?</p> <p>Are penetration test tools required to be approved by the agency before use?</p> <p>Should findings be mapped to NIST, MITRE ATT&amp;CK, CVSS, or another standard?</p> <p>Is a full exploit narrative with screenshots required, or just vulnerability lists?</p> <p>Should the final report include remediation guidance, risk scoring, and a retest to validate fixes?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
--	--	---	--

		<p>Is an executive presentation or board-level briefing required in addition to the technical report?</p> <p>Should deliverables be classified for restricted internal use, or is a summary needed for public/legislative reporting?</p> <p>Are there any requirements/limitations that we need to be aware of in deploying vulnerability assessment tools (i.e. segmentation).</p> <p>Do you want both authenticated and unauthenticated vulnerability assessments?</p> <p>Do you want social engineering to be part of the testing engagement? Including emails? phone calls?</p> <p>Will the security operations team be informed beforehand (assumed breach) or kept unaware (true blind test)?</p> <p>Will the red team coordinate with the agency's incident response team to measure readiness?</p> <p>Are there legal constraints on certain types of testing (e.g., phishing government officials, law enforcement systems)?</p> <p>Is formal authorization required for each phase of testing (Rules of Engagement sign-off)?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
--	--	---	--

		<p>Are there data handling requirements (e.g., FedRAMP, ITAR, state data protection laws) for test artifacts?</p> <p>Do you want physical testing of any locations?</p>	
<p>277</p>	<p>CATEGORY J: GOVERNANCE, RISK, AND COMPLIANCE SERVICES</p>	<p>What are the primary drivers for engaging GRC services—regulatory audit readiness, internal governance improvement, or recent security incidents?</p> <p>Does the agency already have a formal governance framework in place (e.g., COBIT, NIST RMF, ISO 27001)?</p> <p>Are there known policy or compliance gaps that have been identified in previous audits or assessments?</p> <p>Does the agency want GRC services to focus on building foundational capabilities, or maturing existing ones?</p> <p>Does the agency have an existing policy framework or library, and when were policies last reviewed/updated?</p> <p>Are policies centrally maintained or distributed across different departments/agencies?</p> <p>Should policies be aligned to specific frameworks (e.g., NIST CSF, ISO 27001, CIS Controls)?</p> <p>Should the engagement include standards and procedures in addition to policies?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

		<p>Will policies need to be tailored for different audiences (technical staff vs. non-technical employees)? Is there an expectation for policy training and awareness sessions after development?</p> <p>Which specific regulations apply to the agency (e.g., CJIS, HIPAA, IRS 1075, PCI DSS, FISMA, state-level mandates)?</p> <p>Are there multiple overlapping compliance requirements that need to be mapped together?</p> <p>Is the agency currently under active audit or preparing for a specific certification/attestation?</p> <p>Should compliance services include gap analysis, compliance monitoring, or audit support?</p> <p>Will the GRC engagement include creating a compliance calendar and ongoing tracking process?</p> <p>Should we provide compliance mapping between different frameworks for efficiency?</p> <p>Does the agency currently have a formal risk management process (risk register, scoring methodology, reporting)?</p> <p>Should the engagement align risk management to a specific framework (e.g., NIST RMF, ISO 27005, FAIR)?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
--	--	--	--

		<p>Is there a defined risk appetite or tolerance from executive leadership?</p> <p>Are both cybersecurity risks and business/operational risks to be considered?</p> <p>Should risk assessments include vendor/third-party risk management?</p> <p>Is the expectation to build an ongoing risk program or to perform a point-in-time assessment?</p> <p>Should deliverables include policy documents, risk registers, compliance gap reports, and roadmaps?</p> <p>Is a prioritized remediation plan required for compliance and risk gaps?</p> <p>Should all deliverables be mapped to specific framework controls for traceability?</p> <p>Is the agency expecting editable templates for future self-maintenance of policies and risk registers?</p>	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
<p>278</p>	<p>Purpose of the RFP, Category Specific Scopes of Work, Page 7</p>	<p>Would the State consider adding a specific scope of work around cyber resiliency including business continuity and disaster recovery?</p>	<p>No.</p>
<p>279</p>	<p>Attachment D: Category Cost Forms, Page 43</p>	<p>The pricing structure provided seems to be a fit for some of the services, but not all the services being requested would be priced based on these entity sizes. Will there be a consideration or an amendment to provide a pricing model more suitable for more</p>	<p>The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises</p>

		traditional delivery methods by either an established rate card or a blended rate?	
280	Attachment D: Category Cost Forms, Page 43	Do we have flexibility in responding to category service pricing in other formats that would be more suitable to the particular category?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises
281	Attachment D: Category Cost Forms, Page 43	Is the State looking for an hourly rate or a total Not To Exceed price for the category service purely based on the Entity Sizes and is a range of estimated pricing acceptable?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises
282	Attachment D: Category Cost Forms, Page 43	The form indicates that "A separate cost form is required for each bid category". However, the table included indicates that multiple categories will be included in a single table. Would the State like vendors to a) Fill out a single table with rows corresponding to each category or b) create a separate table for each category?	A separate cost form is required for each bid category. A Word version of the form is provided for editing.
283	Pg 10	For penetration testing services where a vendor-provided device is connected to the State's internal network, does the State consider this to fall under "Solutions Hosted on State Infrastructure" in Section 3.2.1, and therefore require a Vendor Readiness Assessment Report (VRAR) at time of offer? If the vendor's SOC 2 Type II audit includes organizational-level controls (e.g., device management, monitoring, access control), could this report satisfy any part of the security review, or is a full VRAR still required for the pen testing device setup?	Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission.
284	Pg 10	Section 3.2.1 of the RFP outlines VRAR requirements specifically for	Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission.

		<p>“Solutions Hosted on State Infrastructure.” If a vendor’s SaaS platform is fully hosted and managed by the vendor, with no deployment into or integration with State-hosted systems, can the State confirm that a VRAR is not required at time of offer submission?</p> <p>The vendor will provide a current SOC 2 Type II audit covering the platform and organizational security controls. Our understanding is that Section 3.2.2 (Solutions Not Hosted on State Infrastructure) is marked “Reserved,” and therefore no VRAR requirement applies in that case.</p>	
285	Pg 33	<p>Section 39(a) grants the State a perpetual, royalty-free, worldwide license to vendor technology contained in Services or Deliverables. If a vendor offers a SaaS solution where the software is hosted entirely by the vendor (i.e., not delivered or installed on State systems), can the State confirm that such SaaS platforms—including underlying code, models, and tools—are not considered “Deliverables” or “vendor technology” subject to licensing under this clause?</p> <p>Additionally, since Attachment B, Section 43 renders all clickwrap agreements void, vendors are unable to rely on them to preserve standard IP protections. To avoid unintended transfer or licensing of a vendor-hosted, preexisting IP, would the State consider revising or clarifying Section 39 to expressly exclude</p>	This RFP is <b>not</b> for SAAS.

		vendor-hosted SaaS platforms and preexisting technology from the scope of licensed rights?	
286	Pg 43	Can we use ranges for pricing? The price of an engagement can change depending on multiple components, not just size of the engagement.	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises
287	Pg 43	Many of the catalog security services listed in the RFP are typically delivered using a combination of professional services and software tools. In practice, this approach is essential for effective, timely, and cost-efficient execution—such as in assessment, monitoring, automation, or reporting activities. While we understand this RFP is for “services,” can the State confirm that vendors may include the use of software as part of their service delivery, where such software supports or enables the delivery of the underlying professional services?	No.
288	Pg 43	Attachment D requests hourly rates for each service category. However, certain services—such as risk assessments or third-party risk management—are often delivered using a combination of professional services and software access, where pricing is based on a fixed subscription model rather than hourly rates. Can the State clarify how vendors should present pricing for offerings that are best structured as fixed or subscription-based (rather than hourly)? Would it be acceptable to include such pricing in the “Additional Information” column, or should vendors submit an attachment	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.

		alongside the required hourly rates to describe these alternative pricing structures?	
289	RFP Section: 3.2 Page Number: 10	Is a VRAR needed for services that do not require any software solutions to be hosted by state (or vendor); e.g., Categories A, B and O listed on Page 7, where work is performed on state infrastructure?	Yes. Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission.
290	RFP Section: 3.2 Page Number: 10	For purely services-based offerings (e.g., Categories A, B and O on Page 7, where work is performed on state infrastructure, with no dependency on vendor infrastructure), is there a need for FedRamp, SOC2, HITRUST of vendor infrastructure? Please note that having these security audit requirements would be a very high bar for many highly qualified micro and small businesses that can provide strong value to state via their consulting services.	The Section 3.2 requirement to provide third party assessment when requested remains unchanged.
291	2.0 PURPOSE OF RFP, 2.1 INTRODUCTION, Page 4	Please confirm that the scope of this RFP is limited to consulting style professional services only, and that managed cybersecurity services (such as managed firewall, managed endpoint protection, etc) and other cybersecurity service products are out of scope and will be addressed in the referenced separate, future RFP?	Confirmed.
292	ATTACHMENT D: CATEGORY COST FORMS Page 43	Related to the first question, in the event that traditional managed services should be include with this RFP, and due to the fact that ATTACHMENT D: CATEGORY COST FORMS only allows for Not to Exceed Hourly Rate pricing, how should Vendors provide service specific pricing such as price per	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.

		license, cost based on throughput, etc.?	
293	3.2 SECURITY SPECIFICATIONS 3.2.1 SOLUTIONS HOSTED ON STATE INFRASTRUCTURE, Page 10	Please confirm that if the professional service(s) included in the Vendor's response do not include technologies hosted on the state infrastructure, then the Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") is not required with offer submission.	Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission.
294	Section 7.14, Page 21	Is the expectation that Special Terms and Conditions will be defined and negotiated in the downstream specific SOWs that will be written against this purchasing vehicle?	The terms and conditions are defined in this RFP.
295	Section 2.5, Page 8	For clarity, is the expectation that this RFP will serve as the Term Contract upon down select and will that Term Contract be the primary contracting document under which each downstream SOW is written?	Each SOW will incorporate the terms and conditions of the RFP.
296	Section 5.3, Page 12	For Clarity from a definitional standpoint, are vendors correct to assume that BAFO will result in the downstream Statements of Work? If not, where do Statements of Work fit into the order of precedence?	Each SOW will incorporate the terms and conditions of the RFP.
297	Attachment B, Section 1, subsection 4 Subcontracting, Page 24	In providing complete copies of all subcontractor agreements per this section, are vendors correct to assume that they may redact those portions of said subcontractor agreements that are confidential between the vendor and their subcontractor (i.e. cost/pricing)?	No.
298	Attachment B, Section 1, Clause 10, Page 26	If more than 30 days is requested by the Agency, is the expectation that this will be defined in the downstream SOW and thereby take precedence over the 30 days in the contract?	No.

299	Attachment B, Section 1 (22), Page 30	What will be the State's indemnification responsibilities and liability under the contract, or will they be defined in the downstream SOWs?	The State does not indemnify Vendors.
300	Attachment I, Category G	Can Security Awareness and Training services be performed by offshore resources?	All resources must be based in the United States.
301	Section 7.14, Page 21	After pool establishment, will vendors be expected to compete for all applicable task orders in categories awarded, or only those they elect to pursue?	Agencies and governmental entities will select the Vendor to work with.
302	Section 6.0, Page 15	Beyond the Statewide Data Classification and Handling policy referenced, are there minimum-security control baselines (e.g., encryption standards, log retention, incident response timelines) that apply across all categories and will be enforced in downstream orders?	Reference Subsection 3.3.9 Enterprise, Services, and Standards.
303	Attachment F, Location of Workers, Page 18	Does Attachment F apply uniformly across the vehicle's full term? How should vendors report post-award changes in worker location (e.g., periodic certification vs. change notices)?	All resources must be based in the United States.
304	Attachment B, Section 1, Page 24	Are background checks, CJIS, or other clearances required at award, or only when specified by an individual task order? Will the State publish the screening standard and timing?	Reference Section 7.8 Security and Background Checks
305	Section 5.5, Page 13	Redacted Bid Copy (Ariba) Should the redacted copy mirror the original proposal's structure and be uploaded as one consolidated file in Ariba Section 5.5, and are there any file-size or page limits we should observe?	Yes. The maximum file size for electronic submittal is 100 MB.

306	Attachment E, Vendor Certification, Page 20	Vendor Certification (E-Verify, Conflict of Interest) Please confirm the timing and evidentiary requirements for E-Verify and conflict-of-interest compliance at award and for each task order.	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.
307	Section 4, Page 11	Pricing and Compensation For professional services categories, will pricing be evaluated on labor rate cards, fixed-fee deliverables, or both? Will the State set rate caps or annual escalation limits in the Term Contract?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
308	Section 4, Page 11	Pricing and Compensation For on-site work, will travel be reimbursed per State per-diem or actuals, and will those terms be standardized in the vehicle or defined per task order?	Travel must be included in your proposed cost.
309	Section 5.3, Page 12	Statements of Work Will the State establish standard deliverable acceptance criteria (e.g., review periods, defect remediation timelines, dispute steps) that apply across categories, or should vendors propose acceptance criteria within Attachment I responses?	That information will be in the SOW.
310	RFP Schedule Q&A, Page 4	Q&A Please confirm the Q&A deadline (date/time) and whether follow-up clarifications will be accepted after the initial window closes, for example in response to late addenda.	Reference RFP Schedule. There is no scheduled Q & A follow-up.
311	Attachment I, Category E, Page 50-51	Is the State expecting vendors to use State-provided vulnerability Management tooling (e.g., scanners, ticketing) or to propose and operate vendor-provided tools, and how will licensing be handled at the task-order level?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

312	Attachment I, Category E, Page 50-51	Will authenticated scanning be required for servers, workstations, network devices, and cloud resources, and can the State provide service accounts/privileged credentials where necessary?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications
313	Attachment I, Category E, Page 50-51	Please confirm scan frequency and maintenance windows by agency (e.g., continuous, weekly, monthly), and whether emergency out of cycle scans can be initiated by the vendor.	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
314	Attachment I, Category E, Page 50-51	What is the State's standard severity definitions and remediation SLAs for vulnerabilities, and should vendors propose default SLAs if none are mandated?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
315	Attachment I, Category E, Page 50-51	How should scan results be integrated with the State's ticketing system (e.g., ServiceNow), and will standard field mappings and APIs be provided?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
316	Attachment I, Category E, Page 50-51	For cloud platforms, will the State provide read-only access and required permissions to enumerate assets, or should vendors assume agent-based discovery?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

317	Attachment I, Category E, Page 50-51	How should false positives and accepted risk be handled—does the State require a formal risk acceptance workflow and POA&M updates per finding?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
318	Attachment I, Category E, Page 50-51	Are there requirements for data residency, encryption, and retention of scan artifacts and vulnerability data stored in vendor tools or repositories?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
319	Attachment I, Category G, Page 54-55	Please confirm LMS technical requirements (e.g., SCORM 1.2/2004, xAPI/cmi5 support) and whether integration with the State's SSO (e.g., Entra ID) will be required.	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
320	Attachment I, Category G, Page 54-55	Are simulated phishing campaigns allowed on State domains, and if so, will the State provide whitelisting, sending domains, and target user populations per campaign?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
321	Attachment I, Category G, Page 54-55	What accessibility, localization, and reading level standards must content meet (e.g., WCAG 2.1 AA, multilingual support), and should vendors provide translations as part of base scope?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

322	Attachment I, Category G, Page 54-55	What learner privacy and data handling requirements apply (e.g., storage location for PII, reporting granularity), and will the State require anonymized or identifiable performance data?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
323	Attachment I, Category G, Page 54-55	Will the State prescribe minimum training frequencies, completion thresholds, and KPI reporting (e.g., phish prone rate, repeat clickers), or should vendors propose targets?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
324	Attachment I, Category G, Page 54-55	Who owns IP for any custom training content developed under this vehicle, and may the vendor reuse derivative materials outside of the State?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
325	Attachment I, Category J, Page 57-58	Which control frameworks and risk methodologies should vendors align to (e.g., NIST CSF/80053, CIS, ISO 27001, FAIR), and will the State provide an enterprise control catalog?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
326	Attachment I, Category J, Page 57-58	Does the State require use of a standard GRC platform (e.g., ServiceNow, Archer) for policy management, risk registers, POA&Ms, and evidence, or should vendors propose a platform agnostic approach?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

327	Attachment I, Category J, Page 57-58	Will the State publish standard report templates and deliverables (e.g., policy updates, risk assessments, compliance mappings), or should vendors propose formats for approval?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
328	Attachment I, Category J, Page 57-58	How should interagency variances be handled—will governance artifacts be standardized statewide, or tailored per agency with a common baseline?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
329	Attachment I, Category J, Page 57-58	What are the expectations for regulatory and audit support (e.g., participation in onsite audits, evidence production SLAs), and how will such support be scoped and priced?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
330	Attachment I, Category J, Page 57-58	What are the classification, retention, and residency requirements for governance artifacts and compliance evidence stored in vendor systems or repositories?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
331	Attachment I, Category S, Page 66-67	Is the endpoint security platform (e.g., EDR/AV) State standard and provided by the State, or should vendors propose tooling and associated licenses at task order stage?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

332	Attachment I, Category S, Page 66-67	Please confirm in scope operating systems and device types (Windows, macOS, Linux, mobile/IoT) and whether on and off network devices are included.	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
333	Attachment I, Category S, Page 66-67	What telemetry, data retention, and privacy constraints apply to endpoint agent data (e.g., process, DNS, file metadata), and will the State provide data handling standards?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
334	Attachment I, Category S, Page 66-67	What are the expectations for containment and response authority (e.g., isolate host, kill process, quarantine file), and are change control approvals required prior to action?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
335	Attachment I, Category S, Page 66-67	Should vendors assume comanaged operations with State SOC/IR teams, including integration with the State SIEM/SOAR, or propose a fully managed model with runbooks?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
336	Attachment I, Category S, Page 66-67	Will patch and configuration management (e.g., OS and third-party applications, disk encryption, application control) be included under this category, and if so, what compliance baselines (e.g., CIS) should be assumed?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

337	Attachment I, Category S, Page 66-67	Will the State define pilot sizes, success criteria, and rollout sequencing for endpoint agent deployments across agencies, or should vendors propose a deployment plan?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
338	RFP Section: Attachment F, Page Number: 45	Are services provided required to be delivered with on-site representation? What services are expected to be provided on-site?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
339	RFP Section: Attachment H & Section 7.2 Page Number: 48 & 19	As a privately held company, Trustwave does not provide financial information. If we are unable to provide the requested financial information, will our response be disqualified? What financial information would suffice for our situation?	Yes. Reference Section 7.2 Financial Statements. Audited financial statements are required. Your CPA must certify that those statements were not prepared for b) to apply.  Attachment H must be submitted.
340	RFP Section, 6.3.3 Page Number 17	The solicitation has not yet been uploaded to the eprocurement portal. When will this be live?	The RFP was electronically posted on July 17, 2025.
341	Attachment D	The state is requesting a time-limited, fixed priced SOW, however the pricing sheet is asking for hourly rates. Can you please confirm how you'd like us to present pricing for this?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
342	Attachment G	Due to the sensitive nature of our customer relationships, we do not disclose private client details, including their technologies, challenges, or solutions, unless an NDA is in place. We can provide additional information upon award. In the meantime, would the state accept case studies in lieu of traditional	No. Reference Section 18 Confidentiality.

		references?	
343	RFP Section: Scope of Work Page Number 07	How you are managing the current Infrastructure. Are you currently using any kind of endpoint management sol. Currently?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
344	RFP Section: Scope of Work Page Number 07	What are your primary goals— compliance, risk reduction, incident response readiness, etc.?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
345	RFP Section: Scope of Work Page Number 07	What is the current network security Architecture/posture for cloud, data centers?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
346	RFP Section: Scope of Work Page Number 07	How frequent you do pen testing and vulnerability assessment?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
347	RFP Section: Scope of Work Page Number 07	Are there any exclusions or restricted areas in the testing scope (e.g., critical infrastructure components)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
348	RFP Section: Scope of Work Page Number 07	Do you prefer black-box, white-box, or grey-box testing?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
349	RFP Section: Scope of Work Page Number 07	Are there mandatory certifications or accreditations required for VAPT providers (e.g., CREST, OSCP, ISO 27001)?	Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services.
350	RFP Section: Scope of Work Page Number 07	Have you deployed any NAC into the infrastructure?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
351	RFP Section: Scope of Work Page Number 07	How are your environments segmented (e.g., DMZ, internal LAN, OT/ICS zones)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
352	RFP Section: Scope of Work Page Number 07	How North-South traffic flows in your Infra?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
353	RFP Section: Scope of Work	Are you using hybrid cloud or on-prem to cloud tunnels (VPN, Direct	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Page Number 07	Connect)?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
354	RFP Section: Scope of Work Page Number 07	Are you using container orchestration platforms (e.g. Kubernetes, OpenShift)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
355	RFP Section: Scope of Work Page Number 07	Are test environments mirrored in the cloud for safe testing?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
356	RFP Section: Scope of Work Page Number 07	Is cloud-native logging and monitoring (e.g., GuardDuty, Azure Sentinel) enabled?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
357	7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY RESERVED.	If the State accepts redlines or proposed revisions to the standard contract terms and/or conditions, would the State have a preferred format (e.g., a template for deviations) for bidders to submit these?	Exceptions taken to the terms and conditions will make a vendor's offer non-responsive.
358	7.3 FINANCIAL RESOURCES	Is the State ok with a non-US based company being one of the contracting	All resources must be based in the United States.

	ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY RESERVED.	parties (e.g., a us-based bidder also invoking non-US based corporate entities to deliver with and therefore would also be one of the contracting parties)?	
359	General	Our organization has a long history of negotiations with the State of North Carolina and does not want to be precluded from the bid process due to our inability to accept the State terms and conditions without any exceptions. To allow for maximum competition and competitive pricing, would the State entertain changing its position in the RFP and allowing bidders to submit limited exceptions within their proposal response for the State's consideration?	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.
360	General	Are offshore resources (staff based outside the US) allowed for services in relation with this RFP?	All resources must be based in the United States.
361	CATEGORY M: IDENTITY AND ACCESS SECURITY SERVICES, Page 64	What identity management systems or solutions are currently in place, and do you expect integration with these systems?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
362	Category D: SECURITY INCIDENT READINESS AND RESPONSE SERVICES, pg. 54	Do you have a centralized IT and cybersecurity? Or, do you have multiple cybersecurity groups?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
363	Category D: SECURITY	Are you open to an IR retainer for digital forensic/incident response	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	INCIDENT READINESS AND RESPONSE SERVICES, pg. 54	(DFIR) services?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
364	Category D, pg. 55	About how many malware samples do you anticipate needing analysis per year?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
365	Category D: SECURITY INCIDENT READINESS AND RESPONSE SERVICES, pg. 55	About how many cyber incidents are you alerted to per year?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
366	Category D: SECURITY INCIDENT READINESS AND RESPONSE SERVICES, pg. 55	What cybersecurity tooling is currently in place to assist with investigations (e.g., EDR/XDR, SIEM/SOAR, ITSM, Firewall, Threat intel, etc.)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
367	Category A: Security Program Assessment and Consulting Services, pg. 51	Are there specific applications or technologies that are of higher priority or that require specialized focus?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
368	Category E: Vulnerability	Can you provide details about the types of assets and environments in	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Management Services, pg. 55	use, such as operating systems, applications, or cloud environments?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
369	CATEGORY G: SECURITY AWARENESS AND TRAINING SERVICES, pg. 58	To what extent are you looking for out-of-the-box, ready-made training content versus customized or bespoke content or live events/activities tailored to your organization?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
370	CATEGORY G: SECURITY AWARENESS AND TRAINING SERVICES, pg. 58	How do you envision working with a training provider to design, implement and/or manage your program? What does an ideal partnership look like?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
371	CATEGORY G: SECURITY AWARENESS AND TRAINING SERVICES, pg. 58	Can you provide a snapshot of the past three years of awareness and training efforts and provide a summary of what you believe is working well and what needs to be improved/addressed further?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
372	CATEGORY G: SECURITY AWARENESS AND TRAINING SERVICES, pg. 58	What does your current security awareness and training team structure look like, and how are responsibilities divided among internal staff, contractors and/or vendors? Do you feel you have the right	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
373	CATEGORY G: SECURITY	Please provide a list of third-party solutions currently being used to	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	AWARENESS AND TRAINING SERVICES, pg. 58	support your awareness and training efforts and how?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
374	Category P: Third-Party Risk Assessment	Is performing the inherent risk evaluation process for new or existing vendors within this scope of work?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
375	Category P: Third-Party Risk Assessment	What assessment methodologies are currently being used (e.g., questionnaire size, assurance reporting review, other evidence required)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
376	Category P: Third-Party Risk Assessment	How many assessments are you anticipating per year according to criticality?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
377	Category P: Third-Party Risk Assessment	Is detection and response against your third parties included in the scope of work?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
378	Category P: Third-Party Risk	Are there continuous monitoring tools / security rating service providers	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Assessment	currently in use?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
379	Category P: Third-Party Risk Assessment	Describe the scope of supply chain security in more detail	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
380	Category E (Vulnerability Management Services)	Do you require remediation treatment as part of the overall scope?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
381	Category F (Network Security Services)	What is the State's definition of "continuous" in "continuous vulnerability assessment and management"? What frequency of scans are they expecting?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
382	Category F (Network Security Services)	What level of patch management support is required (e.g., patch deployment, testing, validation, reporting)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
383	Category F (Network Security Services)	What are the specific models and versions of firewalls currently	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

		deployed across the state's network? How many?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
384	Category J (Governance, Risk, and Compliance Services)	What level of support is needed for email security (e.g., anti-phishing, anti-malware, DLP)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
385	Category J (Governance, Risk, and Compliance Services)	What are the State's requirements for web security services (e.g., web filtering, SSL/TLS inspection, malware protection)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
386	Category J (Governance, Risk, and Compliance Services)	Which regulatory frameworks are the highest priority for the State (e.g., NIST 800-53, NIST CSF, ISO 27001, HIPAA, PCI DSS)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
387	Category J (Governance, Risk, and Compliance Services)	Confirm technology that will be provided or acquired as part of GRC	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
388	Category K (Application Security)	What systems or tools are utilized for tracking and reporting compliance,	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Services)	and how effective are they?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
389	Category K (Application Security Services)	How is data exchanged between systems, and what security measures are currently implemented to protect this data?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
390	Category K (Application Security Services)	What specific application security testing tools and techniques are currently used by the State, and what level of integration is desired?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
391	Category O (Cloud Security Services)	What specific training or guidance is required for developers on secure coding practices?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
392	Category O (Cloud Security Services)	What is the scope of software composition analysis required (e.g., open-source software, third-party libraries)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
393	Category O (Cloud Security Services)	What specific cloud security posture management (CSPM) capabilities are	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

		required (e.g., configuration assessment, compliance monitoring, vulnerability scanning)?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
394	Category O: Cloud Security Services, Pg 66 and 67	What cloud access security broker (CASB) functionality is needed (e.g., visibility into cloud application usage, data security policy enforcement, threat protection)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
395	Category O: Cloud Security Services, Pg 66 and 67	What specific cloud workload protection platforms (CWPP) are currently deployed, and what level of integration is desired?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
396	Category O: Cloud Security Services, Pg 66 and 67	Are there centralized cloud governance or architecture standards that vendors should align with, or will these vary by agency? What is the expected architecture design- Cloud only and or hybrid?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
397	Category O: Cloud Security Services, Pg 66 and 67	What are the tools currently being leveraged for CSMP, Cloud access security, Cloud workload protection, and Cloud security operations?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
398	Category N: Data Security Services	What compliance standards or frameworks do the cloud	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Page 66	environments need to adhere to?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
399	Category N: Data Security Services Page 66	How many SaaS platforms are operating in the environment?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
400	Category N: Data Security Services Page 66	What state standards and regulations for data security apply in North Carolina?	Reference 3.3.9 Enterprise, Services, and Standards.
401	Category N: Data Security Services Page 66	Are there particular compliance requirements or guidelines, such as aligning with federal standards (like NIST or GDPR, if applicable), that should be considered for our operations within North Carolina?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
402	Category N: Data Security Services Page 66	What state-specific laws and regulations govern data privacy in North Carolina?	Reference 3.3.9 Enterprise, Services, and Standards.
403	General	Are there particular privacy standards or frameworks recommended or required for businesses operating in North Carolina?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
404	General	What are the key legal requirements for cross-border data transfer assessments?	All resources must be based in the United States.

405	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section C	Will the State provide test environments or require testing in production?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
406	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section D	What is the expected SLA for incident response times?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
407	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section E	Are there preferred vulnerability scanning platforms already in use?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
408	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section F	Is there a preferred Zero Trust architecture or vendor?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
409	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section J	Are there specific compliance frameworks prioritized (e.g., CJIS, FedRAMP)?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
410	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section O	What cloud platforms are most commonly used across agencies (AWS, Azure, GCP)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

411	General Question, RFP Requirements 3.1	Given the confidential nature of some of the requested responses are you able to sign an NDA?	Reference Section 18 Confidentiality.
412	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Does the State of NC align its OT & Critical Infrastructure to any standard (NERC-CIP, IEC62443, NIST SP800-82, NIST SP 1800-10, or other applicable standard or framework)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
413	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Are there any regulatory requirements for compliance for the Critical Infrastructure environment?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
414	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	How many Critical Infrastructure locations are considered in scope for OT monitoring?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
415	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Is the OT environment centralized to a main SCADA facility, or are there local DCS/SCADA controls for critical infrastructure locations?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
416	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	What services do the critical infrastructure locations provide (gas, water, electricity, wastewater)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
417	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Is there any IACS inventory in use, and is there an estimated asset count?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
418	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Is there a requirement for physical on-site services/assessments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
419	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Are there any specific certifications required by the vendor to perform OT & Critical Infrastructure security services (GIAC GCIP/ GICSP/GRID, IEC62443, or others)	Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services.
420	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Are ICS network segmentation activities in scope, and would the vendor be required to perform or advise?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
421	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Is there a current Incident Response plan and process in place for the industrial environment for OT-specific events?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

422	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	What are considered the biggest concerns or known gaps for cybersecurity within the Critical Infrastructure environment?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
423	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Have there been any risk assessment activities performed on any of the Critical Infrastructure environments that are in scope for the RFP?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
424	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	For an OT monitoring and alerting managed service, is 24 x 7 x 365 required with time zone support?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
425	Category III: CATEGORY SPECIFIC SCOPES OF WORK Section R	Are ICS network segmentation activities in scope, and would the vendor be required to perform or advise?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
426	A, 2d	Are there plans to reassess alignment with NIST SP 800-207 at regular intervals?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

427	A, 2b	What are the primary objectives of the security program and governance assessments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
428	A, 2b	Are there specific compliance requirements or regulations (e.g., NIST, GDPR, HIPAA) driving this assessment in addition to NIST SP 800-207?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
429	A, 2b	What is the expected timeline for completing the security program and governance assessments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
430	A, 2b	What specific deliverables (e.g., reports, presentations, remediation plans) are required, and in what format?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
431	A, 2b	Are there any interim milestones or progress reports expected during the assessment process?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>

432	A, 2b	What level of involvement is expected from the client's internal teams (e.g., IT, security, executive leadership)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
433	A, 2b	Do you expect a gap analysis against NIST SP 800-207 principles or other frameworks (e.g., NIST CSF, ISO 27001)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
434	A, 2b	Should the assessment include a review of security tools, configurations, or operational processes?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
435	A-S, 3b	Our understanding is that this RFP is for services only and specifically excludes products. When referencing, "interoperability, customization, and integration capabilities" does this mean in relation to other services (vendors), in relation to other software/products or to something else entirely (please specify)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
436	C, 2aiii	Please define "intrusion vector".	This is a well-known industry term that should not require definition.
437	C, 3a	Penetration testing can occur both physically and logically, in cloud environments, on-prem, and on workstations. Please clarify this specification, as it is unclear what is	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

		being requested.	Describe your ability to provide the professional services requested in the bid specifications.
438	D, 2aiii	What specific scenarios or frequency of these exercises do you recommend for different types of government entities to ensure comprehensive preparedness?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
439	D, 2av	How should vendors demonstrate that their incident response practices comply with NIST SP 800-61 and ISO/IEC 27035 best practices when working with diverse government entities?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
440	D, 2bv	What level of forensic capability is required from vendors, and are there specific tools or processes that should be included in proposals for government entities?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
441	F	What are the state's key business objectives driving the need for secure network architecture development?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
442	F	What are the key drivers for transitioning to a zero-trust architecture?	The State will not provide this information.
443	G, 2.c	How often should training sessions be conducted to ensure ongoing	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

		engagement and effectiveness, as suggested in subsection 2.c?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
444	General	The solicitation indicates that only fixed fee, fixed duration bids will be accepted for SOWs issued pursuant to this contract, yet Attachment D refers to a Not-To-Exceed hourly rate. Would NCDIT prefer the hourly rate on the category cost form?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
445	General	If a vendor does not support part of the specification in a category, will the vendor be disqualified from the whole category?	No.
446	H	What is the primary goal of this security integration? (e.g., improve data accuracy, automate processes, enhance threat detection, improve compliance)	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
447	L	What factors influence the selection and evaluation of security tools?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
448	O	What are the key priorities for managing cloud security posture across environments?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in

			the bid specifications.
449	O	What are the primary drivers for cloud architecture design (e.g., scalability, security, performance)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
450	S	What are the state's primary security objectives (e.g., prevent ransomware attacks, reduce malware infections, ensure data privacy)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
451	S	What are the primary goals the state hopes to achieve with improved endpoint security (e.g., enhanced threat detection, faster incident response, compliance adherence, improved data protection)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
452	S	What attack scenarios are you most concerned about (e.g., ransomware, phishing, insider threats, data breaches)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
453	R	Are there existing frameworks or standards that vendors must align with (e.g., NERC CIP, IEC 62443, NIST SP800-82, etc.)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p>

			Describe your ability to provide the professional services requested in the bid specifications.
454	R	Are there existing OT security monitoring tools or technologies currently in place?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
455	R	What types of industrial protocols are most commonly used in the State's OT environments?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
456	2.5 CONTRACT TYPE	Will the agencies that use the Cybersecurity Professional Services contract be required to obtain competitive bids from multiple awardees? Or can an agency elect to work exclusively with a single Vendor that is on the contract?	Entities can select to work with an awarded Vendor on this contract.
457	<ul style="list-style-type: none"> <li>· III. CATEGORY SPECIFIC SCOPES OF WORK</li> <li>· CATEGORY I: SECURITY OPERATIONS SERVICES</li> <li>· ATTACHMENT D: CATEGORY COST FORMS</li> </ul>	Regarding Category I: Security Operations Services, the Technical Qualifications imply the bidder should propose a managed service. A managed service typically includes people, processes, and technology/tools. Is this the State's intention? The requested pricing model that limits the bidder to proposing an NTE hourly rate is impractical for a managed service as it only encompasses labor. Is it possible for the State to provide an alternate pricing model that would permit the bidder to include labor,	<p>This RFP is <b>not</b> for SAAS.</p> <p>The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.</p>

		<p>processes, and technology/tools?          Additionally, the number of endpoints is not an effective sizing mechanism for SOC services. Is it possible for the State to provide an alternative sizing mechanism, such as events per second (EPS) or ingestion rate of log source data in GB per day?</p>	
458	<ul style="list-style-type: none"> <li>· III. CATEGORY SPECIFIC SCOPES OF WORK</li> <li>· CATEGORY S: ENDPOINT SECURITY SERVICES</li> <li>· ATTACHMENT D: CATEGORY COST FORMS</li> </ul>	<p>Regarding Category S: Endpoint Security Services, does the State expect a proposal for a managed service using a product, such as CrowdStrike? If yes, the requested pricing model that limits the bidder to proposing an NTE hourly rate is impractical for a managed service as it only encompasses labor. Is it possible for the State to provide an alternate pricing model that would permit the bidder to include labor, processes, and technology/tools? Alternatively, should our response be limited to Professional Services in support of Endpoint Security Architecture and Design, Endpoint Security Assessment, and Endpoint Hardening and Configuration Services? That can be supported with the requested pricing model.</p>	<p>This RFP is <b>not</b> for SAAS.</p> <p>The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.</p>
459	<ul style="list-style-type: none"> <li>· 3.1.5 Enterprise Licensing</li> <li>· Attachment B 1. 43) Clickwrap</li> </ul>	<p>Vendor is a reseller of certain third-party services/deliverables and is contractually required to flow down certain end user license agreement terms to purchasers of these services which may be available via a hyperlink. If such services are part of the overall Vendor solution, can a Vendor include its service attachments in lieu of the State's license agreement with its bid</p>	<p>Exceptions taken to the terms and conditions will make Vendor offers non-responsive.</p>

		response for consideration to be incorporated into a contract with the State?	
460	· Attachment B. Section 1. 4) and 18) b)  · Subcontracting and Confidentiality	Vendor's subcontracts are subject to certain confidentiality agreements, need consent of the subcontractor of its release, and certain information will have to be redacted. Given the language in Section 1. 4) Subcontracting, can the State please confirm when such agreements would need to be released to the State?	The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State agency.
461	· Attachment B. Section 1. 22) c)  · Limitation of Vendor's Liability	Section 1. 22) c) references Service Level Agreement or Deliverables/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, however, Section 2: Terms and Conditions Applicable to IT Goods and Services is reserved. Can the State please clarify this inconsistency?	This RFP is not for SAAS.
462	RFP Section: 3.1.3, 3.15 Page Number: 9	Can vendors optionally include product resell if the products are required for the services? (i.e. penetration tests that require 3-4 tools to conduct the test, that customers often want to buy after the assessment).	No.
463	RFP Section: HISTORICALLY UNDERUTILIZED BUSINESSES Page Number: 42	May responding vendors utilize partnership and/or subcontractor agreements to provide highly qualified offerings across multiple categories, even if the subcontractors are not HUBs?	Partnerships and subcontracts are not restricted to HUBs. Reference Section 4 Subcontracting.
464	RFP Section: 1.0 Page Number: 4	Was the July 31 pre-bid conference recorded? If so, can the recording be shared?	The pre-bid conference was not recorded.
465	RFP Section 7.8 SECURITY AND BACKGROUND	If required, which level would be required for the Background Check?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work

	CHECKS; P. 20 of 73;		(SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
466	Attachment G	Attachment G states: References should be for work within three (3) years from the bid posting date." Will you accept references before 2022?	References must not be earlier than July 16, 2022.
467	Attachment G	Do resumes need to be submitted with our proposal only after an award or engagement has been secured?	The bid requires you to describe the experience, titles etc of your key professional staff expected to perform the services. Resumes of actual individuals will be required at the SOW level.
468	Ariba Sourcing Tool Section 5 - Vendor Response 5.2	This section has a red star next to it and is a required file attachment upload. The title of the Section is "NA". Can you clarify what file needs to be uploaded in this required section?	The Section is Not Applicable as stated. Upload a blank document if the system mandates a document be uploaded.
469	RFP Section: 6.3.3 OFFER SUBMITTAL Page Number: 18	The instructions require vendors to "include all the pages of this solicitation in their response." Does NCDIT intend for vendors to include the 73-page solicitation in our response?	Yes.
470	RFP Section: Attachment J, SECTION 4: Redacted Bid, if applicable. Page Number: 72	The instructions are to include a redacted proposal within the proposal. Will NCDIT permit the submission of the redacted copy as a separate document?	Reference Attachment J. Submittal Checklist.
471	RFP Section: 7.2 Financial Statements Page Number: 19	The instructions states that vendors must return with its offer "A) completed Financial Review Form (Attachment I)..." Please confirm that this should be "Attachment H: Financial Review Form."	Confirmed.
472	RFP Section: 5.2 Evaluation Criteria Page Number: 12	Will NCDIT evaluate proposals at the Category level, or at the subcomponent level?	NCDIT will evaluate all information submitted in response to the bid specifications.

473	RFP Section: Attachment G: References Page Number: 46-47	Please confirm that references for services delivered to international clients are eligible for submission, assuming the work is similar in scope and within the 3-year window, and direct client contact is possible.	Confirmed. Information must be communicated in English.
474	Attachment D: Total Cost of Ownership page 43	Can the State please provide additional details on how the State is calculating and evaluating Total Cost of Ownership (Attachment D)? Is Total Cost of Ownership based on value described in a vendor's response? Or Total Cost of Ownership based on the NTE's (Not to Exceed) provided by competing vendors?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
475	3.2 Security Specifications: Vendor Readiness Assessment Report page 10	If the proposal only covers professional services, is a VRAR necessary?	Vendors shall provide a completed Vendor Readiness Assessment Report State Hosted Solutions ("VRAR") at offer submission.
476	Attachment I: All Categories Requirement 3D page 50	Given that the services under each category and that the entity sizes vary in complexity, and there are undefined variables impacting timelines, how does the state expect vendors to provide a solution roadmap, high-level timeline, and description of enhancements for each category?	Describe your ability to provide the professional services requested in the bid specifications.
477	Attachment F: Offshore Clarification page 45	Understanding Attachment F: LOCATION OF WORKERS UTILIZED BY VENDOR allows for the use of offshore resources and the cost of offshore vs. onshore resources can vary– is the state open to an offshore NTE, an onshore NTE, and a hybrid NTE for each category? In addition are there any categories or any entity types (small, medium, large, x-large) that will not allow for offshore	No. All resources must be based in the United States.

		resources?	
478	Attachment D: Total Cost of Ownership page 43	Understanding there are multiple services under a single category, is the state open to multiple NTE's under a Category and Entity size? In addition, understanding the period of performance is 5 years – is the state willing to allow for a NTE rate escalation?	Yes. The State requires not to exceed pricing per service and per entity size under each category.  The State will not permit price escalation during the initial five year term of the contract.
479	ATTACHMENT G: REFERENCES Page: 46	Can you please define the term “subcategory” within ATTACHMENT G: REFERENCES? Can you please clarify if the State wants vendors to provide client references using “categories” or “subcategories”? If references are to be provided at the category level – given the wide range of services under each Category, is it necessary for all services within the Category to be delivered at a single client reference?	Ignore the term subcategory.
480	Section 2.1, Page 4	Can the State clarify whether the forthcoming solicitation for cybersecurity products will overlap in scope with any implementation services requested under this RFP?	This RFP is for professional services. The forthcoming solicitation is for SAAS and other products.
481	Section 3.2, Page 10	For the required Vendor Readiness Assessment Report (VRAR), can the State confirm if a separate VRAR is required for each category proposed or if one consolidated VRAR is acceptable if the content overlaps?	Reference 3.2.1 Solutions Hosted on State Infrastructure.
482	Attachment I, Page 50	Will sample Statements of Work (SOWs) be shared for any of the categories to illustrate expected scope, deliverables, and timelines?	No. This information is not available.
483	Section 2.5, Page 8	Can the State provide more detail on how awardees under this RFP will be engaged post-award (e.g., centralized	Entities can select to work with an awarded Vendor on this contract.

		task orders, agency-specific SOWs, direct assignments)?	
484	Section 5.2, Page 12	Can the State elaborate on how "Total Cost of Ownership" will be evaluated, particularly given the wide scope of hourly rates across entity sizes?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
485	Section 2.2, Page 7	Will the State allow vendors to propose jointly (e.g., through partnerships or subcontractors) to cover multiple categories comprehensively?	Vendors proposing jointly will each be individually evaluated on all RFP evaluation criteria before award. Reference Section 4 Subcontracting.
486	Attachment D, Page 43	Can the State confirm that the NTE hourly rates should be inclusive of all costs, including travel, and that no reimbursable expenses will be allowed under resulting contracts?	Travel must be included in your proposed cost.
487	Attachment I, All Categories	Is the State looking for past performance and examples for every individual category being proposed, or will general cybersecurity experience suffice across similar service areas?	Yes. References must be relevant to the service category. Reference Attachment G References.
488	Section 6.3.3, Page 17	If a vendor experiences technical difficulties uploading the proposal via the Ariba Sourcing Module, will late submissions be accepted under any circumstances?	Reference 6.3.3 Offer Submittal. It is the Vendor's sole responsibility to upload their offer to the Ariba Sourcing Module by the specified time and date of opening. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues.
489	Section 7.6, Page 19	Can the State provide a materiality threshold for what constitutes reportable litigation, especially for large vendors with extensive contracting history?	Reference Section 7.6 Disclosure of Litigation.
490	Attachment B, Page 24-40	Are there any exceptions that the State will consider to the standard Terms and Conditions, or will all exceptions automatically result in a non-responsive bid?	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.
491	Section 6.3.1, Page 17; Attachment J, Page 72	Can the State confirm whether each category response must be submitted as a separate document or as part of	Reference Attachment J: Submittal Checklist.

		one consolidated proposal with clearly labeled sections?	
492	Section 6.3.3, Page 18	Is there a preferred naming convention for file uploads beyond the vendor name prefix?	No.
493	Section 6.3.1(g), Page 17	Will the State accept hyperlinks to external documentation (e.g., product specs, certifications), or must all content be embedded in the proposal?	No. Reference 6.3.1 General Instructions for Offer.
494	Attachment G, Page 46	Can the same reference be used across multiple categories if relevant, or must each category have unique references?	Yes. Reference 6.3.1 General Instructions for Offer.
495	Attachment G, Page 46	Will the State accept references from subcontracted engagements or only direct prime contracts?	Only direct prime contracts references will be accepted.
496	Attachment D, Page 43	Does the state expect incremental pricing for fixed price solutions?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
497	RFP Section: 2.1 Introduction, Page Number: 4	In Section 2.1, "Introduction" of the RFP, it is mentioned that <i>"The State will issue a solicitation for cybersecurity products after the cybersecurity professional services contract is awarded."</i>  Could you please clarify whether it will be mandatory for awarded vendors to respond to the upcoming cybersecurity products solicitation as well?	Vendors are not required to participate in any bid.
498	RFP Section: 3.2 Security Specifications, Page Number: 10	Could you please confirm whether vendors are required to submit separate Vendor Readiness Assessment Reports (VRARs) for each category they are bidding on as part of the initial bid?	Reference 3.2.1 Solutions Hosted on State Infrastructure.
499	RFP Section: 3.2 Security	In the event that only the subcontractor holds the necessary	No. Reference Section 4 Subcontracting.

	Specifications, Page Number: 10	independent third-party assessment reports, and not the prime vendor, would this be considered sufficient to meet the security requirements outlined in Section 3.2?	
500	RFP Section: 3.2 Security Specifications, Page Number: 10	Regarding the independent third-party assessment reports outlined in Section 3.2 – <i>Security Specifications</i> ,  If a vendor engages a subcontractor, is the subcontractor also required to maintain these assessment reports to remain compliant with the RFP requirements?	Subcontractors shall adhere to the same standards required of the selected Vendor in the Agreement.
501	RFP Section: 3.2 Security Specifications, Page Number: 10	Is submission of third-party security certifications (SOC 2 Type II, ISO 27001, etc.) required at the time of proposal, or only upon request?	Reference 3.2.1 Solutions Hosted on State Infrastructure. Vendors are encouraged to provide a current independent 3rd party assessment report in accordance with subparagraphs (i)-(ii) at the time of offer submission.
502	RFP Section: 3.2 Security Specifications, Page Number: 10	If submitting a substitute security assessment (e.g., SOC 2 Type I), can vendors include plans or commitments to achieve preferred certifications post-award?	The Vendor shall provide an explanation for submitting the alternative assessment report. If awarded this contract, a Vendor who submits an alternative assessment report shall submit one of the preferred assessment reports no later than 365 days of the Effective Date of the contract.
503	RFP Section: 5.0 Evaluation, Page Number: 12	Will vendors receive feedback if their proposals are found non-responsive or are not selected in the initial award phase?	The State will not provide this information.
504	RFP Section: Historically Underutilized Businesses, Page Number: 42	Is there a specific subcontracting goal for Historically Underutilized Businesses (HUBs) associated with this opportunity?	No.
505	RFP Section: Attachment F: Location of Workers Utilized by Vendors, Page Number: 45	Could you please confirm whether the use of offshore resources is permitted for this engagement, provided that the appropriate supporting documentation is	All resources must be based in the United States.

		submitted and prior approval is obtained from the agency?	
506	RFP Section: Attachment G: References, Page Number: 46	In Attachment G: References, it is stated that <i>“Vendor shall submit two (2) different customer references (per subcategory) using this form.”</i>  If the vendor is proposing to use subcontractors, may the subcontractor’s customer references be submitted to fulfill this requirement?	Reference Section 4 Subcontracting.
507	RFP Section: Attachment G: References, Page Number: 46	In Attachment G: References, it is stated that <i>“Vendor shall submit two (2) different customer references (per subcategory) using this form.”</i>  The RFP outlines approximately 19 categories (Category A through Category S). Could you please confirm whether vendors are required to submit two references for each individual category they are proposing to bid on?	Correct.
508	RFP Section: III. Category Specific Scopes of Work, Page Number: 52	In Section III: Category Specific Scopes of Work, under Experience and Key Personnel, it states: <i>“Resumes clearly demonstrating staff qualifications to perform the services specified in the category will be required with each Statement of Work (SOW).”</i>  Could you please clarify whether any resumes— sample or otherwise—are required to be included as part of the initial bid submission for the categories the vendor is proposing?	The bid requires you to describe the experience, titles etc of your key professional staff expected to perform the services. Resumes of actual individuals will be required at the SOW level.
509	RFP Section: Attachment J: Submittal Checklist,	In Attachment J: Submittal Checklist, <b>under</b> Section 1: General Response, it states: <i>“Attachment E: Vendor</i>	Reference Section 6.2.10 Vendor Registration with the Secretary of State.

	Page Number: 72	<p><i>Certification Form (Include Proof of NC Secretary of State License to do Business in North Carolina)."</i></p> <p>Could you please clarify whether vendors are required to possess a North Carolina Secretary of State License at the time of bid submission, or if obtaining the license would only be necessary upon award?</p>	
510	General	Could you please confirm how many vendors are expected to be awarded under this solicitation?	The Agreement shall be and operate as a multiple Vendor contract.
511	General	Should pricing include optional or value-added services not explicitly listed in the RFP?	No.
512	General	Could you please confirm whether vendors will have the opportunity to update or expand their service offerings during the five-year base term of the contract?	NCDIT reserves the right to issue an amendment to awarded contractors to include new service offerings at NCDIT's sole discretion.
513	RFP Section Attachment I: Section 7.2, Page 19	In the introduction to Section 7.2, the RFP references Attachment I. Shouldn't this be Attachment H instead?	Correct.
514	RFP Section Attachment I: Section 2.1, Page Number 5	Please provide more details on small, medium, large and extra-large/ enterprise governmental entities in terms of size and scope in terms of budget, population served, geographic area covered, and organizational complexity.	Reference Attachment A: Definitions.
515	RFP Section Attachment I: Scope Of Work And Specifications Page 61	In addition to remediation recommendations, are you seeking remediation support?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
516	RFP Section Attachment I: Category J: Governance, Risk, And Compliance Services; Page 61	Does the State have prescribed compliance and regulatory requirements for performing the assessment, in addition to the assessment against Best Practices?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
517	RFP Section Attachment I: Identity and Access Security Page 64	Which identity and access management (IAM) tools or platforms are currently in use (e.g., Azure AD, Okta, SailPoint)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
518	RFP Section Attachment I: Identity and Access Security Page 64	Are you currently using any Zero Trust frameworks or continuous authentication models today?	The State has adopted Zero Trust Architecture based on NIST SP 800-207 principles. Reference Section II of Attachment I, Infrastructure Overview.
519	RFP Section Attachment I: Identity and Access Security Page 64	How do you currently manage identity lifecycle events (onboarding, offboarding, role changes)?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
520	RFP Section Attachment I: Identity and Access Security Page 64	Does the government have role-based or attribute-based access controls implemented? If so, how are they governed?	<p>This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.</p> <p>Describe your ability to provide the professional services requested in the bid specifications.</p>
521	RFP Section Attachment I:	Which endpoint protection platforms (EPP/EDR) are currently deployed	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Category I: Security Operations Services Page 60	across your environment?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
522	RFP Section Attachment I: Category I: Security Operations Services Page 60	Do you have standardized hardening baselines for different OS types (Windows, macOS, Linux)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
523	RFP Section Attachment I: Category I: Security Operations Services Page 60	Which tools/technologies do you currently use for SIEM, SOAR, Threat Hunting etc.?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
524	RFP Section Attachment I: Category P: Third-Party Risk Management Services Page 67	Do you have a formal third-party risk assessment process in place? If so, which tools or frameworks are used?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
525	RFP Section Attachment I: Category P: Third-Party Risk Management Services Page 67	How do you currently monitor third-party risks, detect changes in posture, and manage security incidents involving third parties continuously?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
526	RFP Section Attachment I:	What is your process for responding to third-party security incidents and	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Category P: Third-Party Risk Management Services Page 67	coordinating remediation?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
527	RFP Section Attachment I: Category P: Third-Party Risk Management Services Page 67	Are you currently managing software supply chain risks, including Software Bill of Materials?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
528	1.0 Procurement Schedule, page 4	Can a recording of the Pre-Bid presentation or a copy of the presentation document be made available on the Electronic Vendor Portal (eVP)?	The pre-bid conference was not recorded.
529	2.0 Purpose of RFP, page 5	The RFP states: "This contract shall not be used for any kind of staff augmentation." Can you please expand on this by defining or providing examples of what type of cybersecurity-related services would be considered staff augmentation?	Reference the IT Staffing State Term Contract.
530	2.0 Purpose of RFP, page 8	For non-state agencies using this as a "convenience contract", what are the benefits to those agencies of using this mechanism compared to a stand-alone procurement? (i.e. will it save them time in the procurement process, etc.?)	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
531	6.0 Vendor Information and Instructions, page 15	Can you share the overall process for awarding task orders/awards under this indefinite quantity contract?	This RFP is for SOW based cybersecurity professional services.
532	6.0 Vendor Information and Instructions, page 15	Is there an existing pipeline of task orders/scopes of work for this contract?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work

			(SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
533	6.0 Vendor Information and Instructions, page 17	Is there a page limit to the overall proposal and/or for each Category Specific Scope of Work (e.g. Application Risk Assessment and Consulting Services Specifications)?	Yes. The maximum file size for electronic submittal is 100 MB.
534	6.0 Vendor Information and Instructions, page 17	Will you be using any AI tools to review Offers? If so, can you share the specific tools that will be used?	No.
535	Attachment I: Scope of Work and Specifications	Are there specific DIT key performance indicators (KPIs) that vendors will be required to report on and/or be evaluated against?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
536	Section 4, Page 39	“Vendor’s AI has a data cutoff date of _____” What does the state anticipate answers to be for this?	Insert your AI cutoff date.
537	Attachment I, Category K, Sub Section D, Page 63	“Describe how you maintain software bills of materials (SBOMs)” Can the state describe what a SBOM typically contains?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
538	Attachment I, Section II, Page 50	Would the state be willing to switch from VMware to something better and cheaper?	The State will not answer this question.
539	Attachment G, Page 46	If we would like to reference DoD contracts, we are able to provide names. However, the contact information is often considered	Reference Section 18 Confidentiality.

		confidential. We would be able to provide it privately if requested. Would this be acceptable?	
540	1.0 PROCUREMENT SCHEDULE Overview of Services and Contract Purpose	Could you please clarify whether the primary focus of this contract will be on the provision of professional cybersecurity services exclusively, or if vendors are also expected to provide products or technology solutions as part of their offerings?	This is an RFP for SOW based Cybersecurity Professional Services.
541	Category Specific Scopes of Work	Could you please clarify whether the primary focus of this contract will be on the provision of professional cybersecurity services exclusively, or if vendors are also expected to provide products or technology solutions as part of their offerings?	This is an RFP for SOW based Cybersecurity Professional Services.
542	Proposal Submission Instructions	How standardized are the Scopes of Work (SOWs) that will be issued under this contract? Should vendors expect highly customized SOWs per agency, or will there be common templates and consistent requirements across agencies?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract.
543	5.0 EVALUATION Evaluation Criteria	Regarding the utilization of workers located outside the United States, are there any specific restrictions, limitations, or preferences that the State has established beyond what is outlined in Attachment F?	All resources must be based in the United States.
544	6.0 VENDOR INFORMATION AND INSTRUCTIONS Vendor Information Requirements	Given the supplemental terms related to Artificial Intelligence (AI), can you provide guidance on the State's current stance or expectations about the use of AI or GenAI technologies within the services provided under this contract?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract. Describe your ability to provide the professional services requested in the bid specifications.
545	ATTACHMENT D: CATEGORY COST FORMS Cost	In the evaluation process, could you elaborate on how heavily the State will weigh cost factors relative to	No.

	Proposal Forms	technical qualifications, security compliance, and past performance when determining awardees?	
546	ATTACHMENT G: REFERENCES	In the evaluation process, could you elaborate on how heavily the State will weigh cost factors relative to technical qualifications, security compliance, and past performance when determining awardees?	No.
547	Attachment G	Can subcontractor experience and references be used to satisfy Attachment G requirements?	No.
548	Attachment I	Are there any categories/scopes of work that must be performed by on-site resources, and if so, can you please specify which ones?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
549	Attachment I	Are there any categories/scopes of work that must be performed by onshore resources, and if so, can you please specify which ones?	All resources must be based in the United States.
550	Attachment D	Is there a limit to how many vendors will be selected in each category and entity size, and if so, can you please specify what that limit is?	No.
551	Section 2.1, Page 5	Can the State provide examples of typical Scope of Work (SOW) requests expected under this contract?	This information is not available.
552	N/A	What volume of requests (SOWs) per year does the State anticipate across each service category?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.

553	Section 2.1, Page 5; Attachment I, Pages 50–71	Will vendors be pre-qualified by category only, or also by sub-capabilities (e.g., penetration testing vs. red teaming)?	Vendors will be prequalified by category services.
554	Section 2.1, Page 5	Will individual agencies define their own requirements and project success criteria, or will NCDIT coordinate SOW development?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
555	Section 2.1, Page 5	Will SOWs typically involve single agencies or cross-agency collaboration (e.g., joint risk assessments)?	Each governmental entity will individually issue their SOW.
556	Attachment I, Page 50–51	Can the State provide an estimated range of assets (e.g., applications, endpoints, networks) typically in scope for a security assessment or penetration test?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
557	Attachment I, Page 50–51	Are there preferred security tools or platforms (e.g., for SIEM, IAM, ticketing) that vendors should integrate with or support?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
558	N/A	Will vendors be notified when SOWs are released, or is a separate competition held among pre-qualified vendors?	Agencies will contact the Vendors that they choose to contract with.
559	N/A	Are any specific certifications required or preferred for key personnel?	Describe the position titles and associated, experience, qualifications, certifications, and educational background required by Vendor for Vendor's technical/professional staff expected to perform the services.

560	N/A	Will rates submitted on the Category Cost Forms be binding or ceiling rates?	The State requires a not to exceed hourly rate for each category for Small, Medium, Large, and X-large enterprises.
561	Section 3.2.1, Page 10	We are certified as a C3PAO by the CMMC Accreditation Body. Will the CMMC AB assessment report be an adequate substitution for the SOC 2 Type 2 evaluation?	Reference Section 3.2 Security Specifications for acceptable alternate assessments and the timeframe for providing the preferred assessments.
562	RFP Document Section 2.1 Introduction Page 5	Section 2.1 (page 5) of the RFP specifies that offers should not include cybersecurity services that are inherently bundled with IT infrastructure products (e.g., items on the 204X contract). However, many of the services outlined in this RFP-such as endpoint security, DAST/SAST testing, and threat simulations-are typically delivered through integrated security tools or platforms rather than by hourly rates. Can the State clarify how vendors should propose these services when delivery is dependent on products rather than hourly labor?	This RFP is for professional services. There is a forthcoming solicitation is for SAAS and other products.
563	Attachment I Section III Category Specific Scopes of Work Categories A through S Subsection 3 Capability Pages 51-71	In Attachment I, Section III (All Categories), each category includes a question under subsection 3) a) asking vendors to describe the location of service implementation (e.g., endpoint, network, or cloud). Since this RFP is limited to professional services and excludes bundled product offerings, can the State clarify how a vendor should respond, particularly when some services are performed by products rather than direct labor?	Describe your ability to provide the professional services requested in the bid specifications.
564	Attachment I Section III Category Specific Scopes of Work	In Attachment I, Category G, Section 2) b) iv), vendors are asked to describe their simulation capabilities such as phishing or attack	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional

	Category G Subsection 2 Page 58	simulations. These types of services are typically product-driven rather than labor-based. Could the State clarify how it defines these simulations as a “professional service” under this RFP?	services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
565	Attachment I Section III Category Specific Scopes of Work Category H Subsection 2 Page 59	Attachment I, Category H (Security Implementation and Integration), subsection 2) c) iii) asks vendors to describe how they conduct proof of concept (PoC) testing for security technologies. As PoCs are typically conducted by value-added resellers (VARs) or manufacturer products rather than professional services personnel, how should manufacturers respond if their standard delivery model for PoCs is not considered a professional service?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
566	Attachment I Section III Category Specific Scopes of Work Category K Subsection 2 Page 62	In Attachment I, Category K (Application Security), subsection 2) b) asks vendors to describe their capabilities for SAST, DAST, IAST, and API security testing. These are commonly delivered via automated product tools. Given the RFP’s focus on professional services only, how should vendors respond to this section when these capabilities are not labor-based but are product-driven?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
567	Attachment D, Page 43	Since this is a 5-year contract, are the prices provided by vendors valid for all 5 years? Or is there an ability to update pricing periodically? If so, how frequently?	Pricing is for the five (5) year initial contract term.
568	Attachment D, Page 43	After the initial 5-year term, if the State chooses to extend the contract, will pricing be able to be updated at that time?	The State will negotiate pricing with the Vendor at that time.



	Information Technology Terms and Conditions, Pages 24-40	with terms and conditions of Attachment B?	
572	3.2.1; PG 10	This section states a VRAR should be submitted for each category. Would a VRAR be necessary or would an alternative-approved assessment suffice? Can we acknowledge one assessment encompasses all relevant sections?	VRARs are required where requested.
573	22;c; PG 30	There are exclusions in the limitation of liability cap. Is NC DIT open to including and/or negotiating a supercap on the exclusions that would be higher than the 2x cap on all other damages?	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.
574	43; PG 35	If third party software is required for the services being performed under an SOW, and the software publisher utilizes a clickwrap method to license their product, we cannot void or negate that clickwrap. While we can work with the applicable Agency to understand if there is already a license agreement in place between the software publisher and the Agency, that license agreement would be the appropriate mechanism for the publisher to confirm the clickwrap is null and void. Will NC DIT modify this clause to specify that it only applies in the event the clickwrap is for software published/licensed by the Vendor, and not a third party?	This RFP is <b>not</b> for SAAS.
575	Attachment B; PG 24	As SOWs are executed with various Agencies, terms and conditions may be further negotiated as a part of the SOW. There is no current order of precedence in the terms and	Exceptions taken to the terms and conditions will make a Vendor's offer non-responsive.

		conditions clarifying what document would rule in a conflict. Will NC DIT include in Attachment B that terms and conditions negotiated in an SOW take precedence over the master agreement?	
576	Attachment 1; Category H; PG 59	For Category H, would NC DIT like to have examples of Implementation Security Services offered by the responding vendor?	The State only requires the information requested.
577	Attachment 1; PG 50	Is Artificial Intelligence (AI) in scope for the services of this contract? If so, which category would be preferred to reference AI?	This RFP is for cybersecurity professional services. There is a forthcoming solicitation is for SAAS and other products.
578	Attachment I: Scope of Work and Specifications; Category J: Governance, Risk and Compliance Services; Section 1) a. Overview; Page 61	What GRC tool is used within NC DIT to manage GRC requirements? Is it a centralized tool or do the various agencies have their own GRC tools?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
579	Attachment I: Scope of Work and Specifications; Category J: Governance, Risk and Compliance Services; Section 1) a. Overview; Page 61	Will the NC DIT manage the GRC tool(s) or is the expectation of this request to include management of the GRC tool(s)?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
580	Attachment I: Scope of Work and Specifications; Category P: Third-Party Risk Management Services; Section 1) a. Overview; Page 67	What TPRM assessment tool(s) are employed within the NC DIT? Is the tool centralized or do each agency within the state employ a different tool and if so how are the tool(s) deployed (on-prem/off-prem/hybrid/cloud, etc.?)	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
581	Attachment I: Scope of Work and	Can you provide a rough order of magnitude (ROM) of the number of	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term

	Specifications; Category P: Third-Party Risk Management Services; Section 2) a. Technical Qualifications, Third Party Risk Assessment; Page 67 and 68.	third parties assessed on a Monthly, Quarterly and Annual period of time?	Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
582	Attachment I; Categories A,G,H,J,M	How, if any, do you currently leverage organizational change management initiatives/projects in projects/initiatives that impact people and process?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
583	Attachment I; Categories A,G,H,J,M	Do you have an internal organizational change management team in your PMO, outsource change management expertise or a combination of both?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
584	Attachment I; Categories A,G,H,J,M	How much of your budget is typically allocated specifically towards organizational change management activities to mitigate potential disruption, accelerate adoption and help achieve a smooth implementation? If none, why?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
585	Attachment I	If we offer a managed service for specific OEMs, would that fall under Category H, or would DIT consider those under a different Category? (We understand that staff augmentation services are not in	Describe your ability to provide the professional services requested in the bid specifications.

		scope with this RFP).	
586	Attachment I	There are a series of question that start with "Describe the location of..." i.e. "Describe the location of your service implementation e.g. at the endpoint, network based, and/or cloud based." Can we get a better description of what NC DIT is trying to ascertain with this question?	No.
587	RFP Section: 2.1 Page Number: 5	For the state agency sizing that is listed as small, medium, large, extra large, is the expectation that there will be at least one state-employee IT resource per agency who would be available to serve as a main point of contact for the service providers to each agency?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
588	RFP Section: 3.1.5 Page Number: 9	What Security Information and Event Management (SIEM) platforms is the state licensed for?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
589	RFP Section: III. CATEGORY SPECIFIC SCOPES OF WORK • Category B • D) • I) Page Number: 52	Would the state anticipate PCI, HIPAA and similar areas of compliance to be specifically within the scope of services to be provided – e.g., would they need a ROC issued for PCI, would HITRUST be on their radar for HIPAA?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.  Describe your ability to provide the professional services requested in the bid specifications.
590	CATEGORY SPECIFIC SCOPES OF WORK Page 7 of 73	Which locations will the work be completed for Category A through S?	This information is not available across all governmental entities that will be eligible to use the Cybersecurity Professional Services State Term Contract. This information will be collected during the Statement of Work (SOW) process from each entity seeking SOW-based professional services under this contract.

			Describe your ability to provide the professional services requested in the bid specifications.
--	--	--	---

---

**Failure to acknowledge receipt of this Addendum may result in rejection of the response.**

Check ONE of the following options:

- This addendum is being submitted with our Bid. Changes resulting from this addendum are included in our bid response.
- Bid has not been submitted. Any changes resulting from this addendum are included in our bid response.
- Bid has been submitted. No changes resulted from this addendum.
- Bid has been submitted. Changes resulting from this addendum are listed above.

**Addendum Execution:**

**Offeror:** \_\_\_\_\_

**Authorized Signature:** \_\_\_\_\_

**Name and Titled (Typed):** \_\_\_\_\_

**Date:** \_\_\_\_\_