|  |  |
| --- | --- |
| seal-jpg | **STATE OF TENNESSEE DEPARTMENT OF FINANCE & ADMINISTRATION**  **REQUEST FOR PROPOSALS #31701-03385**  **AMENDMENT #TWO**  **FOR NATIONWIDE CYBERSECURITY REVIEW** |

**DATE: November 2, 2022**

**RFP #31701-03385 IS AMENDED AS FOLLOWS:**

1. **This RFP Schedule of Events updates and confirms scheduled RFP dates.** Any event, time, or date containing revised or new text is highlighted.

|  |  |  |
| --- | --- | --- |
| **EVENT** | **TIME  (central time zone)** | **DATE** |
| 1. RFP Issued |  | 9/26/2022 |
| 1. Disability Accommodation Request Deadline | 2:00 p.m. | 9/29/2022 |
| 1. Pre-response Conference | 1:00 p.m. | 9/30/2022 |
| 1. Notice of Intent to Respond Deadline | 2:00 p.m. | 10/3/2022 |
| 1. Written “Questions & Comments” Deadline | 2:00 p.m. | 10/10/2022 |
| 1. State Response to Written “Questions & Comments” |  | 11/2/2022 |
| 1. Response Deadline | 2:00 p.m. | 11/17/2022 |
| 1. State Completion of Technical Response Evaluations |  | 12/12/2022 |
| 1. State Opening & Scoring of Cost Proposals | 2:00 p.m. | 12/13/2022 |
| 1. Negotiations (Optional) |  | 12/14/2022-12/20/2022 |
| 1. State Notice of Intent to Award Released and RFP Files Opened for Public Inspection | 2:00 p.m. | 12/27/2022 |
| 1. End of Open File Period |  | 1/4/2023 |
| 1. State sends contract to Contractor for signature |  | 1/11/2023 |
| 1. Contractor Signature Deadline | 2:00 p.m. | 1/18/2023 |

1. **State responses to questions and comments in the table below amend and clarify this RFP.**

Any restatement of RFP text in the Question/Comment column shall NOT be construed as a change in the actual wording of the RFP document.

| **RFP SECTION** |  | **QUESTION / COMMENT** | **STATE RESPONSE** |
| --- | --- | --- | --- |
|  |  | Looks like there is a contractor (redacted) who is providing similar scope of services to the DGS-STS currently, are they excluded from bidding on this RFP?  If not, is that State satisfied with their performance on the current contract? | No, they are not excluded from providing a response to this RFP.  Contractor performance on a separate contract does not pertain to this RFP and therefore the State will not answer that question here. |
|  |  | Is this a new RFP, or an extension/addition to the current contract # 0000000000000000000073180 | This is a new RFP, no connection to the referenced contract. |
|  |  | Are you planning to award this to multiple vendors? | The State will award to only one Contractor. |
| Section 1.1 |  | Please confirm that STS will engage only a single vendor to provide the services. | See State’s response to question #3. |
| Section 1.1 | 5. | After the NCSR assessments, can we develop POAMs against the NIST CSF, since it is the basis for NCSR? | Yes |
| Section 1.1 | 6. | Is it STS’s expectation that the selected vendor can assemble sufficient subcontractors to process up the 1,332 Tennessee entities between contract date and February 28, 2023, which – accounting for holidays – may be only 2.5 months? | The State will not have time to complete all 1,332 assessments before 2/28/2023.  The new expectation will be for the selected Contractor to begin the planning, scheduling, and pilot (A.8 – A.10) upon contract award and begin the 1,332 assessments and POAMS during the October 2023 – February 2024 submission window.  Please see RFP Release 2 for a revised RFP Attachment 6..6. Pro Forma Contract section A.3 which has been revised to adjust Phase 1 beyond “year 1”. |
| Section 1.1 | 7. | Since in the pre-bid meeting you indicated that STS is to be the “pilot” assessment, this may take the first week of December, further narrowing the assessment window, how many entities are expected to be realistically completed by February 28, 2023? | See State’s response to question #6. |
| Section 1.1 | 8. | Do resulting POAMS also have to be completed by February 28, 2023? | See State’s response to question #6.  In addition, POAMs are to be completed withing 10 business days following the completion of each NCSR assessment per pro forma section A.8. |
| Section 1.1 | 9. | For those Tennessee entities that do not complete their NCSRs by February 28, 2023, what work for them can the vendor be expected to perform from March 1, 2023 until the next NCRS period starting October 1, 2023, if any? | See State’s response to question #6. |
| Section 1.1 | 10. | What process should vendors assume will take place to “recruit” the 1,332 state entities to participate in the assessments? | The State is hiring two FTE to help manage the NCSR. Part of their jobs will be discovery of and communication with the entities. Then contact information will be shared with the vendor. |
| Section 1.1 | 11. | What percentage of the 1,332 entities does STS expect to affirm participation? | The State does not know. It will be determined during phase 1 of the contract as noted in Pro Forma section A.10. |
| Section 1.1 | 12. | What role will the selected vendor play in that “marketing” or “recruitment process”? | See State’s response to question #10 |
| Section 1.1 | 13. | Are our costs for that recruitment work to be assumed in our hourly fee? | Yes, there is not a separate line for recruitment pricing. |
| Section 1.1 | 14. | What is STS’ GRC tool, since our POAMs must be compatible with that platform or tool? | The State’s GRC tool is Archer. Archer supports CSV imports only. |
| Section 1.1 | 15. | Is the STS GRC tool the same as the NCSR portal? If they are not the same tool, who is responsible for entering data into the NCSR portal? | The GRC tool and NCSR portal are separate.  The contractor will be responsible for importing the data into both.  The contractor will enter the responses into the NCSR with the entity's live participation. The exception would be if the NCSR is not available. In that case a substitute system, probably Excel would be used to complete the survey offline. This would be the vendor filling out the Excel workbook with the entity again participating as it is completed. |
| Section 1.1 | 16. | Does the STS GRC tool allow for data import? We might complete the NCSR in our tool and import the data to the STS tool. | See State’s response to question #14 |
| Section 1.1.2 | 17. | Is it assumed that the $15 million funding will cover 1,332 assessments/POAMS and that Year 2-5 remediation work (or “enhanced recommendations”) would be the financial responsibility of each Tennessee entity? | $15 million is the total budget for Phase 1 and Phase 2. We don’t expect Phase 1 to consume the entire $15 million but we also don’t know how far it will go. Any remaining funds following Phase 1 will be put towards Phase 2 work. Tennessee Entities will not be responsible for any of the cost.  Also, remediation is not part of the scope of work. Enhanced Recommendations are defined in pro forma section A.12. |
| Section 1.1.2 | 18. | If less funding is consumed by assessments (perhaps if many of the 1,332 entities decline participation), how is the remaining funding to be allocated to remediation work and “enhanced recommendations”? Must that work be approved by STS? Does the vendor invoice each entity for that work at our hourly rate or invoice STS for that work? | Remediation is not part of the scope of work. Enhanced Recommendations are defined in pro forma section A.12.  The State shall initiate/approve the contractor to begin and provide Enhanced Recommendations per Pro Forma section A.3.i.  The state is not obligated nor guarantee that all $15m will be spent during the contract term. |
| Section 1.1.2 | 19. | Does Tennessee STS expect for Year 2-5 DHS grants to continue funding Year 1 remediation work and enhanced recommendation work as the source of revenue from which to pay the vendor? | The entire contract is to be federally funded via ARPA (The American Rescue Plan Act of 2021) funds. |
| Section 1.4.2.2. and RFP attachment 6.2 – Section B.15(d) [and Note] | 20. | Is there a target or required level of diversified business enterprise participation to be awarded this contract, or is it a best-effort approach to identifying and selecting DBE’s to meet that objective? | The diversity goal is a best effort approach to assist the overall diversity goal of the department of Finance and Administration. |
| Section 1.4.2.2. and RFP attachment 6.2 – Section B.15(d) [and Note] | 21. | What is that target or required percentage of DBE involvement? | The overall diversity goal of the department of Finance & Administration is 4%. |
| Section 1.4.2.2. and RFP attachment 6.2 – Section B.15(d) [and Note] | 22. | If strong DBE contractors have highly competent off-shore assessors, can they be utilized, or is there a U.S. domicile-only requirement? | DBE contractors must be U.S. domicile. |
| Section 4.7.3 | 23. | Since contracting with at least two subcontractors is required, can the prime contractor (respondent) meet the Tennessee registration requirement with the Dept. of Revenue through one or more subcontractors that are registered with the Dept.? | No. The (prime) Contractor must meet the Department of. of Revenue registration requirement or provide proof of exemption. |
| RFP Attachment 6.1, page 18 | 24. | If the respondent is a large, diversified consulting firm, can the Cybersecurity Practice Leader sign the proposal, rather than the overall company CEO or President? | Not unless evidence is provided that person has the authority that can legally bind the company to the RFP requirements. |
| RFP Attachment 6.1, page 18 | 25. | What evidence of “authority to bind” is acceptable to STS? | A letter on company letterhead from the President or Chief Executive Officer that the person signing has the authority to legally bind the company. |
| RFP Attachment 6.2 Section A.5. | 26. | Can respondents employ more than two (2) subcontractors? | Yes. |
| RFP Attachment 6.6. Section A.6. | 27. | Are there any certification requirements for the project manager (i.e., PMP)? | No |
| RFP Attachment 6.6. Section A.9. | 28. | Is the State’s secure repository digital or analog? Assuming it is digital, are there any requirements for documents type (word, PDF, etc.)? | SharePoint with Microsoft Office documents preferred over PDF for ease of processing the content. |
| RFP Attachment 6.6. Section A.12. | 29. | For “enhanced POAM” recommendations, it may be appropriate to include items for which the entity does not have the right skill sets to implement or manage on an ongoing basis. Given the guidance of around tailoring, we assume that this is the correct advice, and this does not fall outside of the RFP guidelines for tailoring. Does STS agree this is appropriate? | Enhanced Recommendations (ERs) are likely to include technology the entity does not possess or have the resources to manage. ERs won't always be easy to implement but should be reasonable given the entity's resources and budget. The NCSR and POAM can be a tool to justify increased funding. |
| RFP Attachment 6.6. Section A.16. | 30. | The RFP states “The Contractor shall provide the State all retained data upon the State’s request. The State shall dictate the format in which the data is provided.” Will the State provide the format upfront? Asking the vendor to covert 1 years’ worth of data after the fact may create a large amount of unfunded work. | Format refers to media and archive formats. Standard and ordinary archiving tools such as gzip, rar, WinZip, Windows OS compressed folders, would be used. The physical media, if any, would be similarly standard and ordinary such as USB drives. |
| RFP Attachment 6.6. Section C.4. | 32. | Travel compensation is not provided. Does this apply to year 1 assessments, year 2 – 5 enhanced POAMs, or both? The enhanced POAMs, according to the RFP Attachment 6.6, section A12, ii “ii. General security consulting services will be required to create enhanced recommendations for the Entities to address items in their respective POAMs.” Since general security consulting typically requires travel, how is this funded, when we cannot forecast accurately now what travel requirements may be for remediation work, and this cannot blend it into hour hourly fee proposal. | The State will not pay separate travel costs for services provided under this Contract, regardless of the years.  Travel costs must be considered in the cost the respondent provides as part of RFP Attachment 6.3. |
|  | 33. | 1. Is the intention to award to multiple companies, or are you intending to award to one company? 2. How big of a pool of vendors are you willing to consider? | See State’s response to question #3.  The State will evaluate all responses that pass Section A, Mandatory, but will award to only one vendor. |
|  | 34. | Would you consider allowing vendors 30 days post award to provide a certificate of insurance? | No. Please refer to Proforma Section D.32 Insurance. |
|  | 35. | Can the Security Assessment be done remotely? | Yes |
|  | 36. | Of the approximately 1,332 counties what states are those counties located in? | All entities are located in Tennessee |
|  | 37. | Will the winning Vendor be provided with all the Entities to be assessed at the start of contract? | The State will provide the winning contractor a contact list of Entities per Pro Forma section A.10. |
|  | 38. | Is a 12-month time frame for Phase 1 a mandatory requirement that needs to be followed?  Or will there be some room to extend past the 12months based on the number of entities? | See State’s response to question #6. |
|  | 39. | When is the project expected to start? | See State’s response to question #6. |
|  | 40. | Will the winning Vendor be responsible for registering for the entity for NSCR? | Yes – each entity will currently be required to have their own dedicated NCSR account, in addition to the vendor and/or State having an account. It is the expectation that the vendor will assist the entity in the registration process. |
|  | 41. | Will the winning Vendor be working together with the entity to complete the NSCRS questionnaire? | Yes |
|  | 42. | Will there be multiple vendors awarded? | See State’s response to question #3. |
|  | 43. | Can Company references and referrals be substituted for principals who will be working on contract to provide references? | No. The State must receive references per the RFP requirement. |
| RFP section 3.3 | 44. | Response and respondent prohibitions:  The RFP does not allow for any alternate terms and conditions to be proposed. Not allowing any proposed changes to the pro forma makes it very difficult for very large companies to respond to this type of procurement. Large companies in general have the best ability to meet your requirements due to the maturity of their product offerings and their financial stability. Additionally, many other State of TN RFPs have allowed for red-lines of the RFP in the past. Will the State please re-consider this requirement, and potentially add a requirement to section B to allow for pro forma red-lines? Will the State consider the addition of terms to the pro forma contract if they do not conflict with the State's terms? | The State will not agree to this request. See Sections 3.3.1., 3.3.2., and 5.3.5. of the RFP. |
| Attachment 6.2, B.13 | 45. | Follow the personnel roster with a resume for each of the people listed  Will the State accept an employee industry experience biography as an alternative to a resume? Resumes contain personal information. | Yes, if it meets the requirements of B.13. |
| RFP Section 2.1 schedule of events | 46. | Response deadline October 31:  There are only 7 days from when the questions are answered by the State and the RFP response is due. This does not give the respondents ample time to review and digest the State's answers to the questions, and update the RFP content accordingly. As such, will the State consider extending the RFP response deadline 2 weeks? | RFP Amendment 1 extended the response deadline. |
| RFP Section 2.1 schedule of events | 47. | Negotiations 11/9/22-11/15/22:  If the State will not consider any proposed changes/red-lines to the pro forma contract, what exactly is the intent of the negotiations period in the RFP schedule of events? | This is for the State to conduct cost negotiations. |
| Attachment 6.6,Pro Forma Contract | 48. | D.32. Insurance:  If bidder's insurance policies comply in all material respects with the requirements of Section D.32, will the State be willing to consider minor modifications to the language in D.32 to more accurately reflect actual language in contractor's coverage? | The State will not agree to this request. |
| RFP attachment 6.3 | 49. | Cost Proposal:  Since the State allows the respondents to return soft copies of the cost proposal in both PDF or XLS format, would the State please provide a copy of the cost proposal in XLS format? | The State will not provide an excel template. |
| Attachment 6.6,Pro Forma Contract | 50. | E.6. Contractor Hosted Services Confidential Data, Audit, and Other Requirements  d. “Confidential State Data” is defined as data deemed confidential by State or Federal statute or regulation. The Contractor shall protect Confidential State Data as follows:  (3) The Contractor shall ensure that all Confidential State Data is housed in the continental United States, inclusive of backup data.  (4) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard (“FIPS”) 140-2 validated encryption technologies.  (5) The Contractor and the Contractor’s processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization (“ISO”) 27001; (ii) Federal Risk and Authorization Management Program (“FedRAMP”); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants (“AICPA”) for a System and Organization Controls for service organizations (“SOC”) Type II audit. The State shall approve the SOC audit control objectives. The Contractor shall provide proof of current ISO certification or FedRAMP authorization for the Contractor and Subcontractor(s), or provide the State with the Contractor’s and Subcontractor’s annual SOC Type II audit report within 30 days from when the CPA firm provides the audit report to the Contractor or Subcontractor. The Contractor shall submit corrective action plans to the State for any issues included in the audit report within 30 days after the CPA firm provides the audit report to the Contractor or Subcontractor.  If the scope of the most recent SOC audit report does not include all of the current State fiscal year, upon request from the State, the Contractor must provide to the State a letter from the Contractor or Subcontractor stating whether the Contractor or Subcontractor made any material changes to their control environment since the prior audit and, if so, whether the changes, in the opinion of the Contractor or Subcontractor, would negatively affect the auditor’s opinion in the most recent audit report.  No additional funding shall be allocated for these certifications, authorizations, or audits as these are included in the Maximum Liability of this Contract.  Can you please explain how this requirement extends to the contractor's existing information technology (IT) infrastructure that is not part of this contract? For example, if the contractor happens to have an IT environment consisting of networks and data centers that are not used in delivery of services for this contract, are they subject to the FedRAMP certification? We understand this requirement as it relates to pro forma contract section "A.16 Project Management – Central Repository and Portal," but request clarification on where else E.5 may apply. Surely the requirement under this contract is not intended to impose FedRAMP requirements on all of a prospective contractor's IT infrastructure not involved in the delivery of services within this RFP. | IT infrastructure involved in the transfer, storage, or processing of data and documents for this project must be either ISO 27001, FedRAMP, or SOC 2 compliant. If there is infrastructure that is not compliant with any of these, it must be outside the security boundary of the compliant environment used for this project. |
| Attachment 6.6,Pro Forma Contract | 51. | C.5 invoice requirements -- contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than 30 days after the goods or services have been provided…  Neither the RFP nor the Proforma Contract template set out a specific date when payments are due from the State to REDACTED. The issue is addressed somewhat conceptually in the documents, but not definitively as to the date when payments will be due. To avoid uncertainty and potential disputes, will the State consider adding language referencing the Tennessee Prompt Payment Act, Tenn. Code Ann. § 12-4-701, et seq. (the “Prompt Pay Act”). The Prompt Payment Act states that that payment shall be made within forty-five (45) days after receipt of invoice and allows interest in a specified amount for overdue payments beginning on the day after payment is due. If the State is not amenable to using the Prompt Payment act as determinative of payment terms, REDACTED would be willing to discuss alternatives proposed by the State regarding the timing of payments. | As the Pro Forma Contract does not specify a date, the Prompt Pay Act is applicable and when an invoice is received in accordance with Pro Forma Contract C.5.c |
| A.6. | 52. | The Contractor shall provide a full-time dedicated project manager to the project. The project manager shall be the key point of contact between the Contractor and the State related to the deliverables of this Contract.  Will the State provide a project manager to assist in coordination with the 1300+ entities or will the contractor project manager be responsible for outreach and coordination based upon the list of contacts provided by STS? | The State intends to hire two full time employees dedicated to this project. They will be tasked with assisting the contractor’s PM. |
| A.11. | 53. | The Department of Homeland Security (DHS) & the Multi-State Information Sharing and Analysis Center (MS-ISAC).accepts NCSR submissions annually from October 1 to February 28. Therefore, the Contractor shall complete Phase 1 NSCR assessments and POAM deliverables as necessary to meet those time constraints.  Given contract signature is scheduled for November 30, 2022 and the NCSR submissions are due February 28, 2023, does the State anticipate that all 1300+ entities will achieve the phase 1 objectives? | See State’s response to question #6. |
| A.11. | 54. | The Department of Homeland Security (DHS) & the Multi-State Information Sharing and Analysis Center (MS-ISAC).accepts NCSR submissions annually from October 1 to February 28. Therefore, the Contractor shall complete Phase 1 NSCR assessments and POAM deliverables as necessary to meet those time constraints.  Will the state provide a contact list for the 1300 + entities? Will the state provide project management resource(s) for phase 1 engagements? | See State’s response to question #6 and #37 |
| A.8. | 55. | Within ten business days following the NCSR assessment, the Contractor shall create a Plan of Actions and Milestones (POAM) for each Entity. A POAM template is provided in Attachment 2, but it shall be developed and/or adjusted in conjunction with the State such that it meets the needs of the Entities and is compatible with STS’ Governance Risk and Compliance (GRC) tool.   1. POAMs will be considered accepted by the State unless otherwise noted within 10 business days.   Will the State require access to STS' GRC tool for POAM creation or will the State provide a template that will be completed offline that can be uploaded into the tool? | The State will provide the template in Attachment 2 and that will be uploaded into the GRC tool. |
| Pro forma contract | 56. | C.5 invoice requirements -- contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than 30 days after the goods or services have been provided…  Will the State consider revising this requirement to within 180 days after the goods and services have been provided? Due to billing cut off cycles occurring once per month, it may not be possible to meet 30 days. | The State will not agree to this request. |
|  | 57. | Can subcontractors be used to deliver the primary services? With 1,300+ entities over 36 months, at 45 hours estimate per, the vendor would need to perform nine (9) assessments per week. | Yes, and see the State’s response to question #6. |
|  | 58 | We are a global company. Can we utilize overseas resources to deliver our assessment services as well as our U.S.-based personnel? | Contractors and subcontractors must be located in the United States. |
|  | 59. | As the NASCIO assessment for year 2022 is due to be completed by Feb 2023 and the contract award date is not expected to be 11/30/2022.  Is the expectation that Phase 1 is to be completed for the 2023 NASCIO submission year (Oct 2023 – Feb 2024) or is the intent of TN to conduct an “out of band NASCIO” assessment. | See State’s response to question #6. |
|  | 60. | The NASCIO assessment will require close coordination with all 1300+ entities indicated by TN.  There are on occasion resource issues and/or scheduling delays that one of the aforementioned entity (not the contractor conducting the assessment) may run into that would delay the delivery of their assessment.  Does TN have a process to track and/or not hold the contractor liable for non-delivery should there be an instance of an entity not being able to get information back to the contractor in a timely manner? | The State will have two FTEs dedicated to tracking deliverables by the vendor. Constant communication about the status of all entities will be expected to track any blockers presented by the entities to avoid holding the vendor to account for specific failed deliverables like this. |
|  | 61. | TN indicates that the assessments and POAMs should be loaded into the TN STS GRC solution.  Is there a format that we are able to see to ensure we can meet this requirement and is the GRC tool being utilized capable of API connections from 3rd parties? | The State will provide the template in Attachment 2 and that will be uploaded into the GRC tool.  There will be no API access to the state's internal Archer system. Any data added to Archer will be either done manually or via CSV imports to be completed by the State. |
|  | 62. | RFP indicates that there must be a prime and two subcontractors listed in the RFP.  It is unclear if the prime must be able to perform all the work solely (and the subcontractors are only if the prime is unable to meet the deliverable requirements) or if the prime and subcontractors are able to load share as part of the strategy (and not as a failsafe). | Respondents may utilize subcontractors at any point to complete any amount of the work.  The utilization of subcontractors is not required, so long as, the prime does not fall behind the master schedule as discussed in A.10.a.  The subcontractor requirement is a failsafe for respondents that intend to complete the entirety of the work as the prime. |
|  | 63. | RFP indicates there must be two subcontractors.  Would TN accept one subcontractor? | No, The Contractor must propose two (2) subcontractors. |
|  | 64. | Will respondent(s)  (Prime & Subs) be allowed to bid on services and opportunities that stem from Phase 1 & 2 or will they be barred from bidding on this work. | This RFP will not preclude any Prime or Subcontractor from being allowed to bid on potential future phases of work. |
|  | 65. | Regarding insurance requirement for respondent(s).  Would TN accept 10M total in cyber and umbrella insurance combined or must it be a specifically 10M in Cyber Insurance? | Yes, the State will accept a combination of an underlying cyber liability policy for $5m with a supporting umbrella for the additional $5m. |
| D. Mandatory Terms and Conditions | 66. | Can the vendor leverage offshore (outside of the US) resources? | Contractors and subcontractors must be located in the United States. |
| Scope (A.11) | 67. | For Phase 1, does the State plan for the Contractor to schedule and assist all 1,300 county, city, K-12, and higher education entities in completing the 2022 NCSR after the contract start date in December 2022 through the time remaining to complete the 2022 NCSR through 2/28/23? Or is acceptable for the Contractor to schedule and assist an initial subset of the county, city, K-12 and higher education entities in completing the 2022 NCSR during the time remaining in the 2022 NCSR open period after contract start date and then schedule and assist the remaining entities during 2023 NCSR open period which starts in 10/1/23? | See State’s response to question #6. |
| Scope (A.17) | 68. | Please clarify if the two required sub-contractors must be actively participating in the NCSR assessment or are the subcontractors only to be maintained throughout the term of the contract to be utilized to complete the contract deliverables if the State identifies a need? | See State’s response to question #62. |
| Scope (A.10) | 69. | Will STS identify the Point Of Contacts (POCs) from each entity that will be responsible for completing the NCSR assessment on behalf of the entity or will it be respondent's responsibility to identify those POCs? | See State’s response to question #37. |
| 1.1. Statement of Procurement Purpose | 70. | Will the state be providing access to the State Governance Risk and Compliance (GRC) tool to each entity (if needed for centralized management of their data, collection of any artifacts as a part of this assessment) or will the respondent be the only party with access for POA&M tracking and updates? | For technical, security, and user management reasons, no Archer access will be granted to the entities. The exact process and extent of NCSR and POAM data to be imported into Archer is to be determined. |
| 3.1 Response Format, 3.1.1.2 | 71. | Is it acceptable to the State for the vendor's narrative text to be formatted as 12 point while graphics and tables are smaller as long as the text is readable? | Yes. |
| A.4 (Phase 1) | 72. | What outreach has STS conducted, or plans to conduct prior to the start of the engagement, to stakeholders with the localities to inform them of the upcoming CIS NCSR assessment activities? | Nothing has yet been advertised other than through word of mouth at one or more conferences. This outreach is the beginning of the project. |
|  | 73. | Are there statewide cyber policies used by all 1,332 Entities or do they have their own? | State agencies must comply with the EISP, which is a public document. It is not mandatory or enforceable for other than state level departments. The other entities will have their own policies. |
|  | 74. | Do any of the Entities currently use or run a SOC? | The State does not know. The question will likely come up in the NCSR survey. |
|  | 75. | Does each Entity conform to the same framework or do some need to have visibility into other compliance frameworks such as PCI, HIPAA, etc. as part of their oversight? | It will vary. Each entity handles different classifications of data. |
|  | 76. | Is each Entity required to participate in this program or is it voluntary? | It is voluntary. |
| A.6. | 77. | Will the State have a dedicated project manager to help assure entities have timely response to provided questionnaires? | See State’s response to question #52. |
| A.8. | 78. | Will the State provide the name of the GRC tool and particular module where this work may be completed? | See State’s response to question #14. |
|  | 79. | Will the contractor awarded this bid be precluded from providing goods and services to satisfy the gaps identified in the assessments? | See State’s response to question #64. |
| Page 6. Section 3.1.2.2 | 80. | Page 6, Section 3.1.2.2. states: The proposed cost shall incorporate ALL costs for services under the contract for the total contract period, including any renewals or extensions. Does this mean that our pricing needs to be good for five years and include any travel (Section C. 4.) as well? | Yes, that is correct. |
|  | 81. | Do we need to meet a certain percentage of participation by business enterprises owned by minorities, women, service-disabled veterans, persons with disabilities and small business enterprises? | Although there is no requirement for this participation, the B.15 portion of the proposal will be evaluated and is included with other questions in the General Qualifications and Experience section with point value. The Dept. of Finance & Administration views diversity in their proposals as very important, with $102 million of their overall spend coming from diversity businesses. |
| RFP Attachment 6.2 – Section B, Item Ref. B.13 | 82. | Rather than listing actual, named individuals in our response, can we provide the information requested using job roles/descriptions? | No, this does not meet this requirement. |
| RFP Attachment 6.2 – Section B, Item Ref. B.15 (c) | 83. | Estimated Participation: Is participation (as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics) by business enterprises owned by minorities, women, service-disabled veterans, etc. a requirement or encouraged? Is this part of the evaluation criteria and how will this be scored? | Participation is highly encouraged. The dept. of Finance and Administration views DBE participation as very important. $102 million of the overall spend from F&A coming from DBE’s last fiscal year. The section will be scored wholistically with the other questions within the B section. Please answer all the B.15 question and its sections to the best of your ability. |
| Pg. 1 (Intro), Pg. 37, (Contract) | 84. | Are we able to use an STS provided tool for CRM (track conversations, scheduling, and call backs with the entities)? | No CRM tool will be provided by the State. |
| A.4 & A.10 | 85. | STS shall provide the contact lists, how many contacts have been identified for each:  -Wide Area Networks: ? of 10  -Counties: ? of 95  -Cities: ? of 345  -Post Secondary Schools: ? of 134  -K-12 Schools: ? of 748 | See State’s response to question #37. |
| A.4 & A.10 | 86. | For planning purposes, what date should we expect each of the contacts to have been identified, the contact list assumes; (Name, Role, Email, Phone Number)? | See State’s response to question #6.  Please also refer to Pro Forma section A.10.a. A schedule will be developed. |
| A.4 & A.10 | 87. | STS shall provide the contact lists, how many entities have been made aware of the project and it's objectives for each:  -Wide Area Networks: ? of 10  -Counties: ? of 95  -Cities: ? of 345  -Post Secondary Schools: ? of 134  -K-12 Schools: ? of 748 | See State’s response to question #85. |
| A.4 & A.10 | 88. | What communications have been developed for education of the program, may we receive copies? | See State’s response to question #72. |
| A.3 & A.11. | 89. | Conflict in requirements: A.3 indicates Phase 1 is one year, A.11 Indicates contractor shall be done with Phase 1 by 2/28/2023, which is 3 months after award. Are we able to continue to support in-scope entities for Phase 1 activities, if they are unprepared to participate by 2/28/2023, in later cycles (i.e., 2024, 2025). | See State’s response to question #6. |
| Section 6.2 B.16 & B.17 | 90 | Do the requirements fall to the subcontractors as well? | No. |
| Section 6.4 Reference Questionnaire | 91. | May the subcontractors contribute to the references? | No. |
|  | 92. | Phase 1 – Is the end Feb ’23 or 1 year from the contract signature? | See State’s response to question #6. |
|  | 93. | NCSR Process – Has all entities NCSR review needs to be completed by Feb ’23 or a limited subset? | See State’s response to question #6. |
|  | 94. | Has NCSR process been communicated to all the entities and are they ready to engage with contractors actively | See State’s response to question #72. |
|  | 95. | Will the selected contractor be required to do outreach to entities to sign them up for participating in NCSR Process? | Yes |
|  | 96. | On schedule – after questions have been answered, there is only one week to make changes. Will State consider extending the deadline to provide a response (or shortening the time state has to respond to questions) | See State’s response to question #46. |
| A.11. | 97. | there is no mention of what complete means (is it all entities or a subset of entities) | See State’s response to question #6.  The contractor shall complete assessments for all entities identified during phase 1.  Additional entities may volunteer to participate during future years of the contract. New volunteers shall have assessments completed during the current/next available NCSR submission period. |
| A.12. | 98. | is there a deadline for this submission? | Yes, Refer to RFP Section 2.1 Schedule of Events. |
|  | 99. | Do all resources in this project need to be based in the US? | Yes |
|  | 100. | Is there reciprocity for Diversity for entities qualified in other States? | Yes |
|  | 101 | How many references does the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions require in response to this RFP? | Please refer to RFP Attachment 6.4 Reference Questionnaire for the number of required references. |
|  | 102 | Does the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions consider and accept past experience within the State as a reference for this RFP response? | Refer to RFP Attachment 6.4. |
|  | 103. | What will be the period of performance for completion of Phase 1? The NCSR opens on October 1 and closes on February 28, and since this contract will not be awarded until December 2022, will the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions allow more time to complete Phase 1 for the NCSR self-assessment? | See State’s response to question #6. |
|  | 104. | Does the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions have a current commitment of entities or a minimum number of entities that have committed to participate in the NCSR self-assessment with the State of Tennessee, Finance & Administration – Strategic Technology Solutions? | No entities have committed at this time. |
|  | 105 | What are the requirements for evidence of signing and commitment authority? | See State’s answer to Question #25. |
|  | 106. | Does the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions require the Contractor to perform the self-assessment on behalf of the 1,332 entities or provide guidance and assistance in enabling those entities’ response to the self-assessment? | Contractor shall complete the NCSR process for the entities per Pro Forma section A.4. |
|  | 107. | Have any of the 1332 entities performed the NCSR self-assessments in prior years? | The State does not know.  That will be part of the assessment process. |
|  | 108. | When will be the deadline for entities to opt-in to the NCSR self-assessment? | See State’s response to question #6 and #97. |
|  | 109. | How does the State of Tennessee Department of Finance & Administration – Strategic Technology Solutions currently view the collection of the NCSR self-assessment material and the uploading of that information to NCSR? | See State’s response to question #15. |
| RFP Section A.12.a.iii. | 110. | “The Contractor shall provide security system(s) design consulting services including but not limited to, networking, storage, intrusion detection/prevention systems, routers, switches, firewalls, logging, physical security systems, server, and workstation security configuration.”   * 1. Will this include broad specifications or direct configuration file technical implementation requirements? | This will be more focused on broad specifications and recommendations as an enhanced, value add POAM for the entity upon completion of the NCSR. The vendor is not expected to have a highly detailed technical understanding of the entities network, but should be able to provide general suggestions on tools to increase their security posture. |
|  | 111. | Can the State confirm if the list of attendees at the pre-proposal conference will be published for this solicitation? | No, this is not public knowledge during the RFP. |
| Introduction - Section 1.1 – Procurement Purpose, Page 2 | 112. | The RFP indicates that there are “approximately 1,332 county, city, K-12, and higher education Entities” in scope. Can you please provide a list of entities by type and approximate size including a public address and contact information for the main point of contact for each in-scope entity? | See State’s response to question #37.  The State does not currently have size/type information at this time. |
| Introduction - Section 1.2 – Procurement Purpose, Page 2 | 113. | Can the State identify which entities have previously completed the NCSR? | See State’s response to question #107. |
| Introduction - Section 1.3 – Procurement Purpose, Page 2 | 114. | Can the State identify which entities will be using the NCSR for grant requirements? | No |
| Section 2 – Schedule, 2.1 | 115. | RFP schedule lists that the contract will be signed on Nov. 30, 2022, with an initial pilot assessment of STS to be completed first. Tool will only be available between October 1, 2022, and February 28, 2023 (annual availability window), and the 1-year anniversary will be Nov. 30, 2023, which does not leave sufficient time to complete all of the assessments and POAM by the end of Year 1. Is the State open to adjusting the Phase 1 timelines to allow all sites to be completed and POAM delivered by February 2024? | See State’s response to question #6. |
| Contract - Phase I – A.5 | 116. | Is the expectation that most of the entities will have the NCSR template data ready for upload into the portal or will the contractor be responsible for collecting the required data from each entity? | The State expects most entities will be starting from scratch and the Contractor will be responsible for assisting with the collection of data. Some entities may be proactive and provide the data, but it is unlikely. |
| Contract - Phase I – A.8 | 117. | Are all 1,332 entities being held to the same security compliance standard(s) while developing POAM recommendations? | Yes but, if the entity handles FTI or other confidential information, the Phase 2 Enhanced Recommendations would be more stringent than for an entity that deals entirely with public information. |
| Contract - Phase I – A.9 | 118. | What is the State's secure repository? And how will the contractor access it? | See State’s response to question #14. |
| Contract - Phase I – A.11 | 119. | Is the expectation that all 1,332 NCSR assessments will be complete and uploaded between 10/1/2023 and 2/28/2024? | See State’s response to question #6 and #97. |
| Contract - Phase II – A.18 | 120. | Warranty - Please provide specifics as to what is covered by the warranty with regards to the NCSR data collection and entry? | The Contractor will be providing a service under this Contract. |
| Contracts - Mandatory T's & C's – D.20 | 121. | HIPAA compliance - Does the State expect the Contractor to process HIPAA data? And if so under what circumstances? | No. Even if the entity is a health care provider, there is no reason for HIPAA data to be a part of the NCSR. |
| Contracts - Mandatory T's & C's – E.7 | 122. | Will the State be providing PC equipment for NCSR data collection teams? Or use a virtual desktop? | No hardware or software will be supplied by the State. Access to STS' SharePoint may be provided. |
| Attachment 6.2 - Section A – A.4 & A.5 | 123. | Regarding references outlined in section A.4 and A.5, will a combination of team references be acceptable if recent acquisitions or divestures present issues with previous clients? | A combination of references is acceptable as long as they part of the same overall project that meets the project size requirements documented in A.4. |
| Attachment 6.2 - Section C. – C.2 | 124. | The technology footprint of the county/city entities in TN: what is the breakdown of independently (locally) run, versus the percentage that have technology services centrally managed and run by a centralized team or location? | STS does not have the visibility into the entities' IT operations to know how they are organized. |
| Scope of Service, Contract Period, & Required Terms and Conditions, RFP Section 1.2 | 125. | The pro forma contract substantially represents the contract document that the successful Respondent must sign.  Whereas the overall success in this project can best be achieved through a professional business relationship predicated on mutually agreed responsibilities, costs and risk allocation as documented in a clear contractual agreement, and the Pro Forma Contract appears to be a standard agreement that has not been tailored to this specific transaction or these services, at what point and under what circumstances will a Respondent be permitted to identify missing provisions and the provisions of the Pro Forma Contract which require refinement to properly govern the services as they are contemplated by this RFP? | Questions or comments identifying missing provisions or provisions that a Respondent believes require refinement must have been submitted during Questions and Comments. |
| Cost Proposal – Section 3.1.2.2 | 126. | The proposed cost shall incorporate ALL costs for services under the contract for the total contract period, including any renewals or extensions.  Whereas inflation and rising labor costs have the potential to substantially increase a Respondent’s costs in delivering the services contemplated by the RFP, what is the State’s tolerance to including a variable rate (year to year) of the rates offered in the cost proposal? For example, a 3% increase of rates offered year over year? | The State will not agree to this request. |
| Response & Respondent Prohibitions – RFP Section 3.3.11 – 3.3.2 | 127. | A response must not include alternate contract terms and conditions. If a response contains such terms and conditions, the State, at its sole discretion, may determine the response to be a non- responsive counteroffer and reject it. 3.3.2. A Respondent shall not include in its response, or after contract award, any end-user license agreement, manufacturer’s terms and conditions, service guide, clickwrap agreement, shrink-wrap agreement, online terms and conditions, or other terms and conditions that supplement, modify, or contradict the terms set forth in the pro forma contract.  Whereas the Pro Forma Contract appears to be a standard agreement that has not been tailored to this specific transaction or these services, but the RFP prohibits the inclusion of additional or alternative contract terms which would be required to sufficiently govern the services as they are contemplated by this RFP, at what point in the procurement process will the Respondents be made aware of what is and is not negotiable by the State? | Questions or comments identifying missing provisions or provisions that a Respondent believes require refinement must have been submitted during Questions and Comments. |
| Response & Respondent Prohibitions – RFP Section 3.3.3 | 128. | A response must not restrict the rights of the State or otherwise qualify either the offer to deliver goods or provide services as required by this RFP or the Cost Proposal. If a response restricts the rights of the State or otherwise qualifies either the offer to deliver goods or provide services as required by this RFP or the Cost Proposal, the State, at its sole discretion, may determine the response to be a non-responsive counteroffer and reject it.  If a Respondent states its proposal is expressly subject to the parties’ mutual agreement on the key legal terms and conditions either missing from or that require refinement within the Pro Forma Contract and should not be considered an acceptance of the Pro Forma Contract as written, does the State view the foregoing condition as a response that “restricts the rights of the State or otherwise qualifies either the offer to deliver goods or provide services as required by this RFP or the Cost Proposal” and thus subject to a finding that the proposal is non-responsive? | Yes, |
| Disclosure of Response Contents – RFP Section 4.8.3 | 129. | Upon completion of response evaluations, indicated by public release of a Notice of Intent to Award, the responses and associated materials will be open for review by the public in accordance with Tenn. Code Ann. § 10-7-504(a)(7).  Are there any applicable exceptions under Tenn. Code Ann. § 10-7-504 that would allow proprietary information, personal identifiable information, or trade secrets that are included as part of a Respondent’s proposal to be withheld from public disclosure? | No, all responses are open for public review during the Intent to Award / Open file period. |
| Evaluation Process – RFP Section 5.2.3 and subsection 5.2.3.2 | 130. | The State reserves the right to award a contract on the basis of initial responses received, therefore, each response shall contain the Respondent’s best terms and conditions from a technical and cost standpoint. The State reserves the right to conduct clarifications or negotiations with one or more Respondents. All communications, clarifications, and negotiations shall be conducted in a manner that supports fairness in response improvement. 5.2.3.2 Negotiations: The State may elect to negotiate with one or more Respondents by requesting revised responses, negotiating costs, or finalizing contract terms and conditions. The State reserves the right to conduct multiple negotiation rounds or no negotiations at all  Whereas RFP Section 3.3 prohibits the Respondents from providing additional or alternative contract terms which the Respondents may perceive are required to sufficiently govern the services as they are contemplated by this RFP, at what point will the Respondents be permitted to identify missing provisions and the provisions of the Pro Forma Contract which require refinement to properly govern the services as they are contemplated by this RFP? Please further elaborate on the process of identification and negotiation of final terms and conditions that will occur between the State and the Respondent identified as offering the apparent best-evaluated response. | See State’s response to Question # 125 and 127.  See also Section 5.3.5. of the RFP. |
| Contract Award Process – RFP Section 5.3.4-5.3.5 | 131. | The Respondent identified as offering the apparent best-evaluated response must sign a contract drawn by the State pursuant to this RFP. The Contract shall be substantially the same as the RFP Attachment 6.6., Pro Forma Contract. The Respondent must sign the contract by the Contractor Signature Deadline detailed in the RFP Section 2, Schedule of Events. If the Respondent fails to provide the signed Contract by this deadline, the State may determine that the Respondent is non-responsive to this RFP and reject the response.  Notwithstanding the foregoing, the State may, at its sole discretion, entertain limited terms and conditions or pricing negotiations prior to Contract signing and, as a result, revise the pro forma contract terms and conditions or performance requirements in the State’s best interests, PROVIDED THAT such revision of terms and conditions or performance requirements shall NOT materially affect the basis of response evaluations or negatively impact the competitive nature of the RFP and contractor selection process.  Whereas the RFP Section 3.3 prohibits the Respondents from providing additional or alternative contract terms which the Respondents may perceive are required to sufficiently govern the services as they are contemplated by this RFP, at what point will the Respondents be permitted to identify missing provisions and the provisions of the Pro Forma Contract which require refinement to properly govern the services as they are contemplated by this RFP?  Please further elaborate on the process of identification and negotiation of final terms and conditions that will occur between the State and the Respondent identified as offering the apparent best-evaluated response and how the inclusion of alternative or additional terms at this stage will be fair and equitable to all other respondents who perceived the terms and conditions of the Pro Forma Contract as non-negotiable? | See State’s response to Question # 125 and 127. |
| STATEMENT OF CERTIFICATIONS AND ASSURANCES – Attachment 6.1 | 132. | • The Respondent, except as otherwise provided in this RFP, accepts and agrees to all terms and conditions set out in the RFP Attachment 6.6., Pro Forma Contract.  • The Respondent acknowledges and agrees that a contract resulting from the RFP shall incorporate, by reference, all proposal responses as a part of the Contract.  • Both the Technical Response and the Cost Proposal submitted in response to this RFP shall remain valid for at least 120 days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract pursuant to the RFP.  Whereas the RFP Section 3.3 prohibits the Respondents from providing additional or alternative contract terms which the Respondents may perceive are required to sufficiently govern the services as they are contemplated by this RFP, but then Sections 5.2.3 and 5.2.4 imply that the State may entertain negotiations of terms and conditions of the Pro Forma Contract, how does the State reconcile that a Respondent “accepts and agrees to all terms and conditions set out in the RFP Attachment 6.6., Pro Forma Contract” but then may be permitted to negotiate terms or conditions during negotiations with the State?  If Respondents aren’t allowed to provide exceptions or supplemental language, please elaborate how and under what circumstances alternative or additional terms and conditions will negotiated. | See State’s response to Question # 125 and 127. |
| Attachment 6.6 PRO FORMA Contract – Attachment 6.6 – Section A.14 | 133. | Contractor shall comply with the State of Tennessee’s enterprise security policies requirements and any other State and federal computer security regulations including cooperation and coordination with the State’s Strategic Technology Solutions security management team and other compliance officers required by its regulations.  Whereas the State is in the best position to identify which policies or regulations will be applicable to the vendor or the specific services required under this RFP, can the State identify or agree to identify and provide those policies and regulations it perceives applicable to vendor throughout life of the contract? | The policies can be found by following the link in Pro Forma section A.14 and reviewing the “Enterprise Information Security Policies” PDF. |
| Attachment 6.6 PRO FORMA Contract – Attachment 6.6 Section A.18 | 134. | Contractor represents and warrants that the term of the warranty (“Warranty Period”) shall be the greater of the Term of this Contract or any other warranty generally offered by Contractor, its suppliers, or manufacturers to customers of its goods or services. The goods or services provided under this Contract shall conform to the terms and conditions of this Contract throughout the Warranty Period. Any nonconformance of the goods or services to the terms and conditions of this Contract shall constitute a “Defect” and shall be considered “Defective.” If Contractor receives notice of a Defect during the Warranty Period, then Contractor shall correct the Defect, at no additional charge.  Contractor represents and warrants that all goods or services provided under this Contract shall be provided in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Contractor’s industry  .  Because the security assessments (Phase 1) are based on circumstances as they existed at a specific point in time and the Advanced Recommendations (Phase 2) are based on the circumstances and the information made available to the vendor at the time of the initial assessment, this warranty does not seem feasible or proper for the type of services as contemplated by the RFP. For example, recommendations could change based on industry updates, technology, or threats and risks. Accordingly, what is the State’ tolerance to refining this provision and limiting the Warranty Period to the time during which the assessment of each entity is ongoing?  Further, whereas the timeliness of delivery is subjective and will not have meaning without agreed schedules or timelines, what is the State’s tolerance to editing this language to reference the mutually agreed schedule or timelines? | The State will not agree to this request. |
| Attachment 6.6 PRO FORMA Contract – Section B.1 | 135. | This Contract may be renewed upon satisfactory completion of the Term. The State reserves the right to execute up to two (2) renewal options under the same terms and conditions for a period not to exceed twelve (12) months each by the State, at the State's sole option. In no event, however, shall the maximum Term, including all renewals or extensions, exceed a total of sixty (60) months.  Whereas inflation and rising labor costs have the potential to substantially increase the vendor’s costs in delivering the services contemplated by the RFP, what is the State’s tolerance to requiring mutual agreement for any renewal terms?  Additionally, or in the alternative, is the State amenable to including a mechanism by which the vendor can seek, no more frequently than annually, approval of a price/rate increase based on consumer price indexes? | The State declines to make these changes. |
| Attachment 6.6 PRO FORMA Contract – C.2. | 136. | Compensation Firm. The payment methodology in Section C.3. of this Contract shall constitute the entire compensation due the Contractor for all goods or services provided under this Contract regardless of the difficulty, materials or equipment required. The payment methodology includes all applicable taxes, fees, overhead, and all other direct and indirect costs incurred or to be incurred by the Contractor.  Whereas inflation and rising labor costs have the potential to substantially increase the vendor’s costs in delivering the services contemplated by the RFP, what is the State’s tolerance to including a mechanism by which the vendor can seek, no more frequently than annually, approval of a price/rate increase based on consumer price indexes? | The cost provided to the State are fixed for the term of the Contract. |
| Attachment 6.6 PRO FORMA Contract – C.7 | 137. | Invoice Reductions. The Contractor's invoice shall be subject to reduction for amounts included in any invoice or payment that is determined by the State, on the basis of audits conducted in accordance with the terms of this Contract, to not constitute proper compensation for goods delivered or services provided.  Whereas the Pro Form Contract does not include any dispute resolution or escalation process, what is the State’s tolerance to including a process in which the Contractor can dispute invoice reductions? Alternatively, is the Sate amendable to clarifying that payments for invoices may only be withheld as a result of the audits contemplated by Section D.11 of the Prof Forma Contract? | The State will not agree to this request. |
| Attachment 6.6 PRO FORMA Contract – D.7 | 138. | The Contractor shall not assign this Contract or enter into a subcontract for any of the goods or services provided under this Contract without the prior written approval of the State. Notwithstanding any use of the approved subcontractors, the Contractor shall be the prime contractor and responsible for compliance with all terms and conditions of this Contract. The State reserves the right to request additional information or impose additional terms and conditions before approving an assignment of this Contract in whole or in part or the use of subcontractors in fulfilling the Contractor’s obligations under this Contract.  What is the State’s tolerance to (1) authorizing the assignment of payments due under the contract; and/or (2) assignment of the contract in the event of merger, acquisition, or other corporate restructuring? | 1) Payments cannot be assigned; the State will pay the Contractor.  2)Per Pro Forma Contract Section D.7., the State would need to be notified of and provide written approval of any assignment resulting from merger, acquisition, or other corporate restructuring. The State would not unreasonably withhold approval. |
| Attachment 6.6 PRO FORMA Contract – D.11 | 139. | Records: The Contractor shall maintain documentation for all charges under this Contract. The books, records, and documents of the Contractor, for work performed or money received under this Contract, shall be maintained for a period of five (5) full years from the date of the final payment and shall be subject to audit at any reasonable time and upon reasonable notice by the State, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.  Can the State identify examples of “documentation for all charges under this Contract” it perceives will be subject to audit? Whereas certain cost and salary data is considered by the Contractor to be confidential, if such information is not necessary to establish what work was performed under this contract or the payments received, can a Respondent assume it will not be part of any audit contemplated by this provision? Further is the State authorized to limit the frequency of any such suits to reduce interruption to a Contractor’s business operations? | The books, records, and documents the Contractor uses to document work performed or money received, such as purchase orders, invoices, financial statements, or other relevant documentation to establish that charges were in accordance with the terms of the contract.  The State declines to make changes to this provision. |
| Attachment 6.6 PRO FORMA Contract – D.18 | 140. | Contractor’s liability for all claims arising under this Contract shall be limited to an amount equal to two (2) times the Maximum Liability amount detailed in Section C.1. and as may be amended, PROVIDED THAT in no event shall this Section limit the liability of the Contractor for: (i) intellectual property or any Contractor indemnity obligations for infringement for third-party intellectual property rights; (ii) any claims covered by any specific provision in the Contract providing for liquidated damages; or (iii) any claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death. For clarity, except as otherwise expressly set forth in this Section, Contractor’s indemnification obligations and other remedies available under this Contract are subject to the limitations on liability set forth in this Section.  Whereas Tenn. Code Ann. § 12-3-701(a)(2) permits a chief procurement officer to authorize a limitation of liability for an amount less than two (2) times the maximum liability of to protect the State from increased costs, what is the State’s tolerance to reducing this limitation to 2x the amount paid to Contractor within the immediate 12 months preceding the claim giving rise to the liability? This clause and the negotiability thereof has the potential to greatly impact the prices a Respondent can offer.  Further, is the State amenable to including a bilateral waiver of consequential damages, in favor of the Contractor, similar to waiver included in the State’s favor in Section D.17? | The State will not agree to this request.  The State will not agree to this request. |
| Attachment 6.6 PRO FORMA Contract – D.19 | 141. | Hold Harmless. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims, liabilities, losses, and causes of action which may arise, accrue, or result to any person, firm, corporation, or other entity which may be injured or damaged as a result of acts, omissions, or negligence on the part of the Contractor, its employees, or any person acting for or on its or their behalf relating to this Contract. The Contractor further agrees it shall be liable for the reasonable cost of attorneys’ fees, court costs, expert witness fees, and other litigation expenses for the State to enforce the terms of this Contract.  In the event of any suit or claim, the Parties shall give each other immediate notice and provide all necessary assistance to respond. The failure of the State to give notice shall only relieve the Contractor of its obligations under this Section to the extent that the Contractor can demonstrate actual prejudice arising from the failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State in any legal matter, as the right to represent the State is governed by Tenn. Code Ann. § 8-6-106.  Please provide the State’s tolerance on refining this provision to ensure it applies only to third-party claims, only requires reimbursement of expenses actually awarded by a court, and otherwise limits the litigation expenses to which a Contractor is subject to reimburse if not given the authority and control over the litigation, since it will have no means to mitigate such costs and expenses. | The State will not agree to this request. |
| Attachment 6.6 PRO FORMA Contract – D.32 | 142. | [TEXT NOT INCLUDED FOR SAKE OF BREVITY]  Please provide the State’s tolerance on refining this provision to ensure that (1) coverage required to be primary and non-contributory is limited to Commercial Liability and Auto Liability policies; (2) obligation to name State as additional insured limited to Commercial Liability and Auto Liability policies; (3) waiver of subrogation limited to Commercial Liability, Auto Liability, and Worker’s compensation (however excluding subrogation in instances of gross negligence by the State); (4) notice of non-renewal to occur in accordance with policy rather than 30 days; (5) subcontractors covered only by their own policies; (6) COI’s are sufficient proofs of insurance and copies of policies will not be required since they are considered confidential; (7) worker’s compensation coverage will comply with what is statutorily required under Tennessee laws; (8) Technology Professional Liability Insurance will be limited only to the errors and omissions of contractor, and not the State and will be limited only to “ notification costs, credit card monitoring, and fines & penalties incurred by the State due to Contractor’s error or mistake”; and (9) Crime Insurance will be limited to “theft and fraud by any means, including a by a computer”, removal of the social engineering endorsement, and obligation to replace limited by the commercial availability of a similar product. | The State will not agree to this request. |
| Attachment 6.6 PRO FORMA Contract – E.5 | 143. | Intellectual Property Indemnity. The Contractor agrees to indemnify and hold harmless the State of Tennessee as well as its officers, agents, and employees from and against any and all claims or suits which may be brought against the State concerning or arising out of any claim of an alleged patent, copyright, trade secret or other intellectual property infringement. In any such claim or action brought against the State, the Contractor shall satisfy and indemnify the State for the amount of any settlement or final judgment, and the Contractor shall be responsible for all legal or other fees or expenses incurred by the State arising from any such claim. The State shall give the Contractor notice of any such claim or suit, however, the failure of the State to give such notice shall only relieve Contractor of its obligations under this Section to the extent Contractor can demonstrate actual prejudice arising from the State’s failure to give notice. This Section shall not grant the Contractor, through its attorneys, the right to represent the State of Tennessee in any legal matter, as provided in Tenn. Code Ann. § 8-6-106.  Please provide the State’s tolerance on refining this provision to ensure it applies only to third-party claims, only requires reimbursement of expenses actually awarded by a court, and otherwise limits the litigation expenses to which a Contractor is subject to reimburse if not given the authority and control over the litigation, since it will have no means to mitigate such costs and expenses. | The State will not agree to this revision. |
| Attachment 6.6 PRO FORMA Contract – E.6 | 144. | TEXT NOT INCLUDED FOR SAKE OF BREVITY]  Whereas the RFP contemplates that relevant data shall be stored and or processed by State owned resources, provide the State’s tolerance on refining this provision to ensure it applies to the services as contemplated by this RFP. | The State will not agree to this revision. |
|  | 145. | Given the limited window of time during which the CIS portal is available, will the awardee be expected to utilize the portal for the assessments? | See State’s response to question #6. |
|  | 146 | Can the State clarify the OCI clause? More specifically, if any of the ~1300 entities elect to NOT participate in the assessment, is the awardee still locked out of future engagements? Furthermore, since the awardee will consist of a single prime and two subs, are all three locked out of all future business? Just the prime? Only the  prime/sub that delivers the assessment for a given entity? | See State’s response to question #64. |
|  | 147. | With regard to the (2) subs, are there any requirements regarding what percentage of work must be performed by each sub? | See State’s response to question #62. |
|  | 148 | What is the PoP (Period of Performance) for the TN RFP? I assume that is the same period of lockout, where applicable? | Please refer to Pro Forma section B. There is no State “lockout.” |
|  | 149. | Would the State please confirm that five separate reference questionnaires must be returned. Would it be acceptable to submit three reference questionnaires from clients that have both open contracts and have completed projects with our firm? Is there any preference on the overlap of these categories? | Please refer to RFP Attachment 6.4 for requirements, but five (5) references are required. |
|  | 150. | Regarding the subcontractor requirement, we note RFP attachment 6.2, subsections B.14 and B.15, require some data on these subcontractors. Is there any additional information the State would like provided regarding their subcontractors? | No. |
|  | 151. | Can vendors provide both a full submission and a redacted public version of the proposal, such that our clients names, data, and contact information will not be released upon award notice? | No, Refer to RFP Section 4.8 Disclosures. |
|  | 152. | When performing the Nationwide Cybersecurity Review (NCSR), is the awarding contractor exclusively using the NCSR Response Scale & Question Set document to receive responses from all participating state of TN agencies and entities? | Any application or process may be used to collect responses, however all ratings and responses must fit the NCSR format otherwise they would be rejected by the NCSR application. |
|  | 153. | Do NCSR responses require security controls evidence, or will simple answers to the NCSR question set with scale suffice? | The NCSR does not require artifacts to back up assertions made in responses, nor does the State. |
|  | 154. | In terms of engaging state agencies and entities review, will physical site visits be required to validate NCSR and build POA&M? | NCSR assessments and POAMs work can be done remotely.  Although it is unlikely, some Enhanced Recommendations may require on-site work. |
|  | 155. | In production of this RFP, was there an RFI or a particular consulting company used to help set these requirements?  If so, who was this company? | There was no RFI conducted before building this RFP. |
|  | 156. | You have estimated an average of 45 hours per entity to complete the NCSR and POAM process. Does this incorporate just the assessment or also the surrounding activities (e.g., reaching out to the entities to convince them to undertake the NCSR, project management, reporting, quality assurance, etc.)? If not, are you open to more hours per entity? | It includes NCSR assessments, POAMS, and the surrounding activities. |
|  | 157. | How shall hours used to market the NCSR project to the state entities be billed if the entity ultimately determines it does not want to undergo an NCSR and POAM? | Hours would be billed under the “Completion of NCSR & POAM” line-item hourly rate for the time used marketing the project to entities. |
|  | 158. | Can you provide an estimate for how many entities you believe would be willing to undertake the NCSR in the first year? This will have a significant impact on how many FTEs are assigned to the scope of work, since the number could range from 0 to 1332. | See State’s response to question #6  Please also refer to Pro Forma section A.10.a. A schedule will be developed. |
|  | 159. | Are you willing to accept changes to the insurance requirements, in particular the Technology Professional Liability/Cyber Liability and Crime Insurance. For example:   * + - The RFP requires Technology Professional Liability (Errors & Omissions)/Cyber Liability Insurance with limits of not less than $10,000,000 per occurrence or claim and $10,000,000 annual aggregate. As a small business, we have found that it is difficult to find insurance companies willing to cover this level of insurance for the type of work requested. Insurance companies typically classify the services under the agreement to fall under General and Professional Liability and not Cyber/Technology Insurance, especially since we do not remove any data from the environment. For those reasons, we are requesting an official change to reflect a Cyber Insurance of $1M which is in accordance with the risk, contract, services we will provide. | See State’s response to Question #65. |
| E.6 (5) | 160. | E.6.(5) of the Sample Contract requires “The Contractor and the Contractor’s processing environment containing Confidential State Data shall either (1) be in accordance with at least one of the following security standards: (i) International Standards Organization (“ISO”) 27001; (ii) Federal Risk and Authorization Management Program (“FedRAMP”); or (2) be subject to an annual engagement by a CPA firm in accordance with the standards of the American Institute of Certified Public Accountants (“AICPA”) for a System and Organization Controls for service organizations (“SOC”) Type II audit.” Does this apply if no Confidential State Data will be collected or stored by the Contractor? | Yes. This is a security requirement of the State because of the potential exposure to confidential State data. |
| Section 1.1 | 161. | How many of the eligible entities have completed the NCSR in the past? Will the contractor be able to access their previous entries | See State’s response to question #107. |
| Section 1.1.a | 162. | The NCSR assessment window is Oct 1 – Feb 28. Phase 1 of the contract is assessment and reporting and is noted as Year 1.   * With the inability to use the NCSR past Feb 28, what is the expected calendar timeline for Phase 1? * If past Feb 28 2023, what are the primary tasks/expectations of the contractor until the NCSR re-opens, since Advanced Recommendations are not until Phase 2? | See State’s response to question #6 and #97. |
| Section 3.1.2.2 | 163. | Proposal should include all costs for services “including any renewals or extensions.” The pricing sheet only allows for pricing through Year 5. How should the Contractor provide pricing for any extension beyond the optional renewals? | The awarded Contract will be only for a period of 5 years for which pricing is firm for that period. |
| Section 4.4.2 | 164. | Since engagement of subcontractors is at the discretion of the State, how should respondents address this requirement to specify exact scope and portions of work for the required subcontractors? | See State’s response to question #62. |
| Attachment 6.2, C.5 | 165. | States that an “example deliverable of a POAM and generic risk assessment report” must be submitted with proposal. Risk Assessment is not mentioned elsewhere in the RFP. Please describe the risk assessment requirements. | Risk assessment report has been deleted and replaced with “Enhanced Recommendation” |
| Attachment 6.4 | 166. | Will the State provide confirmation to the bidder that references have been received via email? | The respondent would need to send an email requesting this confirmation. |
| Sample Contract, A.6 & C.3.c | 167. | Contractor must have “a full-time dedicated project manager to the project.” (A6) Contractor will submit invoices when each entity’s NCSR assessment and POAM are complete. How is the requirement for the full-time project manager to be billed? | This will be built into the cost per the price lines. |
| Sample Contract, A.12.a | 168. | “Site visits could be required” for enhanced recommendations, but C.4 states that Contractor shall not be compensated or reimbursed for any travel expenses. If travel is truly required, then it should be an allowable expense. How are Contractors expected to price and/or cover these potential expenses? | These expenses must be built into the cost. |
| Section 1.1 | 169. | Contract to complete the NCSR process for approximately 1,332 county, city, K-12, and higher education Entities.  A) Please confirm if the contract will be assigned once over a period of 3 years for all 1400+ entities in scope to review and provide POAM or it will be a Master service agreement in which later individual entities-based work will be assigned to the selected vendors.  B)Can the NCSR assessments be done remotely or it will be mandatory to visit each entity? Please specify. As per our understanding , the NCSR assessments can be done remotely via Video/Emails/Questionaries etc.  C) Considering the scale of the program, please specify if the State is open to leverage vendor's Global delivery model by utilizing team from offshore locations or the resources assigned for the engagement has to be based in US region only. | 1. Contract will be assigned once to the winning respondent. The contract will cover the entirety of the work/deliverables. This will not be a MSA style agreement. 2. See State’s response to question #154 3. See State’s response to question #58 |
| Section 1.1 | 170. | A POAM template shall be developed in conjunction with STS such that it meets the needs of the Entities and is compatible with STS’ Governance Risk and Compliance (GRC) tool.  Please provide details of the GRC tool which is being used for STS. Also specify if different entities have different set of GRC tools or its being standardised across State of Tennessee for all the entities in scope. | See State’s response to question #14. |
| Section A.4 | 171. | The Contractor shall have on average 45 hours per entity to complete the NCSR and POAM process.  As per our understanding, 1400 entities have to be grouped into 3 parts to target it as high priority year1, Medium year 2 and low Year 3 with the assumptions of at least 500 entities coverage per year. Please confirm? | See State’s response to question #6 and #97. |
| Section A.12.iii | 172. | iii. The Contractor shall provide security system(s) design consulting services including but not limited to, networking, storage, intrusion detection/prevention systems, routers, switches, firewalls, logging, physical security systems, server, and workstation security configuration.  A) Based upon NCSR assessment, will the gaps be identified and remediation's recommendations will be provided across Network, Storage, Firewalls, Physical security systems etc (As a part of Baseline recommendations). However individual system /device level configurations recommendations will be out of scope and will be handled via additional services (On demand basis). Please specify?  B)As per our understanding, the scope of the engagement is consulting engagement to assess gaps and provide POAM recommendations only. Any implementation of recommendations/technology implementation/configurations will be out of scope for current engagement. Please confirm? | 1. Correct. 2. Correct. Remediation work is not part of this contract’s scope. |
| Mandatory Terms & Conditions – Section D.6 | 173. | Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract in a timely or proper manner, or if the Contractor materially violates any terms of this Contract (“Breach Condition”),the State shall have the right to immediately terminate the Contract and withhold payments in excess of compensation for completed services or provided goods  We propose for a cure period of 30 days in case of any default by Contractor to perform the services. | Pro Forma Section D.6 has been deleted and replaced with updated language that allows for a 30-day cure period. |
|  | 174. | Can the State please confirm the contract start date given the window in which NCSRs may be performed? | See State’s response to question #6 and #97.  Official contract start date to be determined based on completion of RFP process. |
|  | 175. | Can the State please confirm how it defines "complete the NCSR process?" | It is the process of registering a given entity with the NCSR application, completing the survey, and generating any reports thereafter. Creating POAMs based on this NCSR process is the vendor's primary value add in Phase 1. |
|  | 176. | Can the State please confirm if a trial run has been made to ensure that 45 hours is adequate time to gather data, complete the required fields in NCSR online tool, and develop POAM entries (w/an expected 35-40% non-compliant answer rate) for the five types of entities (Data Centers, Counties, Cities, K-12 schools, and post secondary schools) at the median, mean, and/or mathematical average size of each of those types of entities? | No trial has been conducted. 45 hours is an estimated average.  A pilot will be conducted as noted in Pro Forma section A.9. |
|  | 177. | Can the State please confirm if the State entities can be provided with the questionnaires ahead of time with a requirement to fill out their answers as a self-assessment prior to arrival (with documentation to demonstrate their level of maturity)? | The State will not have entities complete questionnaires ahead of contract award.  The methodology for distributing the NCSR questionnaires is not yet determined and is largely at the discretion of the vendor. Consistency and quality of the completed NCSR surveys and POAMs is what matters most. |
|  | 178. | Can the State please confirm if project-related meetings and exchanges of documents can occur virtually via Teams or Zoom where appropriate? | Confirmed. |
|  | 179. | Can the State please confirm the standard for "familiar with the requirements of the Privacy Rules" in D.20.a of the contract as it relates to HIPAA? | D.20 requires the Contractor to warrant that they are familiar with the requirements of the Privacy Rules and comply with all applicable requirements. |
|  | 180. | Can the State please confirm if there is a similar standard as D.20.a as it relates to Family Educational Rights and Privacy Act (FERPA)? | The State cannot confirm. |
|  | 181. | Can the State please confirm if there is a similar standard as D.20.a as it relates to California Privacy Rights Act (CPRA) or the predecessor CCPA? | The State cannot confirm. |
|  | 182. | Can the State please confirm if there is an expectation that those organizations that would have PII belonging to California residents (with the largest concentration probably in the post secondary institutions as part of the student recruiting and financial aid processes) have performed a Privacy Impact Assessment as it relates to PII/PHI and compliance standards that are unique to California residents? | The State cannot confirm. |
|  | 183. | Can the State please confirm the expected licensure requirements/certifications appropriate for the personnel involved to perform both Phase 1 and Phase 2 work? | That State does not require any specific licensure or certifications for this RFP.  Please refer to RFP Attachment 6.2 Section B.11. While not required, respondents are welcome to provide licensure and/or certification information if available. |
|  | 184. | Can the State please confirm if the required project management work falls within the $15M contract cost, or is it a separate billable expense? | The $15M budget includes project management work. It is the total budget for all scope/deliverables noted in the contract. |
|  | 185. | Can the State please confirm if the budget outlined is inclusive of assessing both endpoints and devices? | The $15M budget is for the entire contract.  Whatever is in scope based on NCSR questions. Endpoints (workstations and servers) surely, but network devices are a possibility. Mobile devices probably not. |
| Section 3.1.2.2 | 186. | Page 6, Section 3.1.2.2. states: The proposed cost shall incorporate ALL costs for services under the contract for the total contract period, including any renewals or extensions. Does this mean that our pricing needs to be good for five years and include any travel (Section C. 4.) as well? | Correct, all pricing will include travel for the contract, including renewals. |
|  | 187. | Do we need to meet a certain percentage of participation by business enterprises owned by minorities, women, service-disabled veterans, persons with disabilities and small business enterprises? | Although there is no requirement for this participation, the B.15 portion of the proposal will be evaluated and is included with other questions in the General Qualifications and Experience section with point value. The Dept. of Finance & Administration views diversity in their proposals as very important, with $102 million of their overall spend coming from diversity businesses during the last fiscal year. |
|  | 188. | Do we need to meet a certain percentage of participation by business enterprises owned by minorities, women, service-disabled veterans, persons with disabilities and small business enterprises? | Although there is no requirement for this participation, the B.15 portion of the proposal will be evaluated and is included with other questions in the General Qualifications and Experience section with point value. The Dept. of Finance & Administration views diversity in their proposals as very important, with $102 million of their overall spend coming from diversity businesses during the last fiscal year. |
| RFP Attachment 6.2, Section B Item Ref. B.15 (c) | 189. | Estimated Participation: Is participation (as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics) by business enterprises owned by minorities, women, service-disabled veterans, etc. a requirement or encouraged? Is this part of the evaluation criteria and how will this be scored? | Although there is no requirement for this participation, the B.15 portion of the proposal will be evaluated and is included with other questions in the General Qualifications and Experience section with point value. The Dept. of Finance & Administration views diversity in their proposals as very important, with $102 million of their overall spend coming from diversity businesses during the last fiscal year. |
|  | 190. | It is our understanding that the majority of the Nationwide Cybersecurity Review (NCSR) assessments with State of TN entities will be done remotely, and that it is possible some on-site visits/evaluation may be needed to provide the State the best Enhanced Recommendations. Is our understanding correct? | That is correct. We assume most will be performed remotely, however it is possible an on site visit would be necessary. |
|  | 191. | Due to the short NCSR window for completing the assessments, will you please clarify if ‘Year One’ ends February 28th, 2023, or when it is intended to end? | See State’s response to question #6. |
|  | 192. | We understood the part about not hiring illegal immigrants. Our organization has teammates who reside in multiple jurisdictions. Is it possible for us to leverage our employees and partners from other countries or do all assessors need to be US residents? | All employees and partners must be located in the United States. |
|  | 193. | The Center for Internet security NCSR website asks that all participants be employees of states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments. We’d like to get started as soon as possible preparing materials to ensure the work can be done consistently in the timeframe allotted. What does the State of TN envision will be the timing of our onboarding to the NCSR portal? | See State’s response to question #6.  The onboarding to the NCSR portal will be an ongoing effort as each entity currently is required to have their own accounts as well as an MoU with the entity, the State, and Vendor to allow access to that data. A standard MoU template will be provided once work is expected to begin. |

1. **Delete RFP # 31701-03385, in its entirety, and replace it with RFP # 31701-03385, Release # 2, attached to this amendment.** Revisions of the original RFP document are emphasized within the new release. Any sentence or paragraph containing revised or new text is highlighted.

**4. RFP Amendment Effective Date.** The revisions set forth herein shall be effective upon release. All other terms and conditions of this RFP not expressly amended herein shall remain in full force and effect.