



**REQUEST FOR PROPOSALS # 31701-03150
AMENDMENT # 4
FOR INFORMATION SECURITY ASSESSMENT AND
CONSULTING SERVICES (ISACS)**

DATE: August 12, 2016

RFP # 31701-03150 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		June 17, 2016
2. Disability Accommodation Request Deadline	2:00 p.m.	June 22, 2016
3. Notice of Intent to Respond Deadline	2:00 p.m.	June 23, 2016
4. Written "Questions & Comments" Deadline	2:00 p.m.	July 1, 2016
5. State Response to Written "Questions & Comments"		August 12, 2016
6. Response Deadline	2:00 p.m.	August 24, 2016
7. State Completion of Technical Response Evaluations		September 13, 2016
8. State Opening & Scoring of Cost Proposals	2:00 p.m.	September 14, 2016
9. State Notice of Intent to Award Released	2:00 p.m.	September 19, 2016
10. RFP Files Opened for Public Inspection	10:00 a.m.	September 20, 2016
11. End of Open File Period		September 27, 2016
12. State sends contract to Contractor for signature		September 28, 2016
13. Contractor Signature Deadline	2:00 p.m.	October 5, 2016

INFORMATIONAL NOTE: Please note that this RFP is seeking only one Contractor to provide information security assessment and consulting services. This contract will be for multiple years and is not for a single SOW for a single assessment.

2. 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.

Item #	Question/Comment	State Response
	<p>Note: In the questions that follow, any vendor's restatement of the text of the Request for Proposals (RFP) is for reference purposes only and shall not be construed to change the original RFP wording.</p>	
1.	<p>Will this RFP be awarded to 1 or multiple contractors?</p>	<p>The State's intent is to award only one contract to one prime contractor who may subcontract if necessary.</p> <p>According to Contract Section A.1., "The Contractor shall provide <u>all</u> goods or services and deliverables as required, described, and detailed below and shall meet <u>all</u> service and delivery timelines as specified by this Contract." [emphasis added]</p>
2.	<p>Does the State plan to award contracts to more than one vendor/contractor as a result of this RFP or to just one contractor?</p>	<p>Please see the State's Response to Question #1.</p>
3.	<p>Reference section 3.2.2.1 and 3.2.2.2, these sections request digital copies be submitted on "standard CD-R recordable disc or USB flash drive". Would it be acceptable to submit digital copies on standard DVD recordable disc instead of CD-R?</p>	<p>Yes, a standard DVD recordable disc is an acceptable digital format.</p>
4.	<p>Reference RFP Attachment 6.2, if we intend to use a subcontractor, must our responses for items in Attachment 6.2 that refer to "Respondent" and "Respondent employees" also include information for our subcontractor? For example, items A.3, A.4, and A.5 request bank reference, credit reference, and credit bureau report; so would only the prime contractor need to provide these items or BOTH the prime and subcontractor?</p>	<p>In reference to RFP Attachment 6.2, Section A - Mandatory Requirement Items, Items A.3, A.4, and A.5, the State is requiring the prime contractor's information only.</p> <p>According to RFP Section 4.4.5., "Notwithstanding any State approval relating to subcontracts, the Respondent who is awarded a contract pursuant to the RFP will be the prime contractor and will be responsible for all work under the Contract."</p>
5.	<p>Reference RFP Attachment 6.2, Section A (page 17), can the State confirm that the first 6 rows (without item numbers) do not require the respondent to enter any information in our response or reference a page number in our response?</p>	<p>Yes, the first six (6) unnumbered rows of Attachment 6.2, Section A - Mandatory Requirement Items, are for State use only. The Respondent is not required to enter any information in these rows.</p>
6.	<p>Reference RFP Attachment 6.2, Section B, items B.12 and B.13. These items refer to "key people". How does the State define "key people" for the purposes of this RFP? Is this intended to be all staff that would provide services or just personnel that would serve in leadership and/or management positions for</p>	<p>For purposes of this RFP, "key people" are defined as those known persons directly fulfilling the obligations of the contract at the time the Respondent is providing a response to the solicitation.</p> <p>Also, see the State's Response to Question #7.</p>

Item #	Question/Comment	State Response
	providing the requested services?	
7.	Reference RFP Attachment 6.2, Section B, item B.13. This item asks for response to include “the estimated number of hours that each individual will devote” to performance of the RFP requirements. Given that the number of hours and specific State needs and timing of work to be performed will be based specific agency requests to STS and on the resulting specifics of the actual statement(s) of work (which are unknown at this time), we do not have enough information to provide a reasonable estimate of hours for each staff person. How would the State like for us to respond to this item under these circumstances? Would providing an estimated percentage of time each staff member would or could be available to support these requirements be a reasonable approach to meet the State’s needs?	Since hourly requirements will vary and will be determined based on each project’s Work Breakdown Structure (WBS), the State does not have a preference with regard to how the Respondent describes this commitment. The State will accept numbers of hours, percentages, full time equivalent (FTE), or other reasonable descriptions and timeframes.
8.	Reference RFP Attachment 6.2, Section B, item B.15. When this item refers to “business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises”, does this mean only those types of entities that have been recognized and/or certified by Tennessee as minority, women, and small business enterprises, or would this include businesses recognized in these categories by other states and/or the federal government?	Yes, only those types of entities that have been certified by the State of Tennessee as Minority, Women, Service Disabled Veterans and Small business enterprises, would be recognized. Firms that are certified by other entities must be referred for certification here in the State of Tennessee.
9.	Reference RFP Attachment 6.2, Section B, item B.17. If we plan to include a subcontractor in our response, are we the only ones (as the prime contractor) required to provide references?	Yes, the references provided in response to Item B.17 should be for the prime contractor only.
10.	Does the State have an existing contract for the services requested in this RFP (ie: is this RFP a rebid of an existing contract)? If the State does have an existing contract, who in the incumbent?	See the State’s Response to Question #47.
11.	For RFP # 31701-03150, [Vendor Name Redacted] asks that if the State will ONLY accept respondents qualified in all domains below? i.e. will the State accept responses for only certain services? Services include from RFP Section 1.1.1: <ul style="list-style-type: none"> • vulnerability/compliance assessments • risk assessments • penetration tests • source code reviews • information security program assessment services 	As stated in Contract Section A.1., “The Contractor shall provide <u>all</u> goods or services and deliverables as required, described, and detailed below and shall meet <u>all</u> service and delivery timelines as specified by this Contract.” [emphasis added] However, as provided in RFP Section 4.4.2, subcontractors can be used by the prime contractor. Also, see the State’s Response to Question #4.

Item #	Question/Comment	State Response
	<ul style="list-style-type: none"> • system design services • data loss prevention services • limited data and network forensics services 	
12.	<ol style="list-style-type: none"> 1. External pen test: How many external targets are there total? I.e. email, webservers, ftp, etc. 2. Internal: How many total servers, virtual and physical? 3. How many total WS? 4. Wireless? 5. Centralized? 6. How many locations total? 7. Mostly active directory? 	<p>This contract is for multiple projects spanning the course of 5 years. Each engagement will hold a different number of targets and environments but will be agreed upon by both parties in each engagement's SOW.</p> <ol style="list-style-type: none"> 1. Varies from assessment to assessment. Single targets to thousands. 2. Varies from assessment to assessment. Single targets to thousands. 3. Varies from assessment to assessment. Single targets to thousands. 4. Yes. 5. Yes. 6. Could involve all State departments (up to 54 currently). 7. Not necessarily.
13.	<p>Questions for app pen testing, need this for each application:</p> <ol style="list-style-type: none"> 1. What is the purpose of the application? 2. Is the app internal or external? 3. What languages is it written in? i.e. .php, .asp., java etc. 4. Is it developed in house or externally? 5. What language is the back end database? 6. Approximately how many directories are involved? 7. How many roles are in the app? Admin, power user, end user, etc. 	<p>This contract is for multiple projects spanning the course of 5 years and the specifics being requested for app pen testing varies from assessment to assessment and will be outlined in the SOW. Further, each engagement will apply to a different application and can be written in any language including, but not limited to, C#, VB.NET, J2EE, PHP, Python, and ASP.</p>
14.	<p>RFP Part & Section Reference 1.1.2, RFP Page 1: In regard to services provided to "Non-State Participants," are any entities located outside the state of Tennessee?</p>	<p>No, there are no Non-State Participants outside the State of Tennessee.</p>
15.	<p>RFP Part & Section Reference Attachment 6.2, Section C, Sub Section C.1 - C.3, RFP</p>	<p>The State agrees there is not an overall contract project schedule because the schedule will be determined by each SOW and when that SOW is</p>

Item #	Question/Comment	State Response
	<p>Page 23:</p> <p>In regard to providing a narrative that demonstrates an understanding of the State's project schedule, there is no specific reference included within the RFP. Is there a specific set of milestones that the State is expecting respondents to follow?</p>	<p>issued.</p> <p>With that in mind, the State has revised/replaced Technical Approach Items C.1, C.2, and C.3. of RFP Attachment 6.2, Technical Proposal & Evaluation Guide - Section C with the following as Item C.1:</p> <p>Provide a narrative that describes how the Proposer would respond to varying staffing levels. For example, the State may not require any Contractor personnel for several weeks, and then have an immediate need for several Security Assessment Contractor personnel. Describe, in some detail, how the Proposer would meet this staffing need. Limit your response to 1,000 words or less.</p> <p>See RFP Release 2 in Item #3 below.</p>
16.	<p>RFP Part & Section Reference Section A.9, Sub Section A.9.a, RFP Page 37:</p> <p>Are there time-window constraints or location constraints from where the penetration testing can be conducted?</p>	<p>Yes. The testing windows and locations will vary from project to project; can be on-site or off site, Internet or VPN to the state's network. All tests must be performed within the US.</p>
17.	<p>2 -RFP Schedule of Events:</p> <p>The State's response to written questions and comments is scheduled for July 18th with little over a week for respondents to fully assess the State's answers and revise their responses accordingly. We ask that the State consider granting a two-week extension for the response deadline so vendors have enough time to deliver the best possible proposals.</p>	<p>See previous RFP Amendments #1 and #2 which extended the Response Deadline.</p>
18.	<p>Scope-A.9:</p> <p>1] Will we be conducting a Network and/or Application vulnerability scan? Penetration Test?</p> <p>2] • Penetration Test: Please validate that potential vulnerabilities are exploitable</p> <ul style="list-style-type: none"> o Network o Web Application o Wireless o Physical o Social Engineering o Data Exfiltration 	<p>This contract is for multiple projects spanning the course of 5 years. There will be multiple, separate engagements set up via SOW.</p> <p>In response to 1] – 9], the answer is yes.</p> <p>10] The State cannot provide a definitive answer as it depends on the rules of engagement per project.</p>

Item #	Question/Comment	State Response
	<p>3] Is the vulnerability scan required for a specific compliance requirement?</p> <p>4] Will the vulnerability scan be conducted on Externally or Internally facing systems (or both)?</p> <p>5] Will we be conducting a vulnerability scan using credentials? Note: If credentials are required then we will gather that information from you in a secure manner.</p> <p>6] Does the targeted environment(s) include intrusion detection or other security monitoring mechanisms that could trigger excessive alerts during vulnerability scanning? If so, are these security mechanisms network or host-based?</p> <p>7] Is the penetration test required for a specific compliance requirement?</p> <p>8] Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?</p> <p>9] Does the State want credentialed escalations performed? (Provides credentials and asks us to elevate privilege.)</p> <p>10] In the case that a system is penetrated, how should the testing team proceed?</p> <ol style="list-style-type: none"> 1. Perform a local vulnerability assessment on the compromised machine? 2. Attempt to gain the highest privileges (root on UNIX machines, SYSTEM or Administrator on Windows machines) on the compromised machine? 3. Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc./shadow on UNIX machines)? 	
19.	<p>A.9 - Web Application Penetration Test:</p> <p>1] How many web applications are being assessed?</p> <p>2] How many login systems are being assessed?</p> <p>3] How many static pages are being</p>	<p>This contract is for multiple projects spanning the course of 5 years. Each application to be assessed will have further information provided in the SOW.</p> <p>In response to 1] – 4], the State cannot provide a specific number as it varies from assessment to assessment.</p> <p>5] Yes, but only if a code review is requested.</p>

Item #	Question/Comment	State Response
	<p>assessed? (approximate)</p> <p>4] How many dynamic pages are being assessed? (approximate)</p> <p>5] Will the source code be made readily available?</p> <p>6] Will there be any kind of documentation? 1. If yes, what kind of documentation?</p> <p>7] Will static analysis be performed on this application?</p> <p>8] Does the State want fuzzing performed against this application?</p> <p>9] Does the State want role-based testing performed against this application?</p> <p>10] Does the State want credentialed scans of web applications performed?</p>	<p>6] User guides are sometimes supplied to help the tester explore the application. Often there is no documentation.</p> <p>In response to 7] – 10], the requirement varies from assessment to assessment.</p>
20.	<p>A.9 - Wireless Network Penetration Test:</p> <p>1] How many wireless networks are in place?</p> <p>2] Is a guest wireless network used? If so:</p> <p>1. Does the guest network require authentication?</p> <p>2. [Question missing from vendor submission.]</p> <p>3. What is the square footage of coverage?</p> <p>4. Will enumeration of rogue devices be necessary?</p> <p>5. Will the team be assessing wireless attacks against clients?</p> <p>6. Approximately how many clients will be using the wireless network?</p>	<p>This contract is for multiple projects spanning the course of 5 years. The number of wireless networks in place needing assessment will vary from engagement to engagement and will be agreed upon in the SOW.</p>
21.	<p>A.9 - Physical Penetration Test:</p> <p>1] How many locations are being assessed?</p> <p>Is this physical location a shared facility? If so:</p> <p>1. How many floors are in scope?</p>	<p>This contract is for multiple projects spanning the course of 5 years and the information requested for physical penetration testing of locations, security guards, cameras, and alarm systems, etc., varies from assessment to assessment and will be outlined in the SOW.</p>

Item #	Question/Comment	State Response
	<p>2. Which floors are in scope?</p> <p>2] Are there any security guards that will need to be bypassed? If so:</p> <p>1. Are the security guards employed through a 3rd party?</p> <p>2. Are they armed?</p> <p>3. Are they allowed to use force?</p> <p>3] Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?</p> <p>4] Are all physical security measures documented?</p> <p>5] Are video cameras being used?</p> <p>6] Are the cameras client-owned? If so:</p> <p>1. Should the team attempt to gain access to where the video camera data is stored?</p> <p>7] Is there an armed alarm system being used? If so:</p> <p>1. Is the alarm a silent alarm?</p> <p>2. Is the alarm triggered by motion?</p> <p>3. Is the alarm triggered by opening of doors and windows?</p>	
22.	<p>General Qualifications - B.17 – References: Are commercial account references acceptable?</p>	<p>Yes, commercial account references are acceptable as long as they use the required RFP Attachment 6.4, Reference Questionnaire.</p>
23.	<p>Scope- e. Objective 5: Provide Data Loss Prevention (DLP) Assessment:</p> <p>1] What are you currently using to identify possible data loss?</p> <p>2] How are you currently protecting personal confidential information of state employees?</p> <p>3] How are you currently protecting state</p>	<p>The information you have requested is sensitive and is not required at this time to submit a detailed proposal. The State will provide this information to the awarded vendor upon contract approval and after a non-disclosure agreement (NDA) is in place.</p>

Item #	Question/Comment	State Response
	<p>financial data?</p> <p>4] How do you or can you mitigate data loss events when they are identified?</p> <p>5] Can your current solution identify data loss on the web channel both http and https?</p> <p>6] Can your current solution identify email channels smtp?</p> <p>7] Can your current solution manage data loss for web, data and email on one user interface?</p> <p>8] Does the DLP solution need to provide an executive dashboard review?</p>	
24.	<p>Scope - Objective 6: Security System Design and Configuration Consultation:</p> <p>1] Are there any documented architectural standards that must be followed?</p> <p>2] Is there existing documentation including diagrams that can be referenced?</p> <p>3] Are there any regulatory requirements that need to be followed by the architect?</p> <p>4] Are there any other vendors with whom we must coordinate?</p>	<p>1] – 3] This contract is for multiple projects spanning the course of 5 years. Depending upon the nature of the requested assessment there may be adequate design documentation, diagrams, vendor information, and architectural standards which will be delivered in the SOW.</p> <p>4] Upon being called in for system design, we would look to the vendor for expert architectural standards advice.</p>
25.	<p>Section C - C.7 Technical Qualifications, Experience & Approach Items:</p> <p>1] Please provide a complete and comprehensive overview of the risk assessment and incident handling architecture and procedures currently in place so that we can try to gain better understanding of the needed risk assessment requirements and let us properly value the cost of services.</p> <p>2] Any Governance or Compliance necessary (i.e. PCI/DSS)?</p>	<p>1] We look to the vendor for recommendations on risk assessments.</p> <p>2] This varies from assessment to assessment. Across the State there are many types of data in different types of environments that will fall under certain compliance standards including, but not limited to, PCI, HIPAA, CJIS, FISMA, and FERPA. Each SOW will detail the compliance needs of the individual engagement.</p>
26.	<p>Deliverables: - III. Post-Engagement Questions and Answers Period:</p> <p>Is the State looking at selected vendor to perform the recommended remediation?</p>	<p>No, State personnel will be responsible for performing the remediation. However, the vendor will be required to provide guidance on HOW to perform the remediation.</p>
27.	<p>Social Engineering:</p>	<p>For the State's purposes, social engineering falls</p>

Item #	Question/Comment	State Response
	<p>1] Is the State interested in social engineering? If so:</p> <p>a] Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?</p> <p>b] Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?</p> <p>c] Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so:</p> <p>1. How many people will be targeted?</p>	<p>under general assessment services and is often required. The number of people targeted will vary from engagement to engagement but will be outlined in the SOW.</p>
28.	<p>Data Exfiltration: Without attempting to subvert DLP technologies, attempt to infiltrate target data so DLP technology effectiveness can be measured.</p> <p><u>Questions for Business Unit Managers:</u></p> <p>1] Will the manager be aware that a test is about to be performed?</p> <p>2] What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?</p> <p>3] Are testing and validation procedures to verify that business applications are functioning properly in place?</p> <p>4] Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?</p> <p>5] Are Disaster Recovery Procedures in place for the application data?</p> <p><u>Questions for Systems Administrators:</u></p> <p>6] Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)</p>	<p>This contract is for multiple projects spanning the course of 5 years. The answer to all of these questions will depend upon the nature of the individual engagement agreed upon by the SOW. The rules of engagement will vary from one SOW to the next.</p>

Item #	Question/Comment	State Response
	<p>7] Are there systems on the network which the client does not own, that may require additional approval to test?</p> <p>8] Are Change Management procedures in place?</p> <p>9] What is the mean time to repair systems outages?</p> <p>10] Is any system monitoring software in place?</p> <p>11] What are the most critical servers and applications?</p> <p>12] Are backups tested on a regular basis</p> <p>When was the last time the backups were restored?</p>	
29.	<p>Budget:</p> <p>What is the expected budget for this contract?</p>	<p>As this is a contract for consulting services used only when needed, the State does not have an expected budget. However, see the State's Response to Question #56 for the fiscal years spend on the current contract.</p>
30.	<p>Overall - You are looking for a breakdown of fees for each objective for each year by role. Do you have a risk assessment to drive which services are performed annually, or have a preference on execution schedule. Is the anticipation each one will be performed each year?</p>	<p>The State is only looking for hourly rates by role and not a specific annual risk assessment schedule.</p>
31.	<p>Objective 1 –</p> <p>1. How many externally accessible services will be included in the assessment?</p> <p>a. How many of these services are web servers? How many web pages are present on the web servers?</p> <p>2. Approximately how many internal servers will be tested as part of the assessment? How many workstations?</p> <p>3. Will wireless penetration testing be included as part of the assessment?</p> <p>a. If so, how many wireless SSIDs are included.</p>	<p>This contract is for multiple projects spanning the course of 5 years. The number of services, servers, networks, and applications needing assessment will vary from engagement to engagement and will be agreed upon at the time of the SOW. This also includes the rules of engagement such as those requesting social engineering.</p>

Item #	Question/Comment	State Response
	<p>4. Will application testing be conducted from both an authenticated and unauthenticated perspective?</p> <p>a. If authenticated testing is included, how many applications will be tested?</p> <p>5. Will social engineering / phishing attacks be included in the assessment?</p>	
32.	<p>Objective 2 –</p> <p>1. Can you provide details on the code to be review, including:</p> <p>a. Brief description of the applications</p> <p>b. Number of lines of code</p> <p>c. Development languages</p>	<p>This contract is for multiple projects spanning the course of 5 years. Each engagement will apply to a different application and can be written in any language including, but not limited to, C#, VB.NET, J2EE, PHP, Python, and ASP.</p>
33.	<p>Objective 3 –</p> <p>1. The structure of Objective 3 appears to provide forensic support in the event of an incident. Is this accurate?</p> <p>a. If so, are you looking for a rate card to support activities in the event of an incident?</p>	<p>Yes, to both questions.</p>
34.	<p>Objective 4 –</p> <p>1. Can you please provide context around the number of departments and systems impacted PCI-DSS, HIPAA (storing or processing PHI), and FERPA (storing or processing student information)?</p> <p>2. You reference NIST in this section. Do you mean NIST Cybersecurity, 800-53, or any other NIST standards?</p> <p>3. Are you looking for an assessment that addresses each individual requirement in the standards listed, or a single assessment that broadly addresses each the components of each standard.</p>	<p>1] This contract is for multiple projects spanning the course of 5 years. Each department, agency, or entity will have differing requirements of standards including, but not limited to, FISMA, FERPA, PCI, CJIS, and HIPAA.</p> <p>2] Some entities may require them be compliant with sections of the NIST including, but not limited to, 800-53 and 800-88.</p> <p>3] The breadth and depth of a standards assessment will be different depending upon each engagement and will be agreed upon in the SOW.</p>
35.	<p>Objective 5 –</p> <p>1. Do you have a DLP solution in place currently? If so, what solution are you using?</p>	<p>For security reasons we cannot answer this question without an NDA in place. For the sake of this RFP assume no DLP in place; looking for guidance and expertise.</p>
36.	<p>Objective 6 –</p>	<p>For security reasons we cannot answer this question</p>

Item #	Question/Comment	State Response
	1. Can you provide some background on the technologies in use to support network architecture?	without an NDA in place. Assume robust, industry standard technology in use.
37.	Does the State consider assessments of SIEM configurations to be part of the scope of this contract (Pro Forma Contract A.9, p. 37)?	Yes, SIEM configurations are part of the Scope of Services, pro forma Contract Section A.9.f, <u>Objective 6: Security System Design and Configuration Consultation</u> .
38.	What is the minimum number of resumes required for item B.13 (p.20)?	B.13 requests the Respondent to provide “a resume for each of the people listed.” [emphasis added] The number of resumes provided will be determined by the number of people listed in the personnel roster provided by the Respondent.
39.	Can experience be used as a substitute for the listed certifications for the Security Program Assessor (Pro Forma Contract, A.2.b.ii)?	No, pro forma Contract Section A.2.b.ii requires experience and certification. However, the State has revised the pro forma contract section to provide clarification that all three certifications are not required. See RFP Release 2 in Item #3 below.
40.	Will this be a single award or an award to multiple vendors (as was the case for RFP32110-15100)?	See the State’s Response to Question #1.
41.	Will the rates of the winning vendor(s) be published on the State’s public facing website?	No, the winning vendor’s rates will not be published on the State’s website. However, in accordance with RFP Sections 4.8.3 and 5.3.3, a Respondent’s responses and associated materials are open for public review.
42.	Page 37, Section A.6 of the Pro Forma Contract: Does the contractor have the freedom to choose which penetration testing/vulnerability assessment tools are to be used or will the state specify the tools?	The vendor can choose but all findings must be compatible with the State’s Governance Risk and Compliance (GRC) tool. See RFP Attachment 6.7, Assessment Export File Specification, for details on the format.
43.	In Attachment 6.2, Section C, items 1, 2 and 3, the RFP asks to provide narrative that illustrates understanding of project timelines and project schedules. Could the state provide that breakdown?	No. This contract is for multiple projects spanning the course of 5 years. Each engagement will have different timelines and project schedules agreed upon in that engagement’s SOW. See the State’s Response to Question #15.
44.	If the state cannot provide the breakdown of projects and desired schedules, would the state accept a description of how we establish project schedules, resourcing and timeframes for Attachment 6.2, Section C, items 1, 2 and 3?	See the State’s Response to Question #15.
45.	Attachment 6.2, Section C, items 1, 2, and 3, the RFP asks to provide narrative describing how our firm would complete the scope of services and meet the State’s project schedule. [Vendor Name Redacted] allocates resources based on the size of each project and derive timelines based on that information. We are assuming the state will	See the State’s Response to Question #15.

Item #	Question/Comment	State Response
	<p>be executing a number of projects of various scope based on the requests in that section. Accordingly, we would like to request the following scope information:</p> <ul style="list-style-type: none"> a. Number of compliance assessments and which regulations / standards the assessments should be performed to. b. Number of systems to be assessed for vulnerabilities. c. Number of individual vulnerability assessments projects. d. Number of systems in scope for penetration testing. e. Number of individual penetration testing projects. f. Number of applications to undergo code review. g. Approximate number of lines of code for each application to be reviewed. h. [NEED SCOPE INFO FOR C.11 RE: INFOSEC PROGRAM ASSESSMENT] 	
46.	Our firm does not provide system design, data loss prevention services, or data classification and discovery services. Without bidding those items, would our bid still be considered responsive?	The State cannot make a preliminary determination of whether a Response is responsive or not without a review process. However, please see the State's Response to Questions #1 and #11.
47.	With whom did the State of Tennessee previously contract to perform these services? Why are you choosing to rotate QSA's?	The State currently has a contract with a vendor to provide information security assessment and consulting services; however, there are security concerns surrounding the general disclosure of vendor names. The State does not believe this information is necessary to provide a Response. It is unclear to the State what the vendor means by "QSA's." Nevertheless, the contract is a five year contract that expires on September 10, 2016.
48.	Are we required to bid on all services and all levels of experience, or can we pick and choose the services we want to bid?	Please see the State's Response to Questions #1 and #11.
49.	Will we be penalized if we do not currently have employees in all four of the varying levels of experience for all of the classifications, and/or choose to use subcontractors to fill the gaps?	No, please see the State's Response to Questions #1 and #11.
50.	Will the contract be awarded to multiple	Please see the State's Response to Question #1.

Item #	Question/Comment	State Response
	vendors or a single vendor?	
51.	<p>RFP Section 2, schedule of events - Response Deadline July 28, 2016</p> <p>Due to the extensive requirements defined in the RFP and in order to ensure we can provide you the most competitive price possible, will the State consider an extension to the response deadline? A one month extension could result in more complete responses.</p>	See the State's Response to Question #17.
52.	<p>RFP Section 3.3.1</p> <p>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.</p> <p>Will the State consider red-lines to the pro forma contract as part of the RFP response? Red-lines to the pro forma have been allowed in other RFPs such as the Department of Correction, RFP# 32901-14103 for an Offender Management Solution.</p>	<p>As each contract is stand alone, the State cannot address why red-lines were allowed in a separate procurement.</p> <p>No, the Respondents must <u>not</u> propose modifications to the <i>pro forma</i> contract at the time of proposal submission. Please see the State's Response to Question #53.</p>
53.	<p>RFP Section 3.3.1</p> <p>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.</p> <p>Will the State consider the addition of terms to the pro forma contract if they do not conflict with the State's terms?</p>	<p>No, the Respondents must <u>not</u> propose modifications to the <i>pro forma</i> contract at the time of proposal submission. Clarifications and exceptions will be discussed during limited negotiations with the apparent best-evaluated Respondent subject to any mandates or restrictions imposed on the State by applicable state and federal law. The State reserves the right to unilaterally reject all suggested changes to the <i>pro forma</i> contract and responses to the solicitation must be based on the assumption that only the <i>pro forma</i> contract language will be used in the execution and performance of the contract. Responses conditioned upon acceptance of the Respondents' suggested changes to the <i>pro forma</i> contract terms may be deemed as non-responsive to the solicitation and will not be evaluated or considered for award.</p> <p>Further, the Respondent shall not leave the Statement of Certifications and Assurances, RFP Attachment 6.1, unsigned or include any clarifications, exceptions, or qualifications.</p> <p>Please note that the State has amended RFP Attachment 6.1, item 3, to indicate the position stated above.</p>

Item #	Question/Comment	State Response
		See RFP Release 2 in Item #3 below.
54.	<p>RFP section 4.4. Assignment & Subcontracting 4.4.1.</p> <p>The Contractor may not subcontract, transfer, or assign any portion of the Contract awarded as a result of this RFP without prior approval of the State. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment.</p> <p>Is the Contractor able to add subcontractors after the award of the contract?</p>	<p>Yes, the Contractor can add subcontractors but will be subject to the State's approval pursuant to Contract Section D.7, <u>Assignment and Subcontracting</u>.</p> <p>The Contractor shall notify the State contact identified in Contract Section D.2, <u>Communications and Contacts</u>, of any changes in the use of subcontractors.</p>
55.	<p>RFP section 4.5</p> <p>The State reserves the right to refuse, at its sole discretion and notwithstanding any prior approval, any personnel of the prime contractor or a subcontractor providing goods or services in the performance of a contract resulting from this RFP. The State will document in writing the reason(s) for any rejection of personnel.</p> <p>1] Will the State consider adding language granting the Contractor a reasonable amount of time to replace a particular person that is not acceptable?</p> <p>Will the State confirm that any such request shall be for lawful reasons?</p> <p>2] If a contractor has a consultant on site for several weeks and is not aware of an issue the expense could be sizeable. The risk associated with this section written as it is will have a dramatic impact on price.</p> <p>Will the State confirm that its reasons for any rejection must be lawful?</p>	<p>1] See the State's Response to Question #62, Item 1].</p> <p>2] In the event of an issue, the State will notify the Contractor within a reasonable time.</p>
56.	<p>RFP attachment 6.3 Cost Proposal</p> <p>Will the State please provide total spend on the contract for the past 3 years broken down by year so we can understand the total estimated spend? By providing the total spend over the past 3 years, we can ensure we provide you the most competitive price possible.</p>	<p>Broken down by Fiscal Year (FY); July 1 – June 30</p> <p>FY2013 – \$155,676.82</p> <p>FY2014 – \$419,559.09</p> <p>FY2015 – \$233,860.29</p> <p>FY2016 – \$101,231.30</p>
57.	<p>RFP attachment 6.3 Cost Proposal</p> <p>Will the State please provide the total hours</p>	<p>The information requested by the vendor is not available. The State used a relational weighting methodology which is a representation of the</p>

Item #	Question/Comment	State Response
	<p>billed on a month by month basis for all of the titles listed in the cost proposal for the last year, or preferably the past 3 years? By providing this data, we can ensure we understand the amount of work performed on this contract, and its peaks, so we can ensure we are staffed appropriately to meet your needs in a timely manner.</p>	<p>estimated relative weights of each job classification compared to the other job classifications.</p> <p>In other words, the classifications that were used the most were assigned a higher evaluation factor versus those that were used least.</p>
58.	<p>Pro forma contract, section A.2</p> <p>SOW development is performed by the Contractor based on requirements defined by STS, the agencies and/or Non-State Participants. In addition to the SOW, a Work Breakdown Structure (WBS) will be developed by the Contractor.</p> <p>Is it the State's intent that the Contractor bill STS for these services or will a bill be rendered directly to the city/county/local government, etc. for whom the assessment is performed?</p>	<p>There is no obligation or charge for the SOW and WBS preparation, that is "free estimates" are required. All services under SOWs are billed to STS.</p>
59.	<p>Pro forma contract, section A.4 "A. Contractor consultants may be based on-site and perform their work at State facilities, maintained and managed in Tennessee;</p> <p>b. Contractor consultants may be based off-site and perform their work at a Contractor location;</p> <p>Will the State define during the SOW process where the work must be performed from? In this manner, the contractor can understand if travel to the customer premises will be required.</p>	<p>Yes, the SOW will define the work location.</p>
60.	<p>Pro forma contract, sections C.3.c and C.4</p> <p>c. The Contractor shall not be compensated for travel time to the primary location of service provision.</p> <p>C.4. Travel Compensation. Compensation to the Contractor for travel, meals, or lodging shall be subject to amounts and limitations specified in the current "State Comprehensive Travel Regulations." The Contractor shall not be compensated or reimbursed for travel, meals, or lodging unless approved in advance by the State.</p> <p>C.3.c seems to conflict with C.4.</p>	<p>1] Contract Section C.3.c refers to the hourly rates paid to the Contractor. The State will not pay hourly rates, in addition to travel expenses, for the Contractor personnel to travel to the primary location of service.</p> <p>2] Yes, the SOW will define the primary location of service and if any travel will be involved. All travel must be pre-approved by the State.</p>

Item #	Question/Comment	State Response
	<p>1] Is travel specifically excluded only for travel time to the primary location of service?</p> <p>2] Will the SOW process specifically define where the Contractor may work from and if travel to/from that site is specifically included or excluded?</p>	
61.	<p>Pro forma contract Section C, payment terms and conditions</p> <p>We noticed in section C of the contract that there are no terms surrounding the State's payment of the invoice, such as net 30 from the invoice date. Would the State please clarify the invoice payment terms? If there are no terms, will the State pay the invoice the invoice in accordance with TCA 12-4-703?</p>	<p>The timeline for payment of invoices by the State will be paid in accordance with Contract Section C.5.c and T.C.A. 12-4-703, which are listed below:</p> <p>C.5.c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.</p> <p>12-4-703. When payment required. An agency which acquires property or services pursuant to a contract with a business shall pay for each complete delivered item of property or service in accordance with the provisions of the contract between the business and agency or, if no date or other provision for payment is specified by contract, within forty-five (45) days after receipt of the invoice covering the delivered items or services.</p>
62.	<p>Pro forma section A.11.A</p> <p>Section A. 11.A, The Contractor shall select the Consultants to perform the services requested in the SOW. The State shall be the sole judge of the quality of services provided and the project progress achieved by the Contractor's consultants. The Contractor agrees to remove and replace at the Contractor's expense, consultants whom the State judges to be incompetent, careless, unsuitable or otherwise objectionable, or whose continued use is deemed contrary to the best interests of the State or deemed not to make substantial contributions to the project. The Contractor agrees not to charge the State for services performed which the State designates as being unacceptable.</p> <p>1] Will the State consider adding language granting the Contractor a reasonable amount of time to replace a particular person that is not acceptable? Will the State confirm that any such request shall be for lawful reasons?</p> <p>2] If a contractor has a consultant on site for several weeks and is not aware of an issue the expense could be sizeable. The risk associated with this section written as</p>	<p>1] The State does not agree, at this time, to amend Section A.11.a. However, see the State's Response to Question #53.</p> <p>2] The State cannot agree to pay for unacceptable work; however, the State will not unreasonably designate work as being unacceptable. See the State's Response to Question #55.</p>

Item #	Question/Comment	State Response
	<p>it is will have a dramatic impact on price. Will the State confirm that its reasons for any rejection must be lawful?</p>	
63.	<p>Pro forma section D.7. Assignment and Subcontracting.</p> <p>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.</p> <p>Does the State agree that the Contractor has the right to elect to have its obligations under an Attachment performed by an Affiliate without prior written approval of the State, but shall retain responsibility for all such work?</p>	<p>It is unclear to the State what the vendor means by “Affiliate.” Nevertheless, the Contractor must obtain prior written approval before assigning services performed under this Contract to any third party. The language of <i>pro forma</i> contract D.7 remains as written.</p>
64.	<p>Pro Forma Contract, Section D20 D.20 HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Health Information Technology for Economic and Clinical Health (“HITECH”) Act and any other relevant laws and regulations regarding privacy (collectively the “Privacy Rules”). The obligations set forth in this Section shall survive the termination of this Contract.</p> <p>a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.</p> <p>b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.</p> <p>c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This</p>	<p>Section D.20 requires both the State and the Contractor to comply with all applicable HIPAA and HITECH rules and regulations.</p> <p>“Privacy Rules” is a defined term in the contract which is comprised of the HIPAA and HITECH Acts and any other relevant laws and regulations regarding privacy. The applicable Privacy Rules are dependent on the content of the specific requests submitted by the agencies.</p>

Item #	Question/Comment	State Response
	<p>provision shall not apply if information received or delivered by the parties under this Contract is NOT “protected health information” as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.</p> <p>d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.</p> <p>Please provide a link or otherwise clarify the meaning of and reference to "Privacy Rules"</p>	
65.	<p>Pro Forma Contract, Section D23</p> <p>D. 23 Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:</p> <p>a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;</p> <p>b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;</p> <p>c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and</p> <p>d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.</p> <p>The Contractor shall provide immediate written notice to the State if at any time it</p>	<p>1] The State does not agree to the suggested revision.</p> <p>2] “Future” in this case refers to planned use. The State is not asking for a prediction, but the Contractor will disclose any plans to hire someone who has been debarred, etc.</p>

Item #	Question/Comment	State Response
	<p>learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.</p> <p>1] Would the State entertain clarifications to Section D.23 in order to account for the size and scope of the business of a particular contractor? Specifically, a contractor may need to qualify the certification because the size of its business to the extent that the contractor is not familiar with operations unrelated to the services contemplated by the Contract.</p> <p>2] Also, how can a contractor certify as to "future principals" as required in Section D.23, since such principals are neither identified nor known at this time?</p>	
66.	<p>Pro Forma Contract, Section D24</p> <p>D. 24 Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in</p>	The State does not agree to the suggested revision.

Item #	Question/Comment	State Response
	<p>a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event</p> <p>Is the State willing to extend the timeframes beyond the one day and forty-eight (48) hour requirements set forth in D.24, "Force Majeure"?</p>	
67.	<p>Pro Forma Contract, Section D30</p> <p>D.30 Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:</p> <p>a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;</p> <p>b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes the Memoranda of Understanding (MOUs), their associated Statements of Work (SOWs) and Work Breakdown Structure (WBS);</p> <p>c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;</p> <p>d. the State solicitation, as may be amended, requesting responses in competition for this Contract;</p> <p>e. any technical specifications provided to</p>	<p>As stated in Question #53, the Respondent's proposal shall not contain any redlines or clarification or addenda.</p> <p>If the State seeks any clarification or addenda, those clarifications or addenda may be incorporated by reference.</p>

Item #	Question/Comment	State Response
	<p>proposers during the procurement process to award this Contract; and</p> <p>f. the Contractor's response seeking this Contract.</p> <p>What is the intent of Section D. 30(c)? Specifically, the Contractor would like confirmation that clarifications or modifications to this Contract that are included in Contractor's proposal and that are agreed to by the State shall be deemed to be incorporated into and part of the Contract.</p>	
68.	<p>Pro Forma Contract, Section D31 D. 31 Insurance. If bidder's insurance policies comply in all material respects with the requirements of Section D.31, would the State be willing to consider minor modifications to the language in D.31 to more accurately reflect actual language in contractor's coverage?</p>	<p>At this time, the State does not agree to modifications; however, see the State's Response to Question #53.</p>
69.	<p>Pro Forma Contract, p. 55, Section E2 E.2 Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law.</p> <p>The obligations set forth in this Section shall survive the termination of this Contract.</p> <p>Would the State agree to mark as "confidential" specific information that is to be treated as Confidential Information under this Contract? The standard that all information is to be deemed confidential if such information</p>	<p>See the State's Response to Question #53.</p>

Item #	Question/Comment	State Response
	"is regarded as confidential under state or federal law" is very broad and will be difficult to administer to the possible detriment of the State.	
70.	Pro forma section E.3 ownership of work product Ownership of work product. With respect to Section E.3 Ownership of Software and Work Products, would the State of Tennessee agree to an unrestricted license to the Work Product rather than all ownership rights in the Work Product? Contractor needs to retain ownership rights in the Work Product.	The State does not agree to the suggested revision.
71.	General Will all vendors be provided a copy of all submitted questions and associated responses?	Yes, all questions and comments received, and the State's Responses, will be published as an amendment on the same websites that the original RFP was posted. In addition, vendors who submitted an acceptable Notice of Intent to Respond will receive a direct email notification.
72.	C.4 Travel Compensation Will the State of TN please provide a copy of, or a link to, the "State Comprehensive Travel Regulations" document to which vendors expenses will be subject to?	Yes, the following is a link to the "State Comprehensive Travel Regulations" mentioned in Contract Section C.4. http://www.tn.gov/assets/entities/finance/attachments/policy8.pdf
73.	A.9.a Objective 1: Provide Security Vulnerability Assessment and Penetration Testing Services Are these tests external in nature (i.e. source of testing being a node on the Internet) or internal in nature (i.e. source of testing being a node on the internal State of TN agency network) or a mix of both?	Yes, the tests are external, internal, and a mixture of both.
74.	A.9.a Objective 1: Provide Security Vulnerability Assessment and Penetration Testing Services For internal testing, is there a limited number of locations from which this testing would occur? If so, please indicate the locations.	This contract is for multiple projects spanning the course of 5 years. Each engagement will determine the number of location that testing may occur from and will be agreed upon in the SOW.
75.	A.9.a Objective 1: Provide Security Vulnerability Assessment and Penetration Testing Services For vulnerability and penetration test, is this strictly network relegated testing or should the vendor expect other types of testing on a per-SOW basis; for example Wireless penetration testing, application testing, social engineering, etc.?	Each engagement will be different, so yes, all of the example types and possibly more will be requested and agreed upon in the SOW.
76.	A.9.a Objective 1: Provide Security Vulnerability Assessment and Penetration	It depends on requests coming from the agencies. In the current contract, we averaged 1 to 3

Item #	Question/Comment	State Response
	Testing Services How frequently are vulnerability or penetration test reviews requested?	assessments per month. We anticipate that this rate could slowly grow as it has been for the last several years.
77.	A.9.b Objection 2: Provide Code Review Services What software languages are expected to be in scope for review?	The software languages expected could be any modern or recently deprecated language. Languages used include, but are not limited to, C#, VB.NET, J2EE, PHP, Python, and ASP.
78.	A.9.b Objection 2: Provide Code Review Services How frequently are code reviews requested?	Varies from assessment to assessment. In the current contract, we averaged 1-3 code reviews per year.
79.	A.9.b Objection 2: Provide Code Review Services On average, how many lines of code are requested to be assessed in any given engagement?	Varies from assessment to assessment. It is possible to see applications with 100k lines of code or more.
80.	A.9.b Objection 2: Provide Code Review Services Can code review be performed off-site, or is there a requirement to test source code on customer premises?	The location requirement for code reviews varies from assessment to assessment. Previously most code review has been performed off site; however, this will be agreed upon in the SOW.
81.	A.9.c Objective 3: Provide Forensics Services Does the state have an understanding of the number of forensic engagements that it performs each year? If so, please provide that insight.	The number depends on the agency. The State as a whole has a variety of IDS installed; however, specific information will be provided for each engagement in the SOW.
82.	A.9.c Objective 3: Provide Forensics Services Is there a consistent set of tools for logging and detection of intrusion installed across all agencies in the State of TN or will native capabilities of vary between agencies investigated environments?	The tools for logging and detection of intrusion are varied and depend on the agency. The State as a whole has a variety of IDS installed; however, specific information will be provided for each engagement in the SOW.

3. Delete RFP # 31701-03150, in its entirety, and replace it with RFP # 31701-03150, 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.**

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.



STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION

REQUEST FOR PROPOSALS
FOR
INFORMATION SECURITY ASSESSMENT AND
CONSULTING SERVICES (ISACS)

RFP # 31701-03150

RELEASE 2

RFP CONTENTS

SECTIONS:

1. INTRODUCTION
2. RFP SCHEDULE OF EVENTS
3. RESPONSE REQUIREMENTS
4. GENERAL CONTRACTING INFORMATION & REQUIREMENTS
5. EVALUATION & CONTRACT AWARD

ATTACHMENTS:

- 6.1. Response Statement of Certifications & Assurances
- 6.2. Technical Response & Evaluation Guide
- 6.3. Cost Proposal & Scoring Guide
- 6.4. Reference Questionnaire
- 6.5. Score Summary Matrix
- 6.6. *Pro Forma* Contract
- 6.7. Assessment Export File Specification
- 6.8. Draft Memorandum of Understanding (MOU)
- 6.9. Draft Work Breakdown Structure (WBS)
- 6.10. Draft Statement of Work (SOW)

1. INTRODUCTION

The State of Tennessee, Department of Finance and Administration, hereinafter referred to as “the State,” has issued this Request for Proposals (RFP) to define minimum contract requirements; solicit responses; detail response requirements; and, outline the State’s process for evaluating responses and selecting a contractor to provide the needed goods or services.

Through this RFP, the State seeks to procure necessary goods or services at the most favorable, competitive prices and to give ALL qualified businesses, including those that are owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises, an opportunity to do business with the state as contractors, subcontractors or suppliers.

1.1. Statement of Procurement Purpose

- 1.1.1. The State intends to secure a contract for Information Security Assessment and Consulting Services (ISACS) Consultants to assist in strengthening the State’s security posture. Services include vulnerability/compliance assessments, risk assessments, penetration tests, source code reviews, information security program assessment services, system design services, data loss prevention services, and limited data and network forensics services. Vulnerability assessments and penetration testing services will be used to identify and validate configuration and/or technical flaws within a given system or network. System components include, but are not limited to, load-balancers, firewalls, routers, servers, workstations, operating systems, system software, applications, and databases. Application assessments including code review will be conducted to identify vulnerabilities and programming errors that may lead to security issues such as Cross Site Scripting (XSS) and Structured Query Language (SQL) Injection. Information security program assessment services will be used to determine the maturity and effectiveness of the State’s information security program. Applications will be evaluated against Open Web Application Security Project (OWASP) guidelines. Developer workshops will be conducted where findings are explained and remediation steps detailed with examples. System design services will be used to assist with the architecture and detailed design of complete systems such as networks and physical security. Data Loss Prevention (DLP) services will be used to assess the State’s or individual agency’s infrastructure, policies and procedures around the storage and handling of confidential data. This may include data discovery and data classification. Data and network forensics services will be limited to the “root cause” analysis of information security incidents within the State’s environment. Any other services not specifically mentioned above will be included in this contract as “general security consulting services.” See Contract Section A.2.b.vii.
- 1.1.2. At the State’s request and under the State’s direction, the Contractor shall provide the services described in this Contract to third parties, including federal and local government, K-12, and higher education institutions (collectively, “Non-State Participants”).
- 1.1.3. In the course of providing the services described in this RFP, the Contractor shall produce ISACS-related data and methodologies that the Contractor must retain in accordance with *pro forma* Contract Section A.15. The data values that the Contractor is required to retain are detailed in a document titled “Assessment Export File Specification.” This specification document is subject to change at the State’s discretion and may be unique for a given project. A draft of the Assessment Export File Specification is included as RFP Attachment 6.7. Data retained by the Contractor will be encrypted at rest and in motion with access controls based on job function where only personnel involved with a given project have access to the data. All State of Tennessee data housed by the Contractor must reside in the United States.
- 1.1.4. Work performed under the Contract awarded through this RFP shall be performed in accordance with a Memorandum of Understanding (MOU). The format for this MOU is subject to change from time to time, at the State’s discretion. A draft of the MOU is included as RFP Attachment 6.8.

1.2. Scope of Service, Contract Period, & Required Terms and Conditions

The RFP Attachment 6.6., *Pro Forma* Contract details the State’s requirements:

- Scope of Services and Deliverables (Section A);
- Contract Period (Section B);
- Payment Terms (Section C);
- Standard Terms and Conditions (Section D); and,
- Special Terms and Conditions (Section E).

The *pro forma* contract substantially represents the contract document that the successful Respondent must sign.

1.3. **Nondiscrimination**

No person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of a Contract pursuant to this RFP or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal, Tennessee state constitutional, or statutory law. The Contractor pursuant to this RFP shall, upon request, show proof of such nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

1.4. **RFP Communications**

1.4.1. The State has assigned the following RFP identification number that must be referenced in all communications regarding this RFP:

RFP # 31701-03150

1.4.2. **Unauthorized contact about this RFP with employees or officials of the State of Tennessee except as detailed below may result in disqualification from consideration under this procurement process.**

1.4.2.1. Prospective Respondents must direct communications concerning this RFP to the following person designated as the Solicitation Coordinator:

Mitzi Hale
Tennessee Department of Finance and Administration
Strategic Technology Solutions
901 5th Avenue North
Nashville, TN 37243
Phone: 615-741-3735
Email: Mitzi.Hale@tn.gov

1.4.2.2. Notwithstanding the foregoing, Prospective Respondents may alternatively contact:

- a. staff of the Governor's Office of Diversity Business Enterprise for assistance available to minority-owned, woman-owned, Tennessee service-disabled veteran owned, and small businesses as well as general, public information relating to this RFP (visit <http://www.tn.gov/generalservices/article/godbe-general-contacts> for contact information); and
- b. the following individual designated by the State to coordinate compliance with the nondiscrimination requirements of the State of Tennessee, Title VI of the Civil Rights Act of 1964, the Americans with Disabilities Act of 1990, and associated federal regulations:

David Sledge
Title VI Coordinator
Tennessee Department of Finance and Administration

Human Resource Office
21st Floor, Tennessee Tower
312 Rosa L. Parks Avenue
Nashville, TN 37243
Phone: 615-532-4595
Fax: 615-741-3470
E-mail: David.Sledge@TN.gov

- 1.4.3. Only the State's official, written responses and communications with Respondents are binding with regard to this RFP. Oral communications between a State official and one or more Respondents are unofficial and non-binding.
- 1.4.4. Potential Respondents must ensure that the State receives all written questions and comments, including questions and requests for clarification, no later than the Written Questions & Comments Deadline detailed in the RFP Section 2, Schedule of Events.
- 1.4.5. Respondents must assume the risk of the method of dispatching any communication or response to the State. The State assumes no responsibility for delays or delivery failures resulting from the Respondent's method of dispatch. Actual or digital "postmarking" of a communication or response to the State by a specified deadline is not a substitute for the State's actual receipt of a communication or response.
- 1.4.6. The State will convey all official responses and communications related to this RFP to the prospective Respondents from whom the State has received a Notice of Intent to Respond (refer to RFP Section 1.7).
- 1.4.7. The State reserves the right to determine, at its sole discretion, the method of conveying official, written responses and communications related to this RFP. Such written communications may be transmitted by mail, hand-delivery, facsimile, electronic mail, Internet posting, or any other means deemed reasonable by the State. For internet posting, please refer to the following website: <http://tn.gov/generalservices/article/request-for-proposals-rfp-opportunities>.
- 1.4.8. The State reserves the right to determine, at its sole discretion, the appropriateness and adequacy of responses to written comments, questions, and requests related to this RFP. The State's official, written responses will constitute an amendment of this RFP.
- 1.4.9. Any data or factual information provided by the State (in this RFP, an RFP amendment or any other communication relating to this RFP) is for informational purposes only. The State will make reasonable efforts to ensure the accuracy of such data or information, however it is the Respondent's obligation to independently verify any data or information provided by the State. The State expressly disclaims the accuracy or adequacy of any information or data that it provides to prospective Respondents.

1.5. Assistance to Respondents With a Handicap or Disability

Prospective Respondents with a handicap or disability may receive accommodation relating to the communication of this RFP and participating in the RFP process. Prospective Respondents may contact the Solicitation Coordinator to request such reasonable accommodation no later than the Disability Accommodation Request Deadline detailed in the RFP Section 2, Schedule of Events.

1.6. Respondent Required Review & Waiver of Objections

- 1.6.1. Each prospective Respondent must carefully review this RFP, including but not limited to, attachments, the RFP Attachment 6.6., *Pro Forma* Contract, and any amendments, for questions, comments, defects, objections, or any other matter requiring clarification or correction (collectively called "questions and comments").

1.6.2. Any prospective Respondent having questions and comments concerning this RFP must provide them in writing to the State no later than the Written Questions & Comments Deadline detailed in the RFP Section 2, Schedule of Events.

1.6.3. Protests based on any objection to the RFP shall be considered waived and invalid if the objection has not been brought to the attention of the State, in writing, by the Written Questions & Comments Deadline.

1.7. **Notice of Intent to Respond**

Before the Notice of Intent to Respond Deadline detailed in the RFP Section 2, Schedule of Events, prospective Respondents should submit to the Solicitation Coordinator a Notice of Intent to Respond (in the form of a simple e-mail or other written communication). Such notice should include the following information:

- the business or individual's name (as appropriate)
- a contact person's name and title
- the contact person's mailing address, telephone number, facsimile number, and e-mail address

A Notice of Intent to Respond creates no obligation and is not a prerequisite for submitting a response, however, it is necessary to ensure receipt of any RFP amendments or other notices and communications relating to this RFP.

1.8. **Response Deadline**

A Respondent must ensure that the State receives a response no later than the response Deadline time and date detailed in the RFP Section 2, Schedule of Events. A response must respond, as required, to this RFP (including its attachments) as may be amended. The State will not accept late responses, and a Respondent's failure to submit a response before the deadline will result in disqualification of the response. It is the responsibility of the Respondent to ascertain any additional security requirements with respect to packaging and delivery to the State of Tennessee. Respondents should be mindful of any potential delays due to security screening procedures, weather, or other filing delays whether foreseeable or unforeseeable.

2. RFP SCHEDULE OF EVENTS

2.1. The following RFP Schedule of Events represents the State's best estimate for this RFP.

EVENT	TIME (central time zone)	DATE
1. RFP Issued		June 17, 2016
2. Disability Accommodation Request Deadline	2:00 p.m.	June 22, 2016
3. Notice of Intent to Respond Deadline	2:00 p.m.	June 23, 2016
4. Written "Questions & Comments" Deadline	2:00 p.m.	July 1, 2016
5. State Response to Written "Questions & Comments"		August 12, 2016
6. Response Deadline	2:00 p.m.	August 24, 2016
7. State Completion of Technical Response Evaluations		September 13, 2016
8. State Opening & Scoring of Cost Proposals	2:00 p.m.	September 14, 2016
9. State Notice of Intent to Award Released	2:00 p.m.	September 19, 2016
10. RFP Files Opened for Public Inspection	10:00 a.m.	September 20, 2016
11. End of Open File Period		September 27, 2016
12. State sends contract to Contractor for signature		September 28, 2016
13. Contractor Signature Deadline	2:00 p.m.	October 5, 2016

2.2. **The State reserves the right, at its sole discretion, to adjust the RFP Schedule of Events as it deems necessary.** Any adjustment of the Schedule of Events shall constitute an RFP amendment, and the State will communicate such to prospective Respondents from whom the State has received a Notice of Intent to Respond (refer to section 1.7).

3. RESPONSE REQUIREMENTS

3.1. Response Form

A response to this RFP must consist of two parts, a Technical Response and a Cost Proposal.

- 3.1.1. **Technical Response.** RFP Attachment 6.2., Technical Response & Evaluation Guide provides the specific requirements for submitting a response. This guide includes mandatory requirement items, general qualifications and experience items, and technical qualifications, experience, and approach items all of which must be addressed with a written response and, in some instances, additional documentation.

NOTICE: A technical response must not include any pricing or cost information. If any pricing or cost information amounts of any type (even pricing relating to other projects) is included in any part of the technical response, the state may deem the response to be non-responsive and reject it.

- 3.1.1.1. A Respondent must use the RFP Attachment 6.2., Technical Response & Evaluation Guide to organize, reference, and draft the Technical Response by duplicating the attachment, adding appropriate page numbers as required, and using the guide as a table of contents covering the Technical Response.
- 3.1.1.2. A response should be economically prepared, with emphasis on completeness and clarity. A response, as well as any reference material presented, must be written in English and must be written on standard 8 ½" x 11" pages (although oversized exhibits are permissible) and use a 12 point font for text. All response pages must be numbered.
- 3.1.1.3. All information and documentation included in a Technical Response should respond to or address a specific requirement detailed in the RFP Attachment 6.2., Technical Response & Evaluation Guide. All information must be incorporated into a response to a specific requirement and clearly referenced. Any information not meeting these criteria will be deemed extraneous and will not contribute to evaluations.
- 3.1.1.4. The State may determine a response to be non-responsive and reject it if:
- a. the Respondent fails to organize and properly reference the Technical Response as required by this RFP and the RFP Attachment 6.2., Technical Response & Evaluation Guide; or
 - b. the Technical Response document does not appropriately respond to, address, or meet all of the requirements and response items detailed in the RFP Attachment 6.2., Technical Response & Evaluation Guide.

- 3.1.2. **Cost Proposal.** A Cost Proposal must be recorded on an exact duplicate of the RFP Attachment 6.3., Cost Proposal & Scoring Guide.

NOTICE: If a Respondent fails to submit a cost proposal exactly as required, the State may deem the response to be non-responsive and reject it.

- 3.1.2.1. A Respondent must only record the proposed cost exactly as required by the RFP Attachment 6.3., Cost Proposal & Scoring Guide and must NOT record any other rates, amounts, or information.

- 3.1.2.2. The proposed cost shall incorporate ALL costs for services under the contract for the total contract period, including any renewals or extensions.
- 3.1.2.3. A Respondent must sign and date the Cost Proposal.
- 3.1.2.4. A Respondent must submit the Cost Proposal to the State in a sealed package separate from the Technical Response (as detailed in RFP Sections 3.2.3., *et seq.*).

3.2. Response Delivery

3.2.1. A Respondent must ensure that both the original Technical Response and Cost Proposal documents meet all form and content requirements, including all required signatures, as detailed within this RFP.

3.2.2. A Respondent must submit original Technical Response and Cost Proposal documents and copies as specified below.

3.2.2.1. One (1) original Technical Response paper document labeled:

“RFP # 31701-03150 TECHNICAL RESPONSE ORIGINAL”

and six (6) digital copies of the Technical Response each in the form of one (1) digital document in “PDF” format properly recorded on its own otherwise blank, standard CD-R recordable disc or USB flash drive labeled:

“RFP # 31701-03150 TECHNICAL RESPONSE COPY”

The digital copies should not include copies of sealed customer references, however any other discrepancy between the paper Technical Response document and any digital copies may result in the State rejecting the proposal as non-responsive.

3.2.2.2. One (1) original Cost Proposal paper document labeled:

“RFP # 31701-03150 COST PROPOSAL ORIGINAL”

and one (1) copy in the form of a digital document in “PDF” format properly recorded on separate, blank, standard CD-R recordable disc or USB flash drive labeled:

“RFP # 31701-03150 COST PROPOSAL COPY”

In the event of a discrepancy between the original Cost Proposal document and the digital copy, the original, signed document will take precedence.

3.2.3. A Respondent must separate, seal, package, and label the documents and copies for delivery as follows:

3.2.3.1. The Technical Response original document and digital copies must be placed in a sealed package that is clearly labeled:

“DO NOT OPEN... RFP # 31701-03150 TECHNICAL RESPONSE FROM [RESPONDENT LEGAL ENTITY NAME]”

3.2.3.2. The Cost Proposal original document and digital copy must be placed in a separate, sealed package that is clearly labeled:

“DO NOT OPEN... RFP # 31701-03150 COST PROPOSAL FROM [RESPONDENT LEGAL ENTITY NAME]”

- 3.2.3.3. The separately, sealed Technical Response and Cost Proposal components may be enclosed in a larger package for mailing or delivery, provided that the outermost package is clearly labeled:

“RFP # 31701-03150 SEALED TECHNICAL RESPONSE & SEALED COST PROPOSAL FROM [RESPONDENT LEGAL ENTITY NAME]”

- 3.2.4. A Respondent must ensure that the State receives a response no later than the Response Deadline time and date detailed in the RFP Section 2, Schedule of Events at the following address:

Mitzi Hale
Tennessee Department of Finance and Administration
Strategic Technology Solutions
901 5th Avenue North
Nashville, TN 37243
Phone: 615-741-3735

3.3. Response & Respondent Prohibitions

- 3.3.1. 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 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.
- 3.3.3. A response must not propose alternative goods or services (*i.e.*, offer services different from those requested and required by this RFP) unless expressly requested in this RFP. The State may consider a response of alternative goods or services to be non-responsive and reject it.
- 3.3.4. A Cost Proposal must be prepared and arrived at independently and must not involve any collusion between Respondents. The State will reject any Cost Proposal that involves collusion, consultation, communication, or agreement between Respondents. Regardless of the time of detection, the State will consider any such actions to be grounds for response rejection or contract termination.
- 3.3.5. A Respondent must not provide, for consideration in this RFP process or subsequent contract negotiations, any information that the Respondent knew or should have known was materially incorrect. If the State determines that a Respondent has provided such incorrect information, the State will deem the Response non-responsive and reject it.
- 3.3.6. A Respondent must not submit more than one Technical Response and one Cost Proposal in response to this RFP, except as expressly requested by the State in this RFP. If a Respondent submits more than one Technical Response or more than one Cost Proposal, the State will deem all of the responses non-responsive and reject them.
- 3.3.7. A Respondent must not submit a response as a prime contractor while also permitting one or more other Respondents to offer the Respondent as a subcontractor in their own responses. Such may result in the disqualification of all Respondents knowingly involved. This restriction does not, however, prohibit different Respondents from offering the same subcontractor as a part of their responses (provided that the subcontractor does not also submit a response as a prime contractor).

3.3.8. The State shall not consider a response from an individual who is, or within the past six (6) months has been, a State employee. For purposes of this RFP:

3.3.8.1. An individual shall be deemed a State employee until such time as all compensation for salary, termination pay, and annual leave has been paid;

3.3.8.2. A contract with or a response from a company, corporation, or any other contracting entity in which a controlling interest is held by any State employee shall be considered to be a contract with or proposal from the employee; and

3.3.8.3. A contract with or a response from a company, corporation, or any other contracting entity that employs an individual who is, or within the past six (6) months has been, a State employee shall not be considered a contract with or a proposal from the employee and shall not constitute a prohibited conflict of interest.

3.4. **Response Errors & Revisions**

A Respondent is responsible for any and all response errors or omissions. A Respondent will not be allowed to alter or revise response documents after the Response Deadline time and date detailed in the RFP Section 2, Schedule of Events unless such is formally requested, in writing, by the State.

3.5. **Response Withdrawal**

A Respondent may withdraw a submitted response at any time before the Response Deadline time and date detailed in the RFP Section 2, Schedule of Events by submitting a written request signed by an authorized Respondent representative. After withdrawing a response, a Respondent may submit another response at any time before the Response Deadline. After the Response Deadline, a Respondent may only withdraw all or a portion of a response where the enforcement of the response would impose an unconscionable hardship on the Respondent.

3.6. **Additional Services**

If a response offers goods or services in addition to those required by and described in this RFP, the State, at its sole discretion, may add such services to the contract awarded as a result of this RFP. Notwithstanding the foregoing, a Respondent must not propose any additional cost amounts or rates for additional goods or services. Regardless of any additional services offered in a response, the Respondent's Cost Proposal must only record the proposed cost as required in this RFP and must not record any other rates, amounts, or information.

NOTICE: If a Respondent fails to submit a Cost Proposal exactly as required, the State may deem the response non-responsive and reject it.

3.7. **Response Preparation Costs**

The State will not pay any costs associated with the preparation, submittal, or presentation of any response.

4. GENERAL CONTRACTING INFORMATION & REQUIREMENTS

4.1. RFP Amendment

The State at its sole discretion may amend this RFP, in writing, at any time prior to contract award. However, prior to any such amendment, the State will consider whether it would negatively impact the ability of potential Respondents to meet the response deadline and revise the RFP Schedule of Events if deemed appropriate. If an RFP amendment is issued, the State will convey it to potential Respondents who submitted a Notice of Intent to Respond (refer to RFP Section 1.7). A response must address the final RFP (including its attachments) as amended.

4.2. RFP Cancellation

The State reserves the right, at its sole discretion, to cancel the RFP or to cancel and reissue this RFP in accordance with applicable laws and regulations.

4.3. State Right of Rejection

4.3.1. Subject to applicable laws and regulations, the State reserves the right to reject, at its sole discretion, any and all responses.

4.3.2. The State may deem as non-responsive and reject any response that does not comply with all terms, conditions, and performance requirements of this RFP. Notwithstanding the foregoing, the State reserves the right to waive, at its sole discretion, minor variances from full compliance with this RFP. If the State waives variances in a response, such waiver shall not modify the RFP requirements or excuse the Respondent from full compliance, and the State may hold any resulting Contractor to strict compliance with this RFP.

4.4. Assignment & Subcontracting

4.4.1. The Contractor may not subcontract, transfer, or assign any portion of the Contract awarded as a result of this RFP without prior approval of the State. The State reserves the right to refuse approval, at its sole discretion, of any subcontract, transfer, or assignment.

4.4.2. If a Respondent intends to use subcontractors, the response to this RFP must specifically identify the scope and portions of the work each subcontractor will perform (refer to RFP Attachment 6.2., Section B, General Qualifications & Experience, Item B.14.).

4.4.3. Subcontractors identified within a response to this RFP will be deemed as approved by the State unless the State expressly disapproves one or more of the proposed subcontractors prior to signing the Contract.

4.4.4. After contract award, a Contractor may only substitute an approved subcontractor at the discretion of the State and with the State's prior, written approval.

4.4.5. Notwithstanding any State approval relating to subcontracts, the Respondent who is awarded a contract pursuant to this RFP will be the prime contractor and will be responsible for all work under the Contract.

4.5. Right to Refuse Personnel or Subcontractors

The State reserves the right to refuse, at its sole discretion and notwithstanding any prior approval, any personnel of the prime contractor or a subcontractor providing goods or services in the performance of a contract resulting from this RFP. The State will document in writing the reason(s) for any rejection of personnel.

4.6. **Insurance**

From time-to-time, the State may require the awarded Contractor to provide a Certificate of Insurance issued by an insurance company licensed or authorized to provide insurance in the State of Tennessee. Each Certificate of Insurance shall indicate current insurance coverages meeting minimum requirements as may be specified by this RFP. A failure to provide a current, Certificate of Insurance will be considered a material breach and grounds for contract termination.

4.7. **Professional Licensure and Department of Revenue Registration**

- 4.7.1. All persons, agencies, firms, or other entities that provide legal or financial opinions, which a Respondent provides for consideration and evaluation by the State as a part of a response to this RFP, shall be properly licensed to render such opinions.
- 4.7.2. Before the Contract resulting from this RFP is signed, the apparent successful Respondent (and Respondent employees and subcontractors, as applicable) must hold all necessary or appropriate business or professional licenses to provide the goods or services as required by the contract. The State may require any Respondent to submit evidence of proper licensure.
- 4.7.3. Before the Contract resulting from this RFP is signed, the apparent successful Respondent must be registered with the Tennessee Department of Revenue for the collection of Tennessee sales and use tax. The State shall not award a contract unless the Respondent provides proof of such registration or provides documentation from the Department of Revenue that the Contractor is exempt from this registration requirement. The foregoing is a mandatory requirement of an award of a contract pursuant to this solicitation. For purposes of this registration requirement, the Department of Revenue may be contacted at: TN.Revenue@tn.gov.

4.8. **Disclosure of Response Contents**

- 4.8.1. All materials submitted to the State in response to this RFP shall become the property of the State of Tennessee. Selection or rejection of a response does not affect this right. By submitting a response, a Respondent acknowledges and accepts that the full response contents and associated documents will become open to public inspection in accordance with the laws of the State of Tennessee.
- 4.8.2. The State will hold all response information, including both technical and cost information, in confidence during the evaluation process. Notwithstanding the foregoing, a list of actual Respondents submitting timely responses may be available to the public, upon request, after technical responses are opened.
- 4.8.3. 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 *Tennessee Code Annotated*, Section 10-7-504(a)(7).

4.9. **Contract Approval and Contract Payments**

- 4.9.1. After contract award, the Contractor who is awarded the contract must submit appropriate documentation with the Department of Finance and Administration, Division of Accounts.
- 4.9.2. This RFP and its contractor selection processes do not obligate the State and do not create rights, interests, or claims of entitlement in either the Respondent with the apparent best-evaluated response or any other Respondent. State obligations pursuant to a contract award shall commence only after the contract is signed by the State agency head and the Contractor and after the Contract is approved by all other state officials as required by applicable laws and regulations.

- 4.9.3. No payment will be obligated or made until the relevant Contract is approved as required by applicable statutes and rules of the State of Tennessee.
- 4.9.3.1. The State shall not be liable for payment of any type associated with the Contract resulting from this RFP (or any amendment thereof) or responsible for any goods delivered or services rendered by the Contractor, even goods delivered or services rendered in good faith and even if the Contractor is orally directed to proceed with the delivery of goods or the rendering of services, if it occurs before the Contract start date or after the Contract end date.
- 4.9.3.2. All payments relating to this procurement will be made in accordance with the Payment Terms and Conditions of the Contract resulting from this RFP (refer to RFP Attachment 6.6., *Pro Forma* Contract, Section C).
- 4.9.3.3. If any provision of the Contract provides direct funding or reimbursement for the competitive purchase of goods or services as a component of contract performance or otherwise provides for the reimbursement of specified, actual costs, the State will employ all reasonable means and will require all such documentation that it deems necessary to ensure that such purchases were competitive and costs were reasonable, necessary, and actual. The Contractor shall provide reasonable assistance and access related to such review. Further, the State shall not remit, as funding or reimbursement pursuant to such provisions, any amounts that it determines do not represent reasonable, necessary, and actual costs.

4.10. **Contractor Performance**

The Contractor who is awarded a contract will be responsible for the delivery of all acceptable goods or the satisfactory completion of all services set out in this RFP (including attachments) as may be amended. All goods or services are subject to inspection and evaluation by the State. The State will employ all reasonable means to ensure that goods delivered or services rendered are in compliance with the Contract, and the Contractor must cooperate with such efforts.

4.11. **Contract Amendment**

After contract award, the State may request the Contractor to deliver additional goods or perform additional services within the general scope of the contract and this RFP, but beyond the specified scope of service, and for which the Contractor may be compensated. In such instances, the State will provide the Contractor a written description of the additional goods or services. The Contractor must respond to the State with a time schedule for delivering the additional goods or accomplishing the additional services based on the compensable units included in the Contractor's response to this RFP. If the State and the Contractor reach an agreement regarding the goods or services and associated compensation, such agreement must be effected by means of a contract amendment. Further, any such amendment requiring additional goods or services must be signed by both the State agency head and the Contractor and must be approved by other state officials as required by applicable statutes, rules, policies and procedures of the State of Tennessee. The Contractor must not provide additional goods or render additional services until the State has issued a written contract amendment with all required approvals.

4.12. **Severability**

If any provision of this RFP is declared by a court to be illegal or in conflict with any law, said decision will not affect the validity of the remaining RFP terms and provisions, and the rights and obligations of the State and Respondents will be construed and enforced as if the RFP did not contain the particular provision held to be invalid.

4.13. **Next Ranked Respondent**

The State reserves the right to initiate negotiations with the next ranked Respondent should the State cease doing business with any Respondent selected via this RFP process.

5. EVALUATION & CONTRACT AWARD

5.1. Evaluation Categories & Maximum Points

The State will consider qualifications, experience, technical approach, and cost in the evaluation of responses and award points in each of the categories detailed below (up to the maximum evaluation points indicated) to each response deemed by the State to be responsive.

EVALUATION CATEGORY	MAXIMUM POINTS POSSIBLE
General Qualifications & Experience (refer to RFP Attachment 6.2., Section B)	20
Technical Qualifications, Experience & Approach (refer to RFP Attachment 6.2., Section C)	50
Cost Proposal (refer to RFP Attachment 6.3.)	30

5.2. Evaluation Process

The evaluation process is designed to award the contract resulting from this RFP not necessarily to the Respondent offering the lowest cost, but rather to the Respondent deemed by the State to be responsive and responsible who offers the best combination of attributes based upon the evaluation criteria. ("Responsive Respondent" is defined as a Respondent that has submitted a response that conforms in all material respects to the RFP. "Responsible Respondent" is defined as a Respondent that has the capacity in all respects to perform fully the contract requirements, and the integrity and reliability which will assure good faith performance.)

5.2.1. **Technical Response Evaluation.** The Solicitation Coordinator and the Proposal Evaluation Team (consisting of three (3) or more State employees) will use the RFP Attachment 6.2., Technical Response & Evaluation Guide to manage the Technical Response Evaluation and maintain evaluation records.

5.2.1.1. The State reserves the right, at its sole discretion, to request Respondent clarification of a Technical Response or to conduct clarification discussions with any or all Respondents. Any such clarification or discussion will be limited to specific sections of the response identified by the State. The subject Respondent must put any resulting clarification in writing as may be required and in accordance with any deadline imposed by the State.

5.2.1.2. The Solicitation Coordinator will review each Technical Response to determine compliance with RFP Attachment 6.2., Technical Response & Evaluation Guide, Section A— Mandatory Requirements. If the Solicitation Coordinator determines that a response failed to meet one or more of the mandatory requirements, the Proposal Evaluation Team will review the response and document the team's determination of whether:

- a. the response adequately meets RFP requirements for further evaluation;
- b. the State will request clarifications or corrections for consideration prior to further evaluation; or,
- c. the State will determine the response to be non-responsive to the RFP and reject it.

5.2.1.3. Proposal Evaluation Team members will independently evaluate each Technical Response (that is responsive to the RFP) against the evaluation criteria in this RFP,

and will score each in accordance with the RFP Attachment 6.2., Technical Response & Evaluation Guide.

5.2.1.4. For each response evaluated, the Solicitation Coordinator will calculate the average of the Proposal Evaluation Team member scores for RFP Attachment 6.2., Technical Response & Evaluation Guide, and record each average as the response score for the respective Technical Response section.

5.2.1.5. Before Cost Proposals are opened, the Proposal Evaluation Team will review the Technical Response Evaluation record and any other available information pertinent to whether or not each Respondent is responsive and responsible. If the Proposal Evaluation Team identifies any Respondent that does not to meet the responsive and responsible thresholds such that the team would not recommend the Respondent for Cost Proposal Evaluation and potential contract award, the team members will fully document the determination.

5.2.2. **Cost Proposal Evaluation.** The Solicitation Coordinator will open for evaluation the Cost Proposal of each Respondent deemed by the State to be responsive and responsible and calculate and record each Cost Proposal score in accordance with the RFP Attachment 6.3., Cost Proposal & Scoring Guide.

5.2.3. **Total Response Score.** The Solicitation Coordinator will calculate the sum of the Technical Response section scores and the Cost Proposal score and record the resulting number as the total score for the subject Response (refer to RFP Attachment 6.5., Score Summary Matrix).

5.3. Contract Award Process

5.3.1 The Solicitation Coordinator will submit the Proposal Evaluation Team determinations and scores to the head of the procuring agency for consideration along with any other relevant information that might be available and pertinent to contract award.

5.3.2. The procuring agency head will determine the apparent best-evaluated Response. To effect a contract award to a Respondent other than the one receiving the highest evaluation process score, the head of the procuring agency must provide written justification and obtain the written approval of the Chief Procurement Officer and the Comptroller of the Treasury.

5.3.3. The State will issue a Notice of Intent to Award identifying the apparent best-evaluated response and make the RFP files available for public inspection at the time and date specified in the RFP Section 2, Schedule of Events.

NOTICE: The Notice of Intent to Award shall not create rights, interests, or claims of entitlement in either the apparent best-evaluated Respondent or any other Respondent.

5.3.4. 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.

5.3.5. Notwithstanding the foregoing, the State may, at its sole discretion, entertain limited negotiation 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.

- 5.3.6. If the State determines that a response is non-responsive and rejects it after opening Cost Proposals, the Solicitation Coordinator will re-calculate scores for each remaining responsive Cost Proposal to determine (or re-determine) the apparent best-evaluated response.

RFP # 31701-03150 STATEMENT OF CERTIFICATIONS AND ASSURANCES

The Respondent must sign and complete the Statement of Certifications and Assurances below as required, and it must be included in the Technical Response (as required by RFP Attachment 6.2., Technical Response & Evaluation Guide, Section A, Item A.1.).

The Respondent does, hereby, expressly affirm, declare, confirm, certify, and assure ALL of the following:

1. The Respondent will comply with all of the provisions and requirements of the RFP.
2. The Respondent will provide all services as defined in the Scope of Services of the RFP Attachment 6.6., *Pro Forma Contract* for the total contract period.
3. **The Respondent accepts and agrees that the terms and conditions in the contract awarded pursuant to this RFP shall be substantially the same as the terms and conditions set out in the RFP Attachment 6.6., *Pro Forma Contract*; provided, however, that the State shall entertain limited negotiations with the apparent best-evaluated Respondent.**
4. 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.
5. The Respondent will comply with:
 - (a) the laws of the State of Tennessee;
 - (b) Title VI of the federal Civil Rights Act of 1964;
 - (c) Title IX of the federal Education Amendments Act of 1972;
 - (d) the Equal Employment Opportunity Act and the regulations issued there under by the federal government; and,
 - (e) the Americans with Disabilities Act of 1990 and the regulations issued there under by the federal government.
6. To the knowledge of the undersigned, the information detailed within the response submitted to this RFP is accurate.
7. The response submitted to this RFP was independently prepared, without collusion, under penalty of perjury.
8. No amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Respondent in connection with this RFP or any resulting contract.
9. 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.

By signing this Statement of Certifications and Assurances, below, the signatory also certifies legal authority to bind the proposing entity to the provisions of this RFP and any contract awarded pursuant to it. If the signatory is not the Respondent (if an individual) or the Respondent's company *President or Chief Executive Officer*, this document must attach evidence showing the individual's authority to bind the Respondent.

DO NOT SIGN THIS DOCUMENT IF YOU ARE NOT LEGALLY AUTHORIZED TO BIND THE RESPONDENT

SIGNATURE:

PRINTED NAME & TITLE:

DATE:

**RESPONDENT LEGAL ENTITY
NAME:**

**RESPONDENT FEDERAL EMPLOYER IDENTIFICATION NUMBER (or
SSN):**

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION A: MANDATORY REQUIREMENTS. The Respondent must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). The Respondent must also detail the response page number for each item in the appropriate space below.

The Solicitation Coordinator will review the response to determine if the Mandatory Requirement Items are addressed as required and mark each with pass or fail. For each item that is not addressed as required, the Proposal Evaluation Team must review the response and attach a written determination. In addition to the Mandatory Requirement Items, the Solicitation Coordinator will review each response for compliance with all RFP requirements.

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	Item Ref.	Section A— Mandatory Requirement Items	Pass/Fail
		The Response must be delivered to the State no later than the Response Deadline specified in the RFP Section 2, Schedule of Events.	
		The Technical Response and the Cost Proposal documentation must be packaged separately as required (refer to RFP Section 3.2., <i>et. seq.</i>).	
		The Technical Response must NOT contain cost or pricing information of any type.	
		The Technical Response must NOT contain any restrictions of the rights of the State or other qualification of the response.	
		A Respondent must NOT submit alternate responses (refer to RFP Section 3.3.).	
		A Respondent must NOT submit multiple responses in different forms (as a prime and a sub-contractor) (refer to RFP Section 3.3.).	
	A.1.	Provide the Statement of Certifications and Assurances (RFP Attachment 6.1.) completed and signed by an individual empowered to bind the Respondent to the provisions of this RFP and any resulting contract. The document must be signed without exception or qualification.	
	A.2.	Provide a statement, based upon reasonable inquiry, of whether the Respondent or any individual who shall cause to deliver goods or perform services under the contract has a possible conflict of interest (<i>e.g.</i> , employment by the State of Tennessee) and, if so, the nature of that conflict. NOTE: Any questions of conflict of interest shall be solely within the discretion of the State, and the State reserves the right to cancel any award.	
	A.3.	Provide a current bank reference indicating that the Respondent's business relationship with the financial institution is in positive standing. Such reference must be written in the form of a standard business letter, signed, and dated within the past three (3) months.	
	A.4.	Provide two current positive credit references from vendors with which the Respondent has done business written in the form of standard business letters, signed, and dated within the past three (3) months.	
	A.5.	Provide an official document or letter from an accredited credit bureau, verified and dated within the last three (3) months and indicating a	

RESPONDENT LEGAL ENTITY NAME:			
Response Page # (Respondent completes)	Item Ref.	Section A— Mandatory Requirement Items	Pass/Fail
		satisfactory credit rating for the Respondent (NOTE: A credit bureau report number without the full report is insufficient and will <u>not</u> be considered responsive.)	
	A.6.	<p>The Proposer must have performed a security assessment on a government entity or corporation that supports multiple operating systems and networking technologies and that:</p> <ul style="list-style-type: none"> • has a minimum of 5,000 employees; or • has a minimum of 5,000 endpoint devices including 2,000 servers <p><u>Evidence of this should be in the form of a list of the Proposer’s clients meeting this requirement with the total number for each client identified with the client name.</u> The count should be the total number of employees or endpoint devices in the entire organization (federal agency, state government, county government, corporation, etc.), including all divisions, agencies, sections, etc. and may be rounded to the nearest hundred. (For example, the State of Tennessee has approximately 40,000 employees or approximately 45,000 endpoint devices.)</p>	
<i>State Use – Solicitation Coordinator Signature, Printed Name & Date:</i>			

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION B: GENERAL QUALIFICATIONS & EXPERIENCE. The Respondent must address all items detailed below and provide, in sequence, the information and documentation as required (referenced with the associated item references). The Respondent must also detail the response page number for each item in the appropriate space below. Proposal Evaluation Team members will independently evaluate and assign one score for all responses to Section B— General Qualifications & Experience Items.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	Item Ref.	Section B— General Qualifications & Experience Items
	B.1.	Detail the name, e-mail address, mailing address, telephone number, and facsimile number of the person the State should contact regarding the response.
	B.2.	Describe the Respondent's form of business (<i>i.e.</i> , individual, sole proprietor, corporation, non-profit corporation, partnership, limited liability company) and business location (physical location or domicile).
	B.3.	Detail the number of years the Respondent has been in business.
	B.4.	Briefly describe how long the Respondent has been providing the goods or services required by this RFP.
	B.5.	Describe the Respondent's number of employees, client base, and location of offices.
	B.6.	Provide a statement of whether there have been any mergers, acquisitions, or change of control of the Respondent within the last ten (10) years. If so, include an explanation providing relevant details.
	B.7.	Provide a statement of whether the Respondent or, to the Respondent's knowledge, any of the Respondent's employees, agents, independent contractors, or subcontractors, involved in the delivery of goods or performance of services on a contract pursuant to this RFP, have been convicted of, pled guilty to, or pled <i>nolo contendere</i> to any felony. If so, include an explanation providing relevant details.
	B.8.	Provide a statement of whether, in the last ten (10) years, the Respondent has filed (or had filed against it) any bankruptcy or insolvency proceeding, whether voluntary or involuntary, or undergone the appointment of a receiver, trustee, or assignee for the benefit of creditors. If so, include an explanation providing relevant details.
	B.9.	Provide a statement of whether there is any material, pending litigation against the Respondent that the Respondent should reasonably believe could adversely affect its ability to meet contract requirements pursuant to this RFP or is likely to have a material adverse effect on the Respondent's financial condition. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it would impair the Respondent's performance in a contract pursuant to this RFP. NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of license for each person or entity that renders such opinions.
	B.10.	Provide a statement of whether there are any pending or in progress Securities Exchange Commission investigations involving the Respondent. If such exists, list each separately, explain the relevant details, and attach the opinion of counsel addressing whether and to what extent it will impair the Respondent's performance in a contract pursuant to this RFP.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	Item Ref.	Section B— General Qualifications & Experience Items
		NOTE: All persons, agencies, firms, or other entities that provide legal opinions regarding the Respondent must be properly licensed to render such opinions. The State may require the Respondent to submit proof of license for each person or entity that renders such opinions.
	B.11.	Provide a brief, descriptive statement detailing evidence of the Respondent’s ability to deliver the goods or services sought under this RFP (e.g., prior experience, training, certifications, resources, program and quality management systems, etc.).
	B.12.	Provide a narrative description of the proposed project team, its members, and organizational structure along with an organizational chart identifying the key people who will be assigned to deliver the goods or services required by this RFP.
	B.13.	Provide a personnel roster listing the names of key people who the Respondent will assign to meet the Respondent’s requirements under this RFP along with the estimated number of hours that each individual will devote to that performance. Follow the personnel roster with a resume for each of the people listed. The resumes must detail the individual’s title, education, current position with the Respondent, and employment history.
	B.14.	Provide a statement of whether the Respondent intends to use subcontractors to meet the Respondent’s requirements of any contract awarded pursuant to this RFP, and if so, detail: <ul style="list-style-type: none"> (a) the names of the subcontractors along with the contact person, mailing address, telephone number, and e-mail address for each; (b) a description of the scope and portions of the goods each subcontractor involved in the delivery of goods or performance of the services each subcontractor will perform; <u>and</u> (c) a statement specifying that each proposed subcontractor has expressly assented to being proposed as a subcontractor in the Respondent’s response to this RFP.
	B.15.	Provide documentation of the Respondent’s commitment to diversity as represented by the following: <ul style="list-style-type: none"> (a) <u>Business Strategy</u>. Provide a description of the Respondent’s existing programs and procedures designed to encourage and foster commerce with business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises. Please also include a list of the Respondent’s certifications as a diversity business, if applicable. (b) <u>Business Relationships</u>. Provide a listing of the Respondent’s current contracts with business enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises. Please include the following information: <ul style="list-style-type: none"> (i) contract description; (ii) contractor name and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled); (iii) contractor contact name and telephone number. (c) <u>Estimated Participation</u>. Provide an estimated level of participation by business enterprises owned by minorities, women, Tennessee service-disabled veterans, and small business enterprises if a contract is awarded to the Respondent pursuant to this RFP. Please include the following information: <ul style="list-style-type: none"> (i) a percentage (%) indicating the participation estimate. (Express the estimated participation number as a percentage of the total estimated contract value that will be dedicated to business with subcontractors and supply contractors having such ownership characteristics only and DO NOT INCLUDE DOLLAR AMOUNTS); (ii) anticipated goods or services contract descriptions; (iii) names and ownership characteristics (i.e., ethnicity, gender, Tennessee service-disabled veterans) of anticipated subcontractors and supply contractors.

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	Item Ref.	Section B— General Qualifications & Experience Items
		<p>NOTE: In order to claim status as a Diversity Business Enterprise under this contract, businesses must be certified by the Governor's Office of Diversity Business Enterprise (Go-DBE). Please visit the Go-DBE website at https://tn.diversitysoftware.com/FrontEnd/StartCertification.asp?TN=tn&XID=9810 for more information.</p> <p>(d) <u>Workforce</u>. Provide the percentage of the Respondent's total current employees by ethnicity and gender.</p> <p>NOTE: Respondents that demonstrate a commitment to diversity will advance State efforts to expand opportunity to do business with the State as contractors and subcontractors. Response evaluations will recognize the positive qualifications and experience of a Respondent that does business with enterprises owned by minorities, women, Tennessee service-disabled veterans and small business enterprises and who offer a diverse workforce.</p>
	B.16.	<p>Provide a statement of whether or not the Respondent has any current contracts with the State of Tennessee or has completed any contracts with the State of Tennessee within the previous five (5) year period. If so, provide the following information for all of the current and completed contracts:</p> <p>(a) the name, title, telephone number and e-mail address of the State contact knowledgeable about the contract;</p> <p>(b) the procuring State agency name;</p> <p>(c) a brief description of the contract's scope of services;</p> <p>(d) the contract period; and</p> <p>(e) the contract number.</p> <p>NOTES:</p> <ul style="list-style-type: none"> ▪ Current or prior contracts with the State are <u>not</u> a prerequisite and are <u>not</u> required for the maximum evaluation score, and the existence of such contracts with the State will <u>not</u> automatically result in the addition or deduction of evaluation points. ▪ Each evaluator will generally consider the results of inquiries by the State regarding all contracts noted.
	B.17.	<p>Provide customer references from individuals who are <u>not</u> current or former State employees for projects similar to the goods or services sought under this RFP and which represent:</p> <ul style="list-style-type: none"> ▪ two (2) accounts Respondent currently services that are similar in size to the State; <u>and</u> ▪ three (3) completed projects. <p>References from at least three (3) different individuals are required to satisfy the requirements above, e.g., an individual may provide a reference about a completed project and another reference about a currently serviced account. The standard reference questionnaire, which <u>must</u> be used and completed, is provided at RFP Attachment 6.4. References that are not completed as required may be deemed non-responsive and may not be considered.</p> <p>The Respondent will be <u>solely</u> responsible for obtaining fully completed reference questionnaires and including them in the sealed Technical Response. In order to obtain and submit the completed reference questionnaires follow the process below.</p> <p>(a) Add the Respondent's name to the standard reference questionnaire at RFP Attachment 6.4. and make a copy for each reference.</p> <p>(b) Send a reference questionnaire and new, standard #10 envelope to each reference.</p> <p>(c) Instruct the reference to:</p> <ol style="list-style-type: none"> (i) complete the reference questionnaire; (ii) sign and date the completed reference questionnaire; (iii) seal the completed, signed, and dated reference questionnaire within the envelope provided; (iv) sign his or her name in ink across the sealed portion of the envelope; and

RESPONDENT LEGAL ENTITY NAME:		
Response Page # (Respondent completes)	Item Ref.	Section B— General Qualifications & Experience Items
		<p>(v) return the sealed envelope directly to the Respondent (the Respondent may wish to give each reference a deadline, such that the Respondent will be able to collect all required references in time to include them within the sealed Technical Response).</p> <p>(d) <u>Do NOT open the sealed references upon receipt.</u></p> <p>(e) Enclose all <u>sealed</u> reference envelopes within a larger, labeled envelope for inclusion in the Technical Response as required.</p> <p>NOTES:</p> <ul style="list-style-type: none"> ▪ The State will not accept late references or references submitted by any means other than that which is described above, and each reference questionnaire submitted must be completed as required. ▪ The State will not review more than the number of required references indicated above. ▪ While the State will base its reference check on the contents of the sealed reference envelopes included in the Technical Response package, the State reserves the right to confirm and clarify information detailed in the completed reference questionnaires, and may consider clarification responses in the evaluation of references. ▪ The State is under <u>no</u> obligation to clarify any reference information.
	B.18.	<p>Provide a statement and any relevant details addressing whether the Respondent is any of the following:</p> <p>(a) is presently debarred, suspended, proposed for debarment, or voluntarily excluded from covered transactions by any federal or state department or agency;</p> <p>(b) has within the past three (3) years, been convicted of, or had a civil judgment rendered against the contracting party from commission of fraud, or a criminal offence in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;</p> <p>(c) is presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed above; and</p> <p>has within a three (3) year period preceding the contract had one or more public transactions (federal, state, or local) terminated for cause or default.</p>
		<p>SCORE (for <u>all</u> Section B—Qualifications & Experience Items above): (maximum possible score = 20)</p>
State Use – Evaluator Identification:		

TECHNICAL RESPONSE & EVALUATION GUIDE

SECTION C: TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH. The Respondent must address all items (below) and provide, in sequence, the information and documentation as required (referenced with the associated item references). The Respondent must also detail the response page number for each item in the appropriate space below.

A Proposal Evaluation Team, made up of three or more State employees, will independently evaluate and score the response to each item. Each evaluator will use the following whole number, raw point scale for scoring each item:

0 = little value 1 = poor 2 = fair 3 = satisfactory 4 = good 5 = excellent

The Solicitation Coordinator will multiply the Item Score by the associated Evaluation Factor (indicating the relative emphasis of the item in the overall evaluation). The resulting product will be the item’s Raw Weighted Score for purposes of calculating the section score as indicated.

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	Item Ref.	Section C— Technical Qualifications, Experience & Approach Items	Item Score	Evaluation Factor	Raw Weighted Score
	C.1.	Provide a narrative that describes how the Proposer would respond to varying staffing levels. For example, the State may not require any Contractor personnel for several weeks, and then have an immediate need for several Security Assessment Contractor personnel. Describe, in some detail, how the Proposer would meet this staffing need. Limit your response to 1,000 words or less.		10	
	C.2.	DELETED			
	C.3.	DELETED			
	C.4.	Provide a narrative illustrating your methodology for conducting vulnerability/compliance assessments, penetration tests and risk assessments for compliance with regulations including but not limited to FERPA, PCI-DSS, HIPAA, CJIS, IRS Pub 1075, FISMA, MARS-E, SSA and frameworks including but not limited to NIST and ISO 27000.		15	
	C.5.	Provide a narrative detailing the systems that you are able to assess for vulnerabilities; including but not limited to, operating systems, databases, applications, and infrastructure/networking.		5	
	C.6.	Provide a narrative illustrating your methodology for reviewing code.		5	
	C.7.	Provide a narrative describing how you apply your code review methodologies in performing the services for customers. Including project management; incident and emergency procedures; findings, vulnerabilities, and/or report delivery practices.		4	
	C.8.	Provide a list of the code languages you can review.		4	
	C.9.	Provide anonymous examples of each type of report outlined in the required deliverables as provided in the Scope of Services.		4	

RFP ATTACHMENT 6.2. — SECTION C (continued)

RESPONDENT LEGAL ENTITY NAME:					
Response Page # (Respondent completes)	Item Ref.	Section C— Technical Qualifications, Experience & Approach Items	Item Score	Evaluation Factor	Raw Weighted Score
	C.10.	Provide a narrative describing your process for conducting background checks on your employees and type of check performed including, but not limited to, financial, criminal history, and Department of Defense clearances.		3	
	C.11.	Provide a narrative describing your Information security program assessment services.		10	
	C.12.	Provide an example of an information security program assessment services report including the deliverables in the Scope of Services.		5	
	C.13.	Provide a narrative describing your system design services.		10	
	C.14.	Provide a narrative describing your data loss prevention services.		10	
	C.15.	Provide a narrative describing your data and network forensics services.		10	
	C.16.	Provide a narrative describing your ability to respond to multiple simultaneous service requests (breadth of bench).		5	
	C.17.	Provide a narrative describing your data classification and discovery services including, but not limited to, file, database and cloud data.		5	
	C.18.	Provide a narrative describing your services around risk mitigation strategies and solutions.		5	
<i>The Solicitation Coordinator will use this sum and the formula below to calculate the section score. All calculations will use and result in numbers rounded to two (2) places to the right of the decimal point.</i>					Total Raw Weighted Score: <i>(sum of Raw Weighted Scores above)</i>
Total Raw Weighted Score <hr/> Maximum Possible Raw Weighted Score <i>(i.e., 5 x the sum of item weights above)</i>			X 50 <i>(maximum possible score)</i>	= SCORE:	
<i>State Use – Evaluator Identification:</i>					
<i>State Use – Solicitation Coordinator Signature, Printed Name & Date:</i>					

COST PROPOSAL & SCORING GUIDE

NOTICE: THIS COST PROPOSAL MUST BE COMPLETED EXACTLY AS REQUIRED

COST PROPOSAL SCHEDULE— The Cost Proposal, detailed below, shall indicate the proposed price for goods or services defined in the Scope of Services of the RFP Attachment 6.6., *Pro Forma* Contract and for the entire contract period. The Cost Proposal shall remain valid for at least one hundred twenty (120) days subsequent to the date of the Cost Proposal opening and thereafter in accordance with any contract resulting from this RFP. All monetary amounts shall be in U.S. currency and limited to two (2) places to the right of the decimal point.

The proposed hourly rates must be fully loaded to include all administrative, software tools, and excludes travel costs.

The Respondent must enter only one rate per cost cell; the Respondent must NOT enter more than one rate or a range of rates in a single cost cell. The Respondent must NOT add any other information to the Cost Proposal.

The Respondent may enter zero (0) in a required proposed cost cell; however, the Respondent should not leave any proposed cost cell blank. For evaluation and contractual purposes, the State shall interpret a blank Proposed Cost cell as zero (0).

NOTICE: The Evaluation Factor associated with each cost item is for evaluation purposes only. The evaluation factors do NOT and should NOT be construed as any type of volume guarantee or minimum purchase quantity. The evaluation factors shall NOT create rights, interests, or claims of entitlement in the Respondent.

Notwithstanding the cost items herein, pursuant to the second paragraph of the *Pro Forma* Contract section C.1. (refer to RFP Attachment 6.6.), “The State is under no obligation to request work from the Contractor in any specific dollar amounts or to request any work at all from the Contractor during any period of this Contract.”

This Cost Proposal must be signed, in the space below, by an individual empowered to bind the Respondent to the provisions of this RFP and any contract awarded pursuant to it. If said individual is not the *President* or *Chief Executive Officer*, this document must attach evidence showing the individual’s authority to legally bind the Respondent.

RESPONDENT SIGNATURE:	
PRINTED NAME & TITLE:	
DATE:	
RESPONDENT LEGAL ENTITY NAME:	

Cost Item Description	Proposed Cost					State Use ONLY		
	Year 1	Year 2	Year 3	Year 4	Year 5	Sum	Evaluation Factor	Evaluation Cost (sum x factor)
Information Security Assessor / Penetration Tester – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
Information Security Assessor / Penetration Tester – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		20					
Information Security Assessor / Penetration Tester – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		180					
Information Security Assessor / Penetration Tester – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					
Security Program Assessor – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
Security Program Assessor – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		20					
Security Program Assessor – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		150					
Security Program Assessor – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		20					
Data Loss Prevention (DLP) Consultant – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		4					
Data Loss Prevention (DLP) Consultant – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		8					
Data Loss Prevention (DLP) Consultant – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					

Cost Item Description	Proposed Cost					State Use ONLY		
	Year 1	Year 2	Year 3	Year 4	Year 5	Sum	Evaluation Factor	Evaluation Cost (sum x factor)
Data Loss Prevention (DLP) Consultant – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		5					
Forensic Investigator – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
Forensic Investigator – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		4					
Forensic Investigator – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					
Forensic Investigator – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		6					
Security System Design Engineer/Architect – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
Security System Design Engineer/Architect – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		5					
Security System Design Engineer/Architect – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					
Security System Design Engineer/Architect – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		10					
Incident Response Consultant – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
Incident Response Consultant – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					

Cost Item Description	Proposed Cost					State Use ONLY		
	Year 1	Year 2	Year 3	Year 4	Year 5	Sum	Evaluation Factor	Evaluation Cost (sum x factor)
Incident Response Consultant – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					
Incident Response Consultant – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		20					
General Security Consultant – I (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
General Security Consultant – II (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		2					
General Security Consultant – III (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		40					
General Security Consultant – IV (Cont. Sections A.2.b and A.2.c)	\$ Number / per hour		20					
EVALUATION COST AMOUNT (sum of evaluation costs above):								
The Solicitation Coordinator will use this sum and the formula below to calculate the Cost Proposal Score. Numbers rounded to two (2) places to the right of the decimal point will be standard for calculations.								
$\frac{\text{lowest evaluation cost amount from all proposals}}{\text{evaluation cost amount being evaluated}} \times 30 \text{ (maximum section score)} = \text{SCORE:}$								
State Use – Solicitation Coordinator Signature, Printed Name & Date:								

REFERENCE QUESTIONNAIRE

The standard reference questionnaire provided on the following pages of this attachment MUST be completed by all individuals offering a reference for the Respondent.

The Respondent will be solely responsible for obtaining completed reference questionnaires as required (refer to RFP Attachment 6.2., Technical Response & Evaluation Guide, Section B, Item B.17.), and for enclosing the sealed reference envelopes within the Respondent's Technical Response.

RFP # 31701-03150 REFERENCE QUESTIONNAIRE

REFERENCE SUBJECT: RESPONDENT NAME (completed by Respondent before reference is requested)

The "reference subject" specified above, intends to submit a response to the State of Tennessee in response to the Request for Proposals (RFP) indicated. As a part of such response, the reference subject must include a number of completed and sealed reference questionnaires (using this form).

Each individual responding to this reference questionnaire is asked to follow these instructions:

- complete this questionnaire (either using the form provided or an exact duplicate of this document);
 - sign and date the completed questionnaire;
 - seal the completed, signed, and dated questionnaire in a new standard #10 envelope;
 - sign in ink across the sealed portion of the envelope; and
 - return the sealed envelope containing the completed questionnaire directly to the reference subject.
-

(1) What is the name of the individual, company, organization, or entity responding to this reference questionnaire?

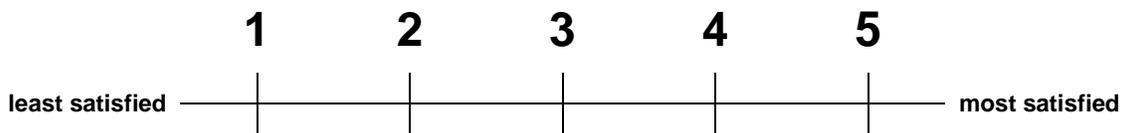
(2) Please provide the following information about the individual completing this reference questionnaire on behalf of the above-named individual, company, organization, or entity.

NAME:	
TITLE:	
TELEPHONE #	
E-MAIL ADDRESS:	

(3) What goods or services does/did the reference subject provide to your company or organization?

(4) What is the level of your overall satisfaction with the reference subject as a vendor of the goods or services described above?

Please respond by circling the appropriate number on the scale below.



If you circled 3 or less above, what could the reference subject have done to improve that rating?

- (5) If the goods or services that the reference subject provided to your company or organization are completed, were the goods or services provided in compliance with the terms of the contract, on time, and within budget? If not, please explain.

- (6) If the reference subject is still providing goods or services to your company or organization, are these goods or services being provided in compliance with the terms of the contract, on time, and within budget? If not, please explain.

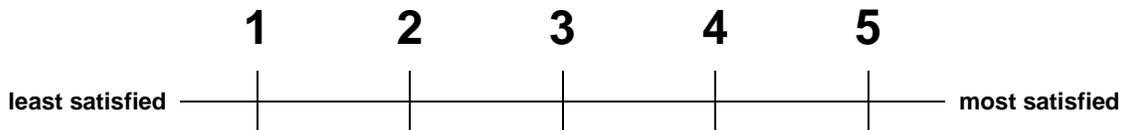
- (7) How satisfied are you with the reference subject's ability to perform based on your expectations and according to the contractual arrangements?

- (8) In what areas of goods or service delivery does/did the reference subject excel?

- (9) In what areas of goods or service delivery does/did the reference subject fall short?

- (10) What is the level of your satisfaction with the reference subject's project management structures, processes, and personnel?

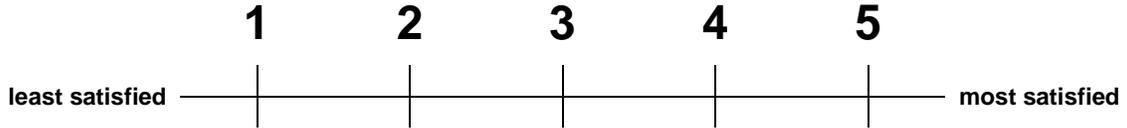
Please respond by circling the appropriate number on the scale below.



What, if any, comments do you have regarding the score selected above?

(11) Considering the staff assigned by the reference subject to deliver the goods or services described in response to question 3 above, how satisfied are you with the technical abilities, professionalism, and interpersonal skills of the individuals assigned?

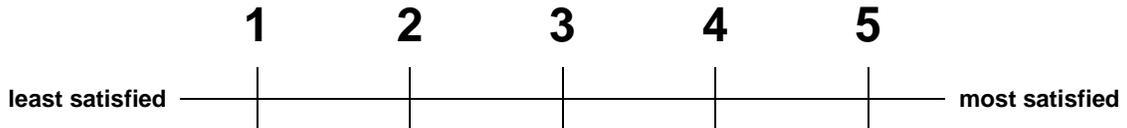
Please respond by circling the appropriate number on the scale below.



What, if any, comments do you have regarding the score selected above?

(12) Would you contract again with the reference subject for the same or similar goods or services?

Please respond by circling the appropriate number on the scale below.



What, if any, comments do you have regarding the score selected above?

REFERENCE SIGNATURE:

(by the individual completing this request for reference information)

_____ (must be the same as the signature across the envelope seal)

DATE:

SCORE SUMMARY MATRIX

	<i>RESPONDENT NAME</i>		<i>RESPONDENT NAME</i>		<i>RESPONDENT NAME</i>	
GENERAL QUALIFICATIONS & EXPERIENCE (maximum: 20)						
<i>EVALUATOR NAME</i>						
<i>EVALUATOR NAME</i>						
<i>REPEAT AS NECESSARY</i>						
	AVERAGE:		AVERAGE:		AVERAGE:	
TECHNICAL QUALIFICATIONS, EXPERIENCE & APPROACH (maximum: 50)						
<i>EVALUATOR NAME</i>						
<i>EVALUATOR NAME</i>						
<i>REPEAT AS NECESSARY</i>						
	AVERAGE:		AVERAGE:		AVERAGE:	
COST PROPOSAL (maximum: 30)	SCORE:		SCORE:		SCORE:	
TOTAL RESPONSE EVALUATION SCORE: (maximum: 100)						

Solicitation Coordinator Signature, Printed Name & Date:

RFP # 31701-03150 *PRO FORMA* CONTRACT

The *Pro Forma* Contract detailed in following pages of this exhibit contains some “blanks” (signified by descriptions in capital letters) that will be completed with appropriate information in the final contract resulting from the RFP.

**CONTRACT
BETWEEN THE STATE OF TENNESSEE,
DEPARTMENT OF FINANCE AND ADMINISTRATION
AND
CONTRACTOR NAME**

This Contract, by and between the State of Tennessee, Department of Finance and Administration ("State") and **Contractor Legal Entity Name** ("Contractor"), is for the provision of Information Security Assessment and Consulting Services (ISACS), as further defined in the "SCOPE." State and Contractor may be referred to individually as a "Party" or collectively as the "Parties" to this Contract.

The Contractor is **a/an Individual, For-Profit Corporation, Non-Profit Corporation, Special Purpose Corporation Or Association, Partnership, Joint Venture, Or Limited Liability Company.**

Contractor Place of Incorporation or Organization: **Location**

Contractor Edison Registration ID # **Number**

A. SCOPE:

A.1. The Contractor shall provide all goods or services and deliverables as required, described, and detailed below and shall meet all service and delivery timelines as specified by this Contract.

A.2. The purpose of this Contract is to provide a source for Information Security Assessment and Consulting Services (ISACS). The Department of Finance & Administration (F&A), Strategic Technology Solutions (STS) will manage the Contract. The services provided by this Contract will be offered to State agencies and/or Non-State Participants through STS. State agencies or Non-State Participants interested in using the services will contact STS and may assist in developing the Statements of Work (SOWs). SOW development is performed by the Contractor based on requirements defined by STS, the agencies and/or Non-State Participants. In addition to the SOW, a Work Breakdown Structure (WBS) will be developed by the Contractor. (See Attachment 6.9 for general WBS format and required information.)

The Contractor must include STS in any and all discussions with State agencies and may include STS in discussions with Non-State Participants (see Contract Section A.16) regarding services provided under this Contract. All SOWs will be initiated and issued by STS and all Memoranda of Understanding (MOUs) will be approved and signed by STS and the Contractor.

- a. Under the terms of this Contract and at the State's request, the Contractor will provide vulnerability assessment and penetration testing services, application source code review services, information security program assessment services, system design services, data loss prevention services and limited data and network forensics services, to the State using the consultants listed in Contract Section A.2.b, below (collectively, "Consultants").
- b. Depending upon the requirements of each specific security assessment project, the Contractor must be prepared to provide Consultants in one or more of the following classifications:
 - i. Information Security Assessor/Penetration Tester. This individual must possess information security-related experience.
 - ii. Security Program Assessor. This individual must possess security program assessment experience, and must be a Certified Information Security Manager (CISM), **or** Certified Information Systems Auditor (CISA), **or** Certified Information Systems Security Professional (CISSP).
 - iii. Data Loss Prevention (DLP) Consultant. This individual must possess DLP experience.

- iv. Forensic Investigator. This individual must possess computer forensics experience and forensics certifications recognized by state and federal courts.
- v. Security System Design Engineer/Architect. This individual must possess security system design experience, must be a CISSP, and also must hold a technical certification such as a Cisco Certified Security Professional (CCSP) and/or Juniper Networks Certified Internet Specialist (JNCIP).
- vi. Incident Response Consultant. This individual must possess incident response certifications such as those from Global Information Assurance Certification (GIAC) GIAC Certified Incident Handler (GCIH) and/or Certified Computer Security Incident Handler (CSIH).
- vii. General Security Consultants. These individuals must have expertise in the compliance areas the State of Tennessee is subject to, including but not limited to PCI-DSS, HIPAA, FERPA, CJIS, IRS Pub 1075, FISMA.

c. In each of the above classifications, the Contractor must be prepared to supply Consultants with varying levels of experience, as follows:

- Level I – Less than five (5) years of experience;
- Level II – From five (5) to less than ten (10) years of experience;
- Level III – From ten (10) to less than fifteen (15) years of experience;
- Level IV – Fifteen (15) or more years of experience.

d. At the Contractor's expense, all Consultants assigned to engagements through this contract must have passed a fingerprint based national criminal history check. The Contractor shall provide the results to the State upon request.

The State, in its discretion, may refuse Consultants if the results reveal a criminal conviction that renders such persons unsuitable for the contract work assignment.

A.3 The specific roles and responsibilities of Contractor consultants shall be as defined in the Contract and future SOWs.

A.4. The SOW will specify the work location(s) of Contractor consultants. Contractor consultants shall provide services under this Contract at one of the following locations:

- a. Contractor consultants may be based on-site and perform their work at State facilities, maintained and managed in Tennessee;
- b. Contractor consultants may be based off-site and perform their work at a Contractor location;
- c. In the case of work that is performed for a Non-State Participant in this Contract, Contractor consultants may be based at facilities operated, maintained, and/or managed by the relevant Non-State Participant (see Contract Section A.16); or
- d. The work may be performed at physical facilities of third parties housing State applications or data.

In any event, the State reserves the right to specify the work location, in the best interest of the project.

A.5. Standard State work schedules are based on a Monday through Friday, thirty seven and one-half (37.5) hour workweek, typically comprised of five (5) seven and one-half (7.5) hour workdays, between the hours of 8:00 a.m. CST and 4:30 p.m. CST, excluding State holidays. Unless

specific times are designated in the SOW, work performed under this Contract may occur during the standard State work schedule, on weekends, on State holidays, and/or at off-hours Monday through Friday. Contractor consultants will be compensated at the payment rates in Contract Section C.3., regardless of the day, date, or time the tasks are performed or the total number of hours worked during a work week.

- A.6. Contractor consultants must provide their own personal computing devices (desktop, laptop, etc.) and licenses for software installed on the devices. Commensurate with the needs of a given project, the State will provide Contractor consultants with office and meeting space, access to telephones, printers, and copiers, and connections to the Internet and/or State network. The State shall be the sole determinant with regard to facilities, supplies, access, and connections required for any given project.
- A.7. The Contractor understands and agrees that the State has executed and may execute contracts with other parties for services the same as or similar to those described herein. The State understands and agrees that the Contractor may perform services the same as or similar to those described herein for other Contractor customers.
- A.8. The purpose of this Contract is to establish a source of supply for information security assessment consultants. However, due to the dynamic nature of projects within State government, the State cannot predict the numbers of Contractor consultants that will be required under this Contract. Therefore, the State makes no guarantees, either stated or implied, about the demand for resources provided through this procurement. The State is not obligated to use any of the Contractor's consultants. Throughout the term of the Contract, the State retains full control and flexibility with regard to the types, quantities, and timing of Contractor consultant usage.
- A.9. Contractor Objectives and Deliverables

- a. Objective 1: Provide Security Vulnerability Assessment and Penetration Testing Services

The Contractor shall conduct vulnerability assessments and penetration tests to assist in strengthening the security posture of the State of Tennessee. Vulnerability assessments and penetration testing services shall be used in identifying and validating configuration and/or technical flaws within a given system or network system components include but are not limited to load-balancers, firewalls, routers, servers, workstations, operating systems, system software, applications, and databases.

Objective 1 Deliverables:

- i. An Assessment Report outlining:
 - (1) Details of the methodology used to conduct the security vulnerability assessments and penetration tests;
 - (2) The results including, but not limited to, the full details of the actions taken; and
 - (3) The detailed documentation of security flaws and remediation recommendations of those flaws found.
- ii. Any additional deliverables as defined in the SOW.
- iii. Exported data from scanning tools for import into the State's Governance Risk and Compliance (GRC) tool. (See RFP Attachment 6.7 for details on the format).

- b. Objective 2: Provide Code Review Services

The Contractor shall conduct code review services to assist the Information Security Assessment and Consulting Services (ISACS) User in strengthening the security posture

of the State of Tennessee. The Contractor shall evaluate source code for programming errors that may lead to security issues (i.e. format string mistakes, buffer overflows, memory leaks, input validation/sanitization mistakes, etc.).

Objective 2 Deliverables:

- i. A Code Review Report outlining:
 - (1) Details of the methodology used to conduct code reviews;
 - (2) The results including, but not limited to, the full details of the actions taken; and
 - (3) The detailed documentation of security flaws and remediation recommendations of those flaws found.
- ii. Any additional deliverables as defined in the SOW.

c. Objective 3: Provide Forensics Services

The Contractor shall provide services for data and network forensics which help to identify the “root cause” of information security incidents within the State’s environment. This includes but is not limited to investigation and retrieval of deleted or modified files, electronic messages and Internet activity; expert testimony; and dedicated hands-on case work investigating intrusions.

Objective 3 Deliverables:

- i. A Forensics Report outlining:
 - (1) Details of the methodology used to conduct forensics;
 - (2) The results including, but not limited to, the full details of the actions taken; and
 - (3) The detailed documentation of findings.
- ii. Any additional deliverables as defined in the SOW.

d. Objective 4: Provide Enterprise Security Program Assessment

The Contractor shall analyze current information security programs and determine the adequacy and effectiveness of the program and its’ associated administrative, technical and management controls using regulatory requirements including, but not limited to, FERPA, PCI-DSS, HIPAA, CJIS, IRS Pub 1075, FISMA, MARS-E, SSA and frameworks including but not limited to NIST **controls 800-53 and 800-88** and ISO 27000.

Objective 4 Deliverables:

- i. A Security Program Assessment Report outlining:
 - (1) Details of the methodology used to conduct the assessment;
 - (2) The results including, but not limited to, the full details of the actions taken; and
 - (3) The detailed documentation of findings.
 - (4) Plan of Action and Milestones (POAM)
- ii. Any additional deliverables as defined in the SOW.

e. Objective 5: Provide Data Loss Prevention (DLP) Assessment

The Contractor shall perform onsite assessments inspecting facilities and operations gaining an understanding of the level of protection desired and effectiveness of policies and controls.

Objective 5 Deliverables:

- i. A DLP Assessment Report outlining:
 - (1) Details of the methodology used to conduct the assessment;
 - (2) The results including, but not limited to, the full details of the actions taken; and
 - (3) The detailed documentation of findings.
- ii. Any additional deliverables as defined in the SOW.

f. Objective 6: Security System Design and Configuration Consultation

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.

Objective 6 Deliverables:

- i. System Specifications: detailed system specification documents and diagrams; and
 - ii. Any additional deliverables as defined in the SOW.
- g. Contractor must provide all software tools required to perform the tasks and deliverables as defined in the State's SOW. All costs associated with software tools must be included in the Consulting Services Hourly Rates listed in Section C.3. The State will not pay separate costs for software tools.

A.10. Procedures/Stipulations for Providing Consultants.

a. Statement of Work.

The State will work with the Contractor to develop an SOW describing the requested services, including as follows.

- i. Project number, which will be used to track the services through completion;
- ii. Description and scope of the requested services including the specific information security and other state standard technologies involved and any special data handling due to issues such as confidentiality;
- iii. Requested project timeframe and any non-standard work schedule tasks;
- iv. Deliverable(s);
- v. Work location;
- vi. State Project Coordinator; and
- vii. Deadline for the Contractor to respond to the State's request (i.e., response period), which will be no more than ten (10) business days measured from the date the SOW was distributed.

b. Submission of Project Proposal.

The Project Proposal consists of the request for service, SOW, WBS and attachments. It is the sole responsibility of the Contractor to develop the WBS. It is the responsibility of

the Contractor to work with the State to develop the SOW. The State will provide all information required to refine requirements. The SOW and WBS process is as follows:

The State contacts the Contractor and briefly discusses a proposed project, which is the request for service. Requirements are gathered via meetings and email until the Contractor understands the project well enough to prepare an SOW and WBS. The SOW and WBS combined constitute the project proposal. If the State agrees to the timeline, scope, description, hours, resource assignments and cost, an MOU is produced by the State. There is no financial obligation from the State until the MOU is executed.

Within the requested response period, the Contractor will respond to the request for a proposal with the SOW and WBS that include the following:

- i. The SOW;
 - ii. Contractor understanding of the work to be performed;
 - iii. WBS, including a project timeframe, tasks, hours by Consultant Classification from Contract Section C.3 and rates (See Attachment 6.9 for more details on WBS requirements.);
 - iv. Maximum project consultant cost, which the Contractor shall calculate by using the payment rates per hour set forth in Section C.3.b. for each Consultant Classification needed for the project. If the project timeframe spans more than one year of the Contract term, the Contractor must calculate the maximum project consultant cost using the payment rates for every effective year. In other words, if the project begin and end dates lie completely within year one of the Contract term, the Contractor would calculate maximum project consultant cost using the payment rates for that Contract year. On the other hand, if the dates begin in Contract year one and extend into any portion of Contract year two, the Contractor must calculate the maximum project consultant cost using the payment rates for both years based on the dates in the WBS. The same rule would apply for all contract years; the maximum project consultant cost must be calculated using the payment rates for the effective years. This maximum project consultant cost shall be a “not to exceed” total cost; the State shall pay no more than this cost for the consultant cost for the project, unless amended in the resulting MOU as described in Contract Section A.10.e; and
 - v. Any Contractor assumptions on which the Project Proposal are based. These assumptions cannot conflict with the terms and provisions of the Contract. In the event of a conflict, the Contract will prevail.
- c. State’s Right to Reject Project Proposals. The State has the sole discretion to accept the Contractor’s Project Proposal, request modifications to the Contractor’s Project Proposal, or to reject the Contractor’s Project Proposal in its entirety.
 - d. Contractor Must Respond to All Requests for Service. The Contractor must respond with a viable Project Proposal as described in A.10.b. Failure to respond to a request for service may result with the State deeming the Contractor to be in Breach of Contract.
 - e. Memorandum of Understanding.

After the State has approved the Project Proposal, it will develop, using the State-approved Memorandum of Understanding format, an MOU, which the Contractor must sign, to bind the Contractor to its Project Proposal for the associated SOW.

The State will provide a copy of the fully executed MOU, containing signatures from Strategic Technology Solutions and the Contractor, to the Contractor. Receipt of a fully

executed MOU authorizes the Contractor to provide the requested services and the Contractor consultants to begin work. The State will not be liable to pay the Contractor for any work performed prior to the Contractor's receipt of a fully executed MOU.

If additional funds are required due to expanded Scope requirements identified by the State, the State, at its discretion, will amend the MOU Maximum Compensation to accommodate completion of the project.

A.11. Contractor Consultant Performance and Replacement.

- a. The Contractor shall select the Consultants to perform the services requested in the SOW. The State shall be the sole judge of the quality of services provided and the project progress achieved by the Contractor's consultants. The Contractor agrees to remove and replace at the Contractor's expense, consultants whom the State judges to be incompetent, careless, unsuitable or otherwise objectionable, or whose continued use is deemed contrary to the best interests of the State or deemed not to make substantial contributions to the project. The Contractor agrees not to charge the State for services performed which the State designates as being unacceptable.

This provision will not be deemed to give the State the right to require the Contractor to terminate any Contractor employee's employment. Rather, this provision is intended to give the State only the right to require that the Contractor discontinue using an employee in the performance of services for the State.

- b. At the State's request, the Contractor will replace an individual that has voluntarily withdrawn or that the Contractor has voluntarily removed from State assignment. Any requirement for such replacement will be at the State's sole discretion; the State is not obligated to accept replacement of removed or withdrawn consultants. The State will compensate the Contractor for acceptable services completed by the consultant prior to voluntary withdrawal or removal.
- c. The termination of an individual consultant's assignment will not necessarily result in the termination of the MOU related to that consultant.

A.12. Miscellaneous Policies and Procedures.

- a. The State will not provide parking for Contractor consultants.
- b. Contractor consultants do not have access to the State clinic.

A.13. Information Security Compliance.

Contractor warrants to the State that it will cooperate with the State in the course of performance of the Contract so that both parties will be in compliance with 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. The Enterprise Security Policies can be found on the State's public website at:

https://www.tn.gov/assets/entities/finance/oir/attachments/PUBLIC-Enterprise-Information-Security-Policies-v2.0_1.pdf

A.14. Periodic Meetings.

The State reserves the right, at the State's option, to request periodic meetings with Contractor management staff to discuss topics including, but not limited to, the following: general project direction, management, and coordination; State technical infrastructure and standards; SOW Clarifications; and time keeping and other project progress records. These meetings shall occur

at a State location or via conference call as agreed to by the parties and shall be at no additional cost to the State.

A.15. Command and Data Retention

The Contractor shall retain the data that they provide to the State and the methodology used to collect it for the duration of the contract for comparative analysis of the same environments. The data values that the Contractor is required to retain are detailed in the "Assessment Export File Specification" document, which will be attached to the associated SOW. This specification is subject to change at the State's discretion and may be unique for a given SOW. The State will provide to the Contractor the most current version of the Assessment Export File Specification as modifications become necessary.

Data retained by the Contractor will be encrypted at rest and in motion and with access controls based on job function where only personnel involved with a given project have access to the data. All State of Tennessee data housed by the Contractor must reside in the United States.

Upon termination of the Contract, a copy of all State information in the Contractor's possession shall be returned to the State. The contractor shall destroy all remaining data in accordance with NIST Publication 800-88.

A.16. Provision of Service to Non-State Participants

At the State's request and under the State's direction, the Contractor shall provide the services described in this Contract to third parties, including federal and local government, K-12, and higher education institutions (collectively, "Non-State Participants").

The State will compensate the Contractor for services performed for Non-State Participants using the hourly rates in Contract Section C.3.b.

A.17. Warranty. 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 general 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 the State is authorized to possess and use all equipment, materials, software, and deliverables provided under this Contract.

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.

If Contractor fails to provide the goods or services as warranted, then Contractor will re-provide the goods or services at no additional charge. If Contractor is unable or unwilling to re-provide the goods or services as warranted, then the State shall be entitled to recover the fees paid to Contractor for the Defective goods or services. Any exercise of the State's rights under this Section shall not prejudice the State's rights to seek any other remedies available under this Contract or applicable law.

A.18. Inspection and Acceptance. The State shall have the right to inspect all goods or services provided by Contractor under this Contract. If, upon inspection, the State determines that the goods or services are Defective, the State shall notify Contractor, and Contractor shall re-deliver the goods or provide the services at no additional cost to the State. If after a period of thirty (30)

days following delivery of goods or performance of services the State does not provide a notice of any Defects, the goods or services shall be deemed to have been accepted by the State.

B. TERM OF CONTRACT:

This Contract shall be effective on **October 12, 2016**, (“Effective Date”) and extend for a period of sixty (60) months after the Effective Date (“Term”). The State shall have no obligation for goods or services provided by the Contractor prior to the Effective Date.

C. PAYMENT TERMS AND CONDITIONS:

C.1. Maximum Liability. In no event shall the maximum liability of the State under this Contract exceed Written Dollar Amount (\$Number) (“Maximum Liability”). This Contract does not grant the Contractor any exclusive rights. The State does not guarantee that it will buy any minimum quantity of goods or services under this Contract. Subject to the terms and conditions of this Contract, the Contractor will only be paid for goods or services provided under this Contract after a purchase order is issued to Contractor by the State or as otherwise specified by this Contract.

C.2. Compensation Firm. The payment methodology in Section C.3 and the Travel Compensation provided in Section C.4. 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.

C.3. Payment Methodology. The Contractor shall be compensated based on the payment methodology for goods or services authorized by the State in a total amount as set forth in Section C.1.

a. The Contractor’s compensation shall be contingent upon the satisfactory provision of goods or services as set forth in Section A.

b. The Contractor shall be compensated based upon the following payment methodology:

Services Description	Amount (per compensable increment)				
	Year 1	Year 2	Year 3	Year 4	Year 5
Information Security Assessor / Penetration Tester - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Information Security Assessor / Penetration Tester - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Information Security Assessor / Penetration Tester - III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Information Security Assessor / Penetration Tester - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security Program Assessor - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security Program Assessor - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security Program Assessor - III	\$ Number	\$ Number	\$ Number	\$ Number	\$ Number

Services Description	Amount (per compensable increment)				
	Year 1	Year 2	Year 3	Year 4	Year 5
	per Hour	per Hour	per Hour	per Hour	per Hour
Security Program Assessor - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Data Loss Prevention (DLP) Consultant - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Data Loss Prevention (DLP) Consultant - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Data Loss Prevention (DLP) Consultant - III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Data Loss Prevention (DLP) Consultant - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Forensic Investigator - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Forensic Investigator - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Forensic Investigator - III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Forensic Investigator - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security System Design Engineer/Architect - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security System Design Engineer/Architect - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security System Design Engineer/Architect - III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Security System Design Engineer/Architect - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Incident Response Consultant - I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Incident Response Consultant - II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Incident Response Consultant - III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
Incident Response Consultant - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
General Security Consultant – I	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
General Security Consultant – II	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour
General Security Consultant – III	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour

Services Description	Amount (per compensable increment)				
	Year 1	Year 2	Year 3	Year 4	Year 5
General Security Consultant - IV	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour	\$ Number per Hour

c. The Contractor shall not be compensated for travel time to the primary location of service provision.

C.4. Travel Compensation. Compensation to the Contractor for travel, meals, or lodging shall be subject to amounts and limitations specified in the current "State Comprehensive Travel Regulations." The Contractor shall not be compensated or reimbursed for travel, meals, or lodging unless approved in advance by the State.

The Contractor must include (in addition to other invoice requirements of this Contract) a complete itemization of requested travel compensation and appropriate documentation and receipts as required by the "State Comprehensive Travel Regulations."

C.5. Invoice Requirements. The Contractor shall invoice the State only for goods delivered and accepted by the State or services satisfactorily provided at the amounts stipulated in Section C.3., above. Contractor shall submit invoices and necessary supporting documentation, no more frequently than once a month, and no later than thirty (30) days after goods or services have been provided to the following address:

Curtis Clan, CISSP
 Chief Information Security Officer
 Department of Finance and Administration
 Strategic Technology Solutions
 901 5th Ave N
 Nashville, TN 37243

a. Each invoice, on Contractor's letterhead, shall clearly and accurately detail all of the following information (calculations must be extended and totaled correctly):

- (1) Invoice number (assigned by the Contractor);
- (2) Invoice date;
- (3) Contract number (assigned by the State);
- (4) Customer account name: Department of Finance and Administration, Strategic Technology Solutions;
- (5) Customer account number (assigned by the Contractor to the above-referenced Customer);
- (6) Contractor name;
- (7) Contractor Tennessee Edison registration ID number;
- (8) Contractor contact for invoice questions (name, phone, or email);
- (9) Contractor remittance address;
- (10) Description of delivered goods or services provided and invoiced, including identifying information as applicable;
- (11) Number of delivered or completed units, increments, hours, or days as applicable, of each good or service invoiced;
- (12) Applicable payment methodology (as stipulated in Section C.3.) of each good or service invoiced;
- (13) Amount due for each compensable unit of good or service; and
- (14) Total amount due for the invoice period.

b. Contractor's invoices shall:

- (1) Only include charges for goods delivered or services provided as described in Section A and in accordance with payment terms and conditions set forth in Section C;
- (2) Only be submitted for goods delivered or services completed and shall not include any charge for future goods to be delivered or services to be performed;
- (3) Not include Contractor's taxes, which includes without limitation Contractor's sales and use tax, excise taxes, franchise taxes, real or personal property taxes, or income taxes; and
- (4) Include shipping or delivery charges only as authorized in this Contract.

c. The timeframe for payment (or any discounts) begins only when the State is in receipt of an invoice that meets the minimum requirements of this Section C.5.

C.6. Payment of Invoice. A payment by the State shall not prejudice the State's right to object to or question any payment, invoice, or other matter. A payment by the State shall not be construed as acceptance of goods delivered, any part of the services provided, or as approval of any amount invoiced.

C.7. 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.

C.8. Deductions. The State reserves the right to deduct from amounts, which are or shall become due and payable to the Contractor under this or any contract between the Contractor and the State of Tennessee, any amounts that are or shall become due and payable to the State of Tennessee by the Contractor.

C.9. Prerequisite Documentation. The Contractor shall not invoice the State under this Contract until the State has received the following, properly completed documentation.

- a. The Contractor shall complete, sign, and present to the State the "Authorization Agreement for Automatic Deposit Form" provided by the State. By doing so, the Contractor acknowledges and agrees that, once this form is received by the State, payments to the Contractor, under this or any other contract the Contractor has with the State of Tennessee, may be made by ACH; and
- b. The Contractor shall complete, sign, and return to the State the State-provided W-9 form. The taxpayer identification number on the W-9 form must be the same as the Contractor's Federal Employer Identification Number or Social Security Number referenced in the Contractor's Edison registration information.

D. MANDATORY TERMS AND CONDITIONS:

D.1. Required Approvals. The State is not bound by this Contract until it is duly approved by the Parties and all appropriate State officials in accordance with applicable Tennessee laws and regulations. Depending upon the specifics of this Contract, this may include approvals by the Commissioner of Finance and Administration, the Commissioner of Human Resources, the Comptroller of the Treasury, and the Chief Procurement Officer. Approvals shall be evidenced by a signature or electronic approval.

D.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by email or facsimile transmission with recipient confirmation. All communications, regardless of method of transmission, shall be addressed to the respective Party at the appropriate mailing address, facsimile number, or email address as

stated below or any other address provided in writing by a Party.

The State:

Curtis Clan, CISSP
Chief Information Security Officer
Department of Finance and Administration
Strategic Technology Solutions
901 5th Ave N
Nashville, TN 37243
Email: Curtis.Clan@tn.gov
Telephone # 615-741-9109

The Contractor:

Contractor Contact Name & Title
Contractor Name
Address
Email Address
Telephone # Number
FAX # Number

All instructions, notices, consents, demands, or other communications shall be considered effective upon receipt or recipient confirmation as may be required.

- D.3. Modification and Amendment. This Contract may be modified only by a written amendment signed by all Parties and approved by all applicable State officials.
- D.4. Subject to Funds Availability. The Contract is subject to the appropriation and availability of State or federal funds. In the event that the funds are not appropriated or are otherwise unavailable, the State reserves the right to terminate this Contract upon written notice to the Contractor. The State's exercise of its right to terminate this Contract shall not constitute a breach of Contract by the State. Upon receipt of the written notice, the Contractor shall cease all work associated with the Contract. If the State terminates this Contract due to lack of funds availability, the Contractor shall be entitled to compensation for all conforming goods requested and accepted by the State and for all satisfactory and authorized services completed as of the termination date. Should the State exercise its right to terminate this Contract due to unavailability of funds, the Contractor shall have no right to recover from the State any actual, general, special, incidental, consequential, or any other damages of any description or amount.
- D.5. Termination for Convenience. The State may terminate this Contract for convenience without cause and for any reason. The State shall give the Contractor at least thirty (30) days written notice before the termination date. The Contractor shall be entitled to compensation for all conforming goods delivered and accepted by the State or for satisfactory, authorized services completed as of the termination date. In no event shall the State be liable to the Contractor for compensation for any goods neither requested nor accepted by the State or for any services neither requested by the State nor satisfactorily performed by the Contractor. In no event shall the State's exercise of its right to terminate this Contract for convenience relieve the Contractor of any liability to the State for any damages or claims arising under this Contract.
- D.6. Termination for Cause. If the Contractor fails to properly perform its obligations under this Contract, or if the Contractor materially violates any terms of this Contract ("Breach Condition"), the State shall provide written notice to Contractor specifying the Breach Condition. If within thirty (30) days of notice, the Contractor has not cured the Breach Condition, the State may terminate the Contract and withhold payments in excess of compensation for completed services or provided goods. Notwithstanding the above, the Contractor shall not be relieved of liability to the State for damages sustained by virtue of any breach of this Contract by the Contractor and the State may seek other remedies allowed at law or in equity for breach of this Contract.

D.7. Assignment and Subcontracting. 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.

D.8. Conflicts of Interest. The Contractor warrants that no part of the Contractor's compensation shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Contractor in connection with any work contemplated or performed under this Contract.

The Contractor acknowledges, understands, and agrees that this Contract shall be null and void if the Contractor is, or within the past six (6) months has been, an employee of the State of Tennessee or if the Contractor is an entity in which a controlling interest is held by an individual who is, or within the past six (6) months has been, an employee of the State of Tennessee.

D.9. Nondiscrimination. The Contractor hereby agrees, warrants, and assures that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the Contractor on the grounds of handicap or disability, age, race, creed, color, religion, sex, national origin, or any other classification protected by federal or state law. The Contractor shall, upon request, show proof of nondiscrimination and shall post in conspicuous places, available to all employees and applicants, notices of nondiscrimination.

D.10. Prohibition of Illegal Immigrants. The requirements of Tenn. Code Ann. § 12-3-309 addressing the use of illegal immigrants in the performance of any contract to supply goods or services to the state of Tennessee, shall be a material provision of this Contract, a breach of which shall be grounds for monetary and other penalties, up to and including termination of this Contract.

a. The Contractor agrees that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract. The Contractor shall reaffirm this attestation, in writing, by submitting to the State a completed and signed copy of the document at Attachment A, semi-annually during the Term. If the Contractor is a party to more than one contract with the State, the Contractor may submit one attestation that applies to all contracts with the State. All Contractor attestations shall be maintained by the Contractor and made available to State officials upon request.

b. Prior to the use of any subcontractor in the performance of this Contract, and semi-annually thereafter, during the Term, the Contractor shall obtain and retain a current, written attestation that the subcontractor shall not knowingly utilize the services of an illegal immigrant to perform work under this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant to perform work under this Contract. Attestations obtained from subcontractors shall be maintained by the Contractor and made available to State officials upon request.

c. The Contractor shall maintain records for all personnel used in the performance of this Contract. Contractor's records shall be subject to review and random inspection at any reasonable time upon reasonable notice by the State.

d. The Contractor understands and agrees that failure to comply with this section will be subject to the sanctions of Tenn. Code Ann. § 12-3-309 for acts or omissions occurring after its effective date.

- e. For purposes of this Contract, "illegal immigrant" shall be defined as any person who is not: (i) a United States citizen; (ii) a Lawful Permanent Resident; (iii) a person whose physical presence in the United States is authorized; (iv) allowed by the federal Department of Homeland Security and who, under federal immigration laws or regulations, is authorized to be employed in the U.S.; or (v) is otherwise authorized to provide services under the Contract.
- D.11. 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.
- D.12. Monitoring. The Contractor's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by the State, the Comptroller of the Treasury, or their duly appointed representatives.
- D.13. Progress Reports. The Contractor shall submit brief, periodic, progress reports to the State as requested.
- D.14. Strict Performance. Failure by any Party to this Contract to require, in any one or more cases, the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the Parties.
- D.15. Independent Contractor. The Parties shall not act as employees, partners, joint venturers, or associates of one another. The Parties are independent contracting entities. Nothing in this Contract shall be construed to create an employer/employee relationship or to allow either Party to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one Party are not employees or agents of the other Party.
- D.16. Patient Protection and Affordable Care Act. The Contractor agrees that it will be responsible for compliance with the Patient Protection and Affordable Care Act ("PPACA") with respect to itself and its employees, including any obligation to report health insurance coverage, provide health insurance coverage, or pay any financial assessment, tax, or penalty for not providing health insurance. The Contractor shall indemnify the State and hold it harmless for any costs to the State arising from Contractor's failure to fulfill its PPACA responsibilities for itself or its employees.
- D.17. Limitation of State's Liability. The State shall have no liability except as specifically provided in this Contract. In no event will the State be liable to the Contractor or any other party for any lost revenues, lost profits, loss of business, decrease in the value of any securities or cash position, time, money, goodwill, or any indirect, special, incidental, punitive, exemplary or consequential damages of any nature, whether based on warranty, contract, statute, regulation, tort (including but not limited to negligence), or any other legal theory that may arise under this Contract or otherwise. The State's total liability under this Contract (including any exhibits, schedules, amendments or other attachments to the Contract) or otherwise shall under no circumstances exceed the Maximum Liability. This limitation of liability is cumulative and not per incident.
- D.18. Limitation of Contractor's Liability. In accordance with Tenn. Code Ann. § 12-3-701, the 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.

- D.19. 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 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.

- D.20. HIPAA Compliance. The State and Contractor shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health ("HITECH") Act and any other relevant laws and regulations regarding privacy (collectively the "Privacy Rules"). The obligations set forth in this Section shall survive the termination of this Contract.

- a. Contractor warrants to the State that it is familiar with the requirements of the Privacy Rules, and will comply with all applicable requirements in the course of this Contract.
- b. Contractor warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by the Privacy Rules, in the course of performance of the Contract so that both parties will be in compliance with the Privacy Rules.
- c. The State and the Contractor will sign documents, including but not limited to business associate agreements, as required by the Privacy Rules and that are reasonably necessary to keep the State and Contractor in compliance with the Privacy Rules. This provision shall not apply if information received or delivered by the parties under this Contract is NOT "protected health information" as defined by the Privacy Rules, or if the Privacy Rules permit the parties to receive or deliver the information without entering into a business associate agreement or signing another document.
- d. The Contractor will indemnify the State and hold it harmless for any violation by the Contractor or its subcontractors of the Privacy Rules. This includes the costs of responding to a breach of protected health information, the costs of responding to a government enforcement action related to the breach, and any fines, penalties, or damages paid by the State because of the violation.

- D.21. Tennessee Consolidated Retirement System. Subject to statutory exceptions contained in Tenn. Code Ann. §§ 8-36-801, *et seq.*, the law governing the Tennessee Consolidated Retirement System ("TCRS"), provides that if a retired member of TCRS, or of any superseded system administered by TCRS, or of any local retirement fund established under Tenn. Code Ann. §§ 8-35-101, *et seq.*, accepts State employment, the member's retirement allowance is suspended during the period of the employment. Accordingly and notwithstanding any provision of this Contract to the contrary, the Contractor agrees that if it is later determined that the true nature of the working relationship between the Contractor and the State under this Contract is that of "employee/employer" and not that of an independent contractor, the Contractor, if a retired member of TCRS, may be required to repay to TCRS the amount of retirement benefits the Contractor received from TCRS during the Term.

- D.22. Tennessee Department of Revenue Registration. The Contractor shall comply with all applicable registration requirements contained in Tenn. Code Ann. §§ 67-6-601 – 608. Compliance with applicable registration requirements is a material requirement of this Contract.
- D.23. Debarment and Suspension. The Contractor certifies, to the best of its knowledge and belief, that it, its current and future principals, its current and future subcontractors and their principals:
- a. are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or state department or agency;
 - b. have not within a three (3) year period preceding this Contract been convicted of, or had a civil judgment rendered against them from commission of fraud, or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or grant under a public transaction; violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, or receiving stolen property;
 - c. are not presently indicted or otherwise criminally or civilly charged by a government entity (federal, state, or local) with commission of any of the offenses detailed in section b. of this certification; and
 - d. have not within a three (3) year period preceding this Contract had one or more public transactions (federal, state, or local) terminated for cause or default.

The Contractor shall provide immediate written notice to the State if at any time it learns that there was an earlier failure to disclose information or that due to changed circumstances, its principals or the principals of its subcontractors are excluded or disqualified.

- D.24. Force Majeure. "Force Majeure Event" means fire, flood, earthquake, elements of nature or acts of God, wars, riots, civil disorders, rebellions or revolutions, acts of terrorism or any other similar cause beyond the reasonable control of the Party except to the extent that the non-performing Party is at fault in failing to prevent or causing the default or delay, and provided that the default or delay cannot reasonably be circumvented by the non-performing Party through the use of alternate sources, workaround plans or other means. A strike, lockout or labor dispute shall not excuse either Party from its obligations under this Contract. Except as set forth in this Section, any failure or delay by a Party in the performance of its obligations under this Contract arising from a Force Majeure Event is not a default under this Contract or grounds for termination. The non-performing Party will be excused from performing those obligations directly affected by the Force Majeure Event, and only for as long as the Force Majeure Event continues, provided that the Party continues to use diligent, good faith efforts to resume performance without delay. The occurrence of a Force Majeure Event affecting Contractor's representatives, suppliers, subcontractors, customers or business apart from this Contract is not a Force Majeure Event under this Contract. Contractor will promptly notify the State of any delay caused by a Force Majeure Event (to be confirmed in a written notice to the State within one (1) day of the inception of the delay) that a Force Majeure Event has occurred, and will describe in reasonable detail the nature of the Force Majeure Event. If any Force Majeure Event results in a delay in Contractor's performance longer than forty-eight (48) hours, the State may, upon notice to Contractor: (a) cease payment of the fees until Contractor resumes performance of the affected obligations; or (b) immediately terminate this Contract or any purchase order, in whole or in part, without further payment except for fees then due and payable. Contractor will not increase its charges under this Contract or charge the State any fees other than those provided for in this Contract as the result of a Force Majeure Event.
- D.25. State and Federal Compliance. The Contractor shall comply with all applicable state and federal laws and regulations in the performance of this Contract.

- D.26. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Tennessee Claims Commission or the state or federal courts in Tennessee shall be the venue for all claims, disputes, or disagreements arising under this Contract. The Contractor acknowledges and agrees that any rights, claims, or remedies against the State of Tennessee or its employees arising under this Contract shall be subject to and limited to those rights and remedies available under Tenn. Code Ann. §§ 9-8-101 - 407.
- D.27. Entire Agreement. This Contract is complete and contains the entire understanding between the Parties relating to its subject matter, including all the terms and conditions of the Parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the Parties, whether written or oral.
- D.28. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions of this Contract shall not be affected and shall remain in full force and effect. The terms and conditions of this Contract are severable.
- D.29. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.30. Incorporation of Additional Documents. Each of the following documents is included as a part of this Contract by reference. In the event of a discrepancy or ambiguity regarding the Contractor's duties, responsibilities, and performance under this Contract, these items shall govern in order of precedence below:
- a. any amendment to this Contract, with the latter in time controlling over any earlier amendments;
 - b. this Contract with any attachments or exhibits (excluding the items listed at subsections c. through f., below), which includes the Memoranda of Understanding (MOUs), their associated Statements of Work (SOWs) and Work Breakdown Structure (WBS);
 - c. any clarifications of or addenda to the Contractor's proposal seeking this Contract;
 - d. the State solicitation, as may be amended, requesting responses in competition for this Contract;
 - e. any technical specifications provided to proposers during the procurement process to award this Contract; and
 - f. the Contractor's response seeking this Contract.
- D.31. Insurance. Contractor shall provide the State a certificate of insurance ("COI") evidencing the coverages and amounts specified below. The COI shall be provided ten (10) business days prior to the Effective Date and again upon renewal or replacement of coverages required by this Contract. If insurance expires during the Term, the State must receive a new COI at least thirty (30) calendar days prior to the insurance's expiration date. If the Contractor loses insurance coverage, does not renew coverage, or for any reason becomes uninsured during the Term, the Contractor shall notify the State immediately.

The COI shall be on a form approved by the Tennessee Department of Commerce and Insurance ("TDCI") and signed by an authorized representative of the insurer. The COI shall list each insurer's national association of insurance commissioners (also known as NAIC) number or federal employer identification number and list the State of Tennessee, Risk Manager, 312 Rosa L. Parks Ave., 3rd floor Central Procurement Office, Nashville, TN 37243 in the certificate holder section. At any time, the State may require the Contractor to provide a valid COI detailing coverage description; insurance company; policy number; exceptions; exclusions; policy effective date; policy expiration date; limits of liability; and the name and address of insured. The

Contractor's failure to maintain or submit evidence of insurance coverage is considered a material breach of this Contract.

If the Contractor desires to self-insure, then a COI will not be required to prove coverage. In place of the COI, the Contractor must provide a certificate of self-insurance or a letter on the Contractor's letterhead detailing its coverage, liability policy amounts, and proof of funds to reasonably cover such expenses. Compliance with Tenn. Code Ann. § 50-6-405 and the rules of the TDCI is required for the Contractor to self-insure workers' compensation.

All insurance companies must be: (a) acceptable to the State; (b) authorized by the TDCI to transact business in the State of Tennessee; and (c) rated A- VII or better by A. M. Best. The Contractor shall provide the State evidence that all subcontractors maintain the required insurance or that the subcontractors are included under the Contractor's policy.

The Contractor agrees to name the State as an additional insured on any insurance policies with the exception of workers' compensation (employer liability) and professional liability (errors and omissions) ("Professional Liability") insurance. Also, all policies shall contain an endorsement for a waiver of subrogation in favor of the State.

The deductible and any premiums are the Contractor's sole responsibility. Any deductible over fifty thousand dollars (\$50,000) must be approved by the State. The Contractor agrees that the insurance requirements specified in this Section do not reduce any liability the Contractor has assumed under this Contract including any indemnification or hold harmless requirements. The State agrees that it shall give written notice to the Contractor as soon as practicable after the State becomes aware of any claim asserted or made against the State, but in no event later than thirty (30) calendar days after the State becomes aware of such claim. 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 or its insurer, 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.

All coverage required shall be on a primary basis and noncontributory with any other insurance coverage or self-insurance carried by the State. The State reserves the right to amend or require additional endorsements, types of coverage, and higher or lower limits of coverage depending on the nature of the work. Purchases or contracts involving any hazardous activity or equipment, tenant, concessionaire and lease agreements, alcohol sales, cyber-liability risks, environmental risks, special motorized equipment, or property may require customized insurance requirements (e.g. umbrella liability insurance) in addition to the general requirements listed below.

The Contractor shall obtain and maintain, at a minimum, the following insurance coverages and policy limits:

a. Commercial General Liability Insurance

- 1) The Contractor shall maintain commercial general liability insurance, which shall be written on an Insurance Services Office, Inc. (also known as ISO) occurrence form (or a substitute form providing equivalent coverage) and shall cover liability arising from property damage, premises/operations, independent contractors, contractual liability, completed operations/products, personal and advertising injury, and liability assumed under an insured contract (including the tort liability of another assumed in a business contract).
- 2) The Contractor shall maintain bodily injury/property damage with a combined single limit not less than one million dollars (\$1,000,000) per occurrence and two million dollars (\$2,000,000) aggregate for bodily injury and property damage, including products and completed operations coverage with an aggregate limit of at least two million dollars (\$2,000,000).

b. Workers' Compensation and Employer Liability Insurance

- 1) For Contractors statutorily required to carry workers' compensation and employer liability insurance, the Contractor shall maintain:
 - i. Workers' compensation and employer liability insurance in the amounts required by appropriate state statutes; or
 - ii. In an amount not less than one million dollars (\$1,000,000) including employer liability of one million dollars (\$1,000,000) per accident for bodily injury by accident, one million dollars (\$1,000,000) policy limit by disease, and one million dollars (\$1,000,000) per employee for bodily injury by disease.
- 2) If the Contractor certifies that it is exempt from the requirements of Tenn. Code Ann. §§ 50-6-101 – 103, then the Contractor shall furnish written proof of such exemption for one or more of the following reasons:
 - i. The Contractor employs fewer than five (5) employees;
 - ii. The Contractor is a sole proprietor;
 - iii. The Contractor is in the construction business or trades with no employees;
 - iv. The Contractor is in the coal mining industry with no employees;
 - v. The Contractor is a state or local government; or
 - vi. The Contractor self-insures its workers' compensation and is in compliance with the TDCI rules and Tenn. Code Ann. § 50-6-405.

c. Automobile Liability Insurance

- i. The Contractor shall maintain automobile liability insurance which shall cover liability arising out of any automobile (including owned, leased, hired, and non-owned automobiles).
- ii. The Contractor shall maintain bodily injury/property damage with a limit not less than one million dollars (\$1,000,000) per occurrence or combined single limit.

E. SPECIAL TERMS AND CONDITIONS:

- E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, the special terms and conditions shall be subordinate to the Contract's other terms and conditions.
- E.2. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the

confidentiality of such material or information in conformance with applicable state and federal law.

The obligations set forth in this Section shall survive the termination of this Contract.

E.3. Ownership of Software and Work Products.

a. Definitions.

- (1) "Contractor-Owned Software," shall mean commercially available software the rights to which are owned by Contractor, including but not limited to commercial "off-the-shelf" software which is not developed using State's money or resources.
- (2) "Custom-Developed Application Software," shall mean customized application software developed by Contractor solely for State.
- (3) "Rights Transfer Application Software," shall mean any pre-existing application software owned by Contractor or a third party, provided to State and to which Contractor will grant and assign, or will facilitate the granting and assignment of, all rights, including the source code, to State.
- (4) "Third-Party Software," shall mean software not owned by the State or the Contractor.
- (5) "Work Product," shall mean all deliverables exclusive of hardware, such as software, software source code, documentation, planning, etc., that are created, designed, developed, or documented by the Contractor exclusively for the State during the course of the project using State's money or resources, including Custom-Developed Application Software. If the deliverables under this Contract include Rights Transfer Application Software, the definition of Work Product shall also include such software. Work Product shall not include Contractor-Owned Software or Third-Party Software.

b. Rights and Title to the Software

- (1) All right, title and interest in and to the Contractor-Owned Software shall at all times remain with Contractor, subject to any license granted under this Contract.
- (2) All right, title and interest in and to the Work Product, and to modifications thereof made by State, including without limitation all copyrights, patents, trade secrets and other intellectual property and other proprietary rights embodied by and arising out of the Work Product, shall belong to State. To the extent such rights do not automatically belong to State, Contractor hereby assigns, transfers, and conveys all right, title and interest in and to the Work Product, including without limitation the copyrights, patents, trade secrets, and other intellectual property rights arising out of or embodied by the Work Product. Contractor and its employees, agents, contractors or representatives shall execute any other documents that State or its counsel deem necessary or desirable to document this transfer or allow State to register its claims and rights to such intellectual property rights or enforce them against third parties.
- (3) All right, title and interest in and to the Third-Party Software shall at all times remain with the third party, subject to any license granted under this Contract.

c. The Contractor may use for its own purposes the general knowledge, skills, experience, ideas, concepts, know-how, and techniques obtained and used during the course of performing under this Contract. The Contractor may develop for itself, or for others,

materials which are similar to or competitive with those that are produced under this Contract.

- E.4. Additional Services. At its sole discretion, the State may make written requests to the Contractor to add services that are needed and within the Scope but were not included in the original Contract. Such services will be added to the Contract through a Memorandum of Understanding ("MOU"), not an amendment.
- a. After the Contractor receives a written request to add the service(s), the Contractor shall have ten (10) business days to respond with a written proposal. The Contractor's written proposal shall include:
 - (1) The effect, if any, of adding the new service(s) on the other services required under the Contract;
 - (2) Any pricing related to the new services;
 - (3) The expected effective date for the availability of the new services; and
 - (4) Any additional information requested by the State.
 - b. The State may negotiate the terms of the Contractor's proposal by requesting revisions to the proposal.
 - c. To indicate acceptance of a proposal, the State will sign it. The signed proposal shall constitute a MOU between the Parties, and the lines, items, or options shall be incorporated into the Contract as if set forth verbatim.
 - d. Only after a MOU has been executed shall the Contractor perform or deliver the new services.
- E.5. Prohibited Advertising or Marketing. The Contractor shall not suggest or imply in advertising or marketing materials that Contractor's goods or services are endorsed by the State. The restrictions on Contractor advertising or marketing materials under this Section shall survive the termination of this Contract.
- E.6. Contractor Commitment to Diversity. The Contractor shall comply with and make reasonable business efforts to exceed the commitment to diversity represented by the Contractor's Response to RFP # 31701-03150 (RFP Attachment 6.2., Section B, General Qualifications & Experience Item B.15.) and resulting in this Contract.
- The Contractor shall assist the State in monitoring the Contractor's performance of this commitment by providing, as requested, a quarterly report of participation in the performance of this Contract by small business enterprises and businesses owned by minorities, women, and Tennessee service-disabled veterans. Such reports shall be provided to the State of Tennessee Governor's Office of Diversity Business Enterprise in the required form and substance.
- E.7. Partial Takeover of Contract. The State may, at its convenience and without cause, exercise a partial takeover of any service that the Contractor is obligated to perform under this Contract, including any service which is the subject of a subcontract between Contractor and a third party (a "Partial Takeover"). A Partial Takeover of this Contract by the State shall not be deemed a breach of contract. The Contractor shall be given at least thirty (30) days prior written notice of a Partial Takeover. The notice shall specify the areas of service the State will assume and the date the State will be assuming. The State's exercise of a Partial Takeover shall not alter the Contractor's other duties and responsibilities under this Contract. The State reserves the right to withhold from the Contractor any amounts the Contractor would have been paid but for the State's exercise of a Partial Takeover. The amounts shall be withheld effective as of the date the State exercises its right to a Partial Takeover. The State's exercise of its right to a Partial Takeover of this Contract shall not entitle the Contractor to any actual, general, special, incidental, consequential, or any other damages irrespective of any description or amount.
- E.8. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For

the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify and/or procure that Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law.

IN WITNESS WHEREOF,

CONTRACTOR LEGAL ENTITY NAME:

CONTRACTOR SIGNATURE

DATE

PRINTED NAME AND TITLE OF CONTRACTOR SIGNATORY (above)

TENNESSEE DEPARTMENT OF FINANCE AND ADMINISTRATION:

LARRY B. MARTIN, COMMISSIONER

DATE

ATTESTATION RE PERSONNEL USED IN CONTRACT PERFORMANCE

SUBJECT CONTRACT NUMBER:	
CONTRACTOR LEGAL ENTITY NAME:	
EDISON VENDOR IDENTIFICATION NUMBER:	

The Contractor, identified above, does hereby attest, certify, warrant, and assure that the Contractor shall not knowingly utilize the services of an illegal immigrant in the performance of this Contract and shall not knowingly utilize the services of any subcontractor who will utilize the services of an illegal immigrant in the performance of this Contract.

CONTRACTOR SIGNATURE

NOTICE: This attestation MUST be signed by an individual empowered to contractually bind the Contractor. Attach evidence documenting the individual's authority to contractually bind the Contractor, unless the signatory is the Contractor's chief executive or president.

PRINTED NAME AND TITLE OF SIGNATORY

DATE OF ATTESTATION

ASSESSMENT EXPORT FILE SPECIFICATION

This assessment export file is to facilitate transfer of data from reports to a GRC system.

The file should be in a non-proprietary format, such as XML. Many tools such as Nessus and Burp Suite Pro are able to export findings to XML format that can include long narratives, tables and URLs.

Field	Explanation, examples
Assessment Identifier	A number or string to uniquely identify the assessment, such as the project number (DC57-Apr09-1)
Issue Identifier	H1, M3, L1, N1
Severity	Critical, High Risk, Medium, Low Risk, Note
Difficulty of exploit	Low to High
Date discovered	
Issue Title	"PHP Multiple Remote Vulnerabilities" or "Application Susceptible to SQL Injection"
External IP address	
Internal IP address	If known or returned in testing
Application name	If applicable
Application URL	If applicable
Agency name	If known
Domain name	If known
Machine name	If known or returned in testing
Host-specific notes	Data specific to this host/application where multiple hosts appear on the report; such as software versions, ports, specific pages, CVE references

Everything other than graphics can be included directly in the XML. Screenshots should be referenced by unique filenames in the XML so that they can be joined to individual findings.

**MEMORANDUM OF UNDERSTANDING
BETWEEN THE
STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION
AND
CONTRACTOR LEGAL ENTITY NAME
FOR
PROJECT YYYY-MM NAME**

This agreement, by and between the State of Tennessee, Department of Finance & Administration, Strategic Technology Solutions, hereinafter referred to as the "State" and **CONTRACTOR LEGAL ENTITY NAME**, hereinafter referred to as the "Contractor" is as follows:

The Contractor understands and agrees that this Memorandum of Understanding (MOU) is governed by the provisions of Department of Finance and Administration Contract Number **Edison ID#**, hereinafter referred to as the "Master Contract". In the provision of services pursuant to this MOU, the Contractor will conform to these provisions in their entirety.

The Contractor will provide the services as described in this MOU and its Addenda, Statement of Work (SOW) and Work Breakdown Structure (WBS), which are attached hereto. In the event of a conflict between the MOU (and its Addenda), and the Master Contract, the documents shall govern in the order of preference given in the Master Contract. This MOU shall be effective for the period commencing on DATE and ending on DATE, unless amended.

Excluding travel estimated at \$###.## in no event shall the maximum liability of the State under this MOU exceed \$##,###.## unless amended at the State's discretion. Travel reimbursement is above and beyond the total fee. For the services provided pursuant to this MOU, the maximum liability amount shall constitute the entire potential compensation due the Contractor for the services and all of the Contractor's obligations hereunder regardless of the difficulty, or materials or equipment required. The Contractor shall be compensated and invoices submitted in accordance with the provisions of the Master Contract.

The State may, at any time and for any reason, terminate this MOU in accordance with the provisions of the Master Contract. Termination of this MOU does not necessarily mean that the State will terminate the Master Contract.

This agreement may be modified only by a written amendment which has been executed and approved by the appropriate State officials as indicated below:

MOU Signatures:

CONTRACTOR LEGAL ENTITY NAME

NAME AND TITLE OF CONTRACTOR SIGNATORY

DATE

DEPARTMENT OF FINANCE AND ADMINISTRATION, STRATEGIC TECHNOLOGY SOLUTIONS

NAME AND TITLE OF STATE PROJECT COORDINATOR DATE

Curtis Clan, CISO DATE

Draft Work Breakdown Structure (WBS)

PROJECT YYYY-MM NAME
Work Breakdown Structure

Duration	WBS	SOW Reference / Description	Hours	Resource & Classification	Resource & Classification	Resource & Classification	On/Off-Site	Notes
				\$RATE	\$RATE	\$RATE		
		Service Description						
		Overall Task						
N Days	1	Overall Task One	\$RATE*HOURS				On-Site	
	1.1	Individual Tasks						
	1.2	Individual Tasks						
	1.3	Individual Tasks						
	1.4	Individual Tasks						
	1.9	Travel						
		Total Hours	\$ - 0	0	0	0		

Worker	Total Amount/Worker	Rate	Hours
Res-Class	\$ -	\$ -	0
Res-Class	\$ -	\$ -	0
Res-Class	\$ -	\$ -	0
Res-Class	\$ -	\$ -	0
Res-Class	\$ -	\$ -	0
Total	\$ -		0
Travel	\$ -		
W/Travel	\$ -		

Draft Statement of Work (SOW)

State of Tennessee
Information Security Assessment Services
Statement of Work

Confidential Under TCA 10-7-504

Contract No.:	FA#####	Project No.:	YYYY-MM NAME
State Project Coordinator:	Steve Swann	Telephone:	615.253.8844
Job Title:	Application Security Consultant	Mobile:	931.334.0272
Address:	Finance & Admin. - STS	E-mail:	Steve.Swann@tn.gov
	901 5 th Avenue North		
	Nashville, TN 37243		

Project Proposal Deadline:

- This SOW and the Work Breakdown Structure constitute the Project Proposal. No additional documentation is requested to proceed to the Memorandum of Understanding (MOU).

Project Timeframe (Specific dates will be mutually agreed to at task kickoff):

- Project Start: DATE
- Report Due: Upon completion of the Assessment

Work Location: [Onsite and/or Offsite]**Project Goals:**

- Goal 1
- Goal 2

Project Description and Scope:

The Office of Strategic Technology Solutions (STS) is requesting an assessment of [X] that meets Project Goals outlined above. This engagement will [DESCRIPTION]. Schedule of events:

- Event 1
- Event 2

The assessment project team shall consist of one project manager and a capable mix of level I, II, III, and IV assessors.

The project manager is responsible for working with the State Project Coordinator to schedule the engagement meetings, keeping the assessment project team on schedule, making sure the deliverables required by this Statement of Work are met, writing the assessment report, and presenting the final presentation to the Comptroller and/or Selected Agencies. The project manager may delegate any of these responsibilities to another team member as appropriate.

Statement of Work:

This SOW is organized into [X] primary functions:

- Assessment
 - Interviews
 - Testing
- Reporting

- a. Develop draft report
 - b. Perform internal review of draft report and document edits
 - c. Develop final report and presentation
3. Prepare and Present Out-Brief
 - a. Coordinate with customer to schedule the out-brief
 - b. Present the out-brief to the customer on-site
 - c. Post-engagement Q&A period

Deliverables:

- I. Executive Summary PPT Presentation following the assessment including:
 - Executive summary of the results and recommendations of the engagement
 - Recommended mitigation strategies
- II. Documents and Data
 - All analyzed data shall be delivered to the State via secure file transfer, accessible only to the project team and those persons identified by the State
 - All documents, correspondence and/or data related to the project are deemed confidential and shall be identified with "Confidential Under TCA 10-7-504."
- III. Post-Engagement Questions and Answers Period
 - Once the Executive Summary has been delivered, the State shall have a timeframe for posing questions to the tester(s) regarding the recommendation and/or remediation suggestions detailed in the Assessment Report. The time allotted for the questions and answers period shall not exceed 10 hours.

STS Contact Information:

1. Steve Swann
 - a. Work: (615) 253-8844
 - b. Mobile: (931) 334-0272
2. Prentice Morgan
 - a. Work: (615) 532-3673