SB1-2018 RFP for Security Risk Assessment

Questions and Responses

Question #1: Would SMU accept alternative proposals to offer these same services as a managed recurring risk assessment over a multi-year period (example, 2 years)?

Response: *No.*

Question #2: On page 4, the request to provide "the total number of qualified personnel that could be available if SMU needs them". Can this be clarified? Does "needs them" mean if they are needed on-site? What would be the work effort anticipated if SMU needed access to these resources?

Response: *The intent of this question is to allow the vendor to provide information on the depth and breadth of the resources available and how the resources would be accessed, if needed.*

Question #3: Does SMU have a requirement for the work to be conducted on-site or can it be done largely remotely?

Response: *Not all of the work will need to be conducted onsite. However, SMU's expectation is that there will need to be a significant amount of interviews with personnel on campus and it will be most effective if everyone is in the same room.*

Question #4: Can the risk assessment be done, in part or whole, by a strategic partner of the submitting firm?

Response: *Yes. All partners/sub-contractors should be clearly identified.*

Question #5: The RFP indicates all network security information will be provided to the awardee(s). Will access to policies, procedures and interview time with key staff also be provided?

Response: *Yes.*

Question #6: Section D, Page 5 indicates a specific format for the response. It appears you are asking for 9 "sections" for our response. Please clarify in exactly what format SMU desires the response.

Response: *Responses should clearly indicate each of the nine (9) sections listed in the order as listed. The specific format is left to the discretion of each vendor keeping in mind that ease of review is important to the Evaluation Committee.*

Question #7: From Section #1.1 – Background: Is the IT organization centralized (all locations/departments administered from a central IT organization) or does each business unit/location have its own IT organization? (ex: bursar, dining, health clinic, public safety, transportation, athletics, academia, administration, etc.)

Response: *SMU's IT organization is centralized.*

Question #8: From Section #1.1 – Background: If the IT organization is de-centralized, please describe how each de-centralized IT organization interacts and works with the University's core IT organization.

Response: *Please see response to question #7.*

Question #9: From Section #1.1 – Background: If the IT organizations are de-centralized, describe how compliance, security, & privacy gap analyses and security risk assessments are performed in a "hierarchical" fashion?

Response: *Please see response to question #7.*

Question #10: From Section #1.2 - Purpose: Has SMU previously conducted a security risk assessment or regulatory compliance gap analysis? If so, when and to which regulatory laws and regulations?

Response: *Yes, SMU will share the relevant prior assessment information with the awarded firm. However, SMU will not disclose the detail of these assessments or whether or not they have been done in the past.*

Question #11: From Section #1.2 - Purpose: Does SMU have an accurate list of "regulatory compliance" requirements that are required of the University? (FERPA, GLBA, GDPR, FISMA, NIST SP-171 CUI, HIPAA, PCI DSS v3.2, State of Texas Privacy Laws, TMRPA, etc.). Also – is the intent – that once the consultant is selected, that the first task order may be to help define the "Regulatory Compliance" requirements?

Response: *Yes. The scope of the assessment has been defined in the proposal and is limited to those regulations, all other compliance regulations will be outside the scope.*

Question #12: From Section #1.2 - Purpose: Where does the responsibility and how is that responsibility shared within SMU for regulatory compliance? (ex. Legal, compliance, IT, etc.)

Response: *This assessment is being done in partnership with several SMU departments including Legal Affairs, Internal Audit, Risk, and IT.*

Question #13: From Section #1.2 - Purpose: Is SMU acting as a PCI DSS Merchant and/or Service Provider too?

Response: *This is outside the scope of this engagement.*

Question #14: From Section #1.2 - Purpose: How does SMU handle "donations" and "alumni payments" via Credit Card – all through the 3rd party 3-commerce payment portal? No dial-up phone donations, etc.?

Response: *This is outside the scope of this engagement.*

Question #15: From Section #1.2 - Purpose: Does SMU currently provide R&D for DoD and US Fed Gov agencies under DFARS regulations, NIST SP800-171 CUI, and/or NIST SP800-53, R4 (FIPS 199 – "Low" or "Moderate", etc.)?

Response: *SMU has contracts with the United States government, but the detail of this can only be shared with the awarded firm.*

Question #16: From Section #1.2 - Purpose: If yes, please describe how many US Fed Gov/DoD contracts are in place now and if the R&D is "isolated" or "segmented" to a specific Department or School and the IT assets are "isolated" or "segmented" within this environment. By "isolated" or "segmented" we mean the IT assets are on its "own" IP data network, locked-down VLAN, or other network infrastructure separate from the rest of the SMU IP data networking infrastructure.

Response: *SMU has contracts with the United States government, but the detail of this can only be shared with the awarded firm.*

Question #17: From Section #1.2 - Purpose: Is the intent of this RFP to award multiple vendors and then release task orders or Statements of Work individually or is this a one-time come in and help us with performing a security risk assessment as per SMU's regulatory compliance requirements in a firm fixed price capacity?

Response: *The intent is to make a one-time award to one vendor at a fixed price. However, if it is in the best interest of SMU to consider alternative award scenarios, they will be considered.*

Question #18: From Section #3 – Scope of Work What is the period of performance for this RFP (Start Date – End Date)? (3.D.4 - Proposal Content Requirements – Timeline)

Response: *The timeline somewhat flexible with an expectation that work would be complete within three (3) months.*

Question #19: From Section #3 – Scope of Work: In Section 1.2 it states, "SMU (and/or SMU's outside counsel) shall issue a firm, fixed-price contract (the "Contract") for the services resulting from this RFP." But in Section 3.D.6 – it states including rates and hours (if applicable) – since this is Firm Fixed Price Contract – does SME require hourly rates and math calculations to derive the Firm Fixed Price or a single, price is all that is required? (3.D.6 – Pricing Proposal – including rates and hours, if applicable)

Response: *Both the firm, fixed-price and hourly rates are required to evaluate/compare vendor estimated hours to complete the project.*

Question #20: In Section 1.2 it states, "Examples of the regulations to be reviewed include, but should not be limited to:

- the European Union's General Data Protection Regulation,
- the National Institute of Standards and Technology's Special Publication 800-171,
- the Health Insurance Portability and Accountability Act (including the Health Information Technology for Economic and Clinical Health Act), and
- the Gramm-Leach-Bliley Act."

Response: *Yes.*

Question #21: It is NOT possible to submit a Firm Fixed Price Pricing Proposal without knowing upfront what the regulatory baseline definition and requirements are. May we make a suggestion:

1. Release a 1st task order to the "selected" consultants and in that 1st task order is the research and definition of SMU's baseline requirements for ALL regulatory compliance laws and mandates.
2. After the 1st task order, release a 2nd task order to the "selected" consultants and in that 2nd task order is the "scope" of the security risk assessment addressing ALL regulatory compliance requirements that are "in scope" of this security risk assessment. That is what the consultant can Firm Fix Price, etc.
3. Is this approach acceptable to SMU?

Response: *Please see response to question #20.*

Question #22: From Section #6.0 - Evaluation Criteria: Is there any consideration given to MBE/DBE/WBE companies or use of sub-contractors?

Response: *No.*

Question #23: From Section #6.0 - Evaluation Criteria: The evaluation criteria stated in the RFP adds up to 90%, what is the remaining 10% comprised of?

Response: *This RFP will be evaluated on a 90 point scale.*

Question #24: Section 1.1 Background: Are assessors meant to assess all three locations or just the main campus in Dallas, TX?

Response: *This scope of this engagement involves the main campus only.*

Question #25: Section 1.2 Purpose What are the objectives for GDPR assessment? Are the assessors meant to determine capability to respond to "Rights of the Individual" requests, identify relevant data types/data store, or both?

Response: *The GDPR assessment should be a complete assessment and gap analysis of SMU's obligations under GDPR, what data is in scope, what elements may or may not be "forgotten" under section 17 and the process for responding to and evaluating requests.*

Question #26: Section 1.2 Purpose What compliance framework or regulation is SMU required to follow for Defense Contractors (e.g. ITAR)?

Response: *SMU follows NIST 800-171.*

Question #27: Section 1.2 Purpose For the NIST 800-171 assessment, is SMU requesting an assessment against each of the Derived Security Requirements noted in the special publication? The alternative is to assess against the Basic Security Requirements and make an expert judgment on the relevance of the derived requirements.

Response: *SMU is requesting an assessment against the Basic Security Requirements plus using expert judgement to meet our requirements. Responses responses that discuss both requirement levels would be accepted.*

Question #28: Could SMU provide a high-level organizational breakdown of IT and Security to help identify the scope of necessary meetings and interviews?

Response: *SMU anticipates that interviews will be necessary not just with IT, but with multiple business units as well. IT is centralized on the campus and there are 6 divisions within IT (security, customer service, academic technology, infrastructure, applications, and project management).*

Question #29: To what degree are data types in the environment documented/diagrammed? Is there a need for some level of data discovery as part of this engagement?

Response: *SMU has documentation and data flow diagrams. However, there may be a need for discovery based on interviews with business units.*

Question #30: Section 1.2 Purpose: SMU states that "the awardee(s) will be provided with appropriate network security information." Is security testing in scope for this project? If so, please elaborate on the services required and quantities for each, including active network IPs, device counts, number of operating systems, and/or number of applications in scope.

Response: *Security testing is out of scope.*

Question #31: Is the IT organization centralized?

Response: *Please see response to question #7.*

Question #32: Are documented policies and procedures in place? If so, how many?

Response: *SMU will provide access to the large volume of documentation that is currently in place to the awarded firm.*

Question #33: When was the last project of this nature performed?

Response: *The last combined compliance assessment was completed in 2013.*

Question #34: Section 1.1 Background: Will the assessment scope include SMU medical school?

Response: *SMU does not have a medical school.*

Question #35: Section 1.2 Purpose: Any previous assessments completed for these areas?

Response: *Please see response to question #33.*

Question #36: Section 1.2 Purpose: Is there a centralized IT/IS team that manages controls across the university, or multiple departments responsible for the different schools?

Response: *There is a centralized IT department and there is shared responsibility for controls with business units.*

Question #37: If IT/IS is managed separately through multiple departments, how many separate teams are expected to be included in the assessment?

Response: *Please see response to question #7.*

Question #38: Section 1.2 Purpose: Does that University expect the contractor to perform network penetration testing (e.g. external or internal)?

Response: *No.*

Question #39: Section 1.2 Purpose: Are there any additional specific regulatory compliance requirements that the contractor should be aware of?

Response: *No.*

Question #40: Section 1.2 Purpose: What type of activities under the stated regulatory requirements for "Defense Contractor" does the University conduct?

Response: *This information is confidential and will be shared with the awarded firm.*

Question #41: Can the proposal be submitted via electronic copy only? Or is a hard copy and USB required?

Response: *As noted on page 5, one hard copy and one electronic copy are required. The electronic copy can be submitted via email rather than on a USB device but must be a single PDF document, with no password protection, and sized to be received by SMU's email system. Vendors can request confirmation that proposals have been received.*

Question #42: The order of the proposal is highlighted in the RFP, is there any requirements for type of proposal (document, powerpoint, etc.)?

Response: *Please see response to question #6.*

Question #43: What event / circumstance has driven this RFP? Is it a grant funded initiative, and if so, what is the grant name? Additionally, can you share the budget for this initiative?

Response: *This RFP is driven by SMU's desire to maintain appropriate data security in an ever-evolving environment. No funding/budget information will be shared.*

Question #44: Is it safe to assume that there is one single IT and Information Security group that supports all the colleges at SMU, and that this assessment will focus on them? Or are there multiple IT groups/organizations we will need to work with for this assessment?

Response: *Please see response to question #7.*

Question #45: Does SMU have an understanding and/or categorization of all applications in their environment?

Response: *Yes.*

Question #46: For regulations that cover more than just Information Security, such as GDPR, do we only need to focus on the Information Security components, or should the proposal include the larger assessment?

Response: *The responses should focus on all components of the regulations to be reviewed.*

Question #47: Does SMU want one assessment that covers all of the identified regulations collectively; or is SMU looking for a separate assessment against each of the identified regulations - resulting in multiple deliverables?

Response: *SMU desires one comprehensive assessment the covers all of the regulations identified in the original RFP document. The timeline provided in the response can detail how the deliverables are given to SMU.*

Question #48: Would one physical penetration test at the main campus (Dallas) be sufficient based on network topology, or would 3 separate site (campus) visits be required?

Response: *Penetration testing is out of scope.*

Question #49: The RFP mentions that 15% of the evaluation is based on acceptance of SMU's terms and conditions. Can you please send a copy of the T&C's that need to be reviewed?

Response: *SMU's standard terms and conditions are attached to this document as Exhibit A.*

Question #50: Page 3, 3. Scope of Work. This section provides a list of items that are to be included in our response and does not provide a Scope of Work - where can we find the Scope of Work?

Response: *Please review Section 1.2 Purpose for the scope of the RFP.*

Question #51: Page 3, 3. Scope of Work and Page 5, D. Proposal Content Requirements. Aside from the obvious, i.e. Pricing and References, under what sections provided in D. Proposal Content Requirements are we to put the items listed on page 3 under A. Demonstrated Qualifications…?

Response: *Each responding vendor is responsible for determining the content provided within the framework of the Proposal Content Requirements.*

Question #52: Page 4, Item 6.b. You request our methodology for conducting a risk assessment. Are you seeking a security risk assessment or a threat risk assessment? They typically have different outcomes.

Response: *The focus of this RFP is a compliance analysis and gap assessment.*

Question #53: Page 4, Item 8. Would you like for us to provide a Certificate of Insurance in our proposal?

Response: *Yes.*

Question #54: Page 4, C. Fee Proposal, third paragraph, 2nd line. You mention "…the entire award period, including any contract extensions." Are you considering a contract period in addition to the time required to complete this assessment?

Response: *SMU reserves the right to extend any contract past the initial contract period if the extension is in the best interest of SMU.*

Question #55: Page 5, D. Proposal Content Requirements. It is stated that "Proposals are required to follow the exact order as provided…" – this order does not follow the order provided in Scope of Work on page 3 – which are we to follow?

Response: *Responses should be organized in the categories and order presented on Page 5, Section D. Proposal Content Requirements.*

Question #56: Page 5, 4. Proposal Submittal, Delivery information. There is an option for "electronic" submission to shannonbrown@smu.edu – in addition to the hard copy and flash drive are we to submit a copy via email as well?

Response: *Please see response to question #41.*

Question #57: Page 6, 6. Evaluation Criteria. The criteria add up to 90%, not 100%. Are we missing pages to the RFP (this RFP ends at the bottom of page 6)?

Response: *Please see response to question #23.*

Question #58: How many external IP addresses are in-scope?

Response: *Please see response to question #48.*

Question #59: How many firewalls/routers are in-scope?

Response: *Please see response to question #48.*

Question #60: Do you want external testing as well as internal?

Response: *Please see response to question #48.*

Question #61: How many departments are in-scope?

Response: *Please see response to question #24.*

Question #62: IT environment-specific questions:

i. Number of computer entities in the organization (DTs, LTs, VMs, Server endpoints)?
ii. Number of employees in the organization?
iii. Number of cyber security personnel?
iv. Number of internal facing and back office applications?
v. Number of external facing/customer facing applications?
vi. Number of VPN gateways?
vii. Number of remote access/VDI gateways?
viii. Does the University have a Security Incident Event Management (SIEM) system?
ix. How many geographical sites exist that are in-scope?
x. How many data centers are included in this engagement?
xi. What organizational security devices or appliances and software are in use today?
xii. Where are the organizational security devices or appliances and software located?
xiii. Regarding organizational security devices, how many alerts occur per day in each location?

Response: *The original RFP document and the responses provided in this document should provide sufficient information for a vendor to submit a proposal. SMU will provide detailed information to the selected firm.*

Question #63: How many specific sites to be visited, and their addresses?

Response: *Please see response to question #24.*

Question #64: Policies to be reviewed and updated?

Response: *Please see response to question #32.*

Question #65: Is a technical vulnerability assessment in scope? If yes, how many IP addresses for: External, Internal

Response: *Vulnerability scans or penetration testing is out of scope for this engagement.*

Question #66: Is a wireless assessment to be performed? # of locations?

Response: *Please see response to question #48.*

Question #67: Is the firewall to be assessed?

Response: *Please see response to question #48.*

Question #68: How many externally accessible IP addresses

Response: *Please see response to question #48.*

Question #69: How many internal IP addresses

Response: *Please see response to question #48.*

Question #70: Do they want every system tested, or can sampling be used?

Response: *Please see response to question #48.*

Question #71: How many internal domains (i.e. Active Directory domains)?

Response: *Please see response to question #48.*

Question #72: How many internal user accounts?

Response: *Please see response to question #48.*

Question #73: Is there an Information Security Management program in place?

Response: *Yes.*