Question & Answers:

Q 1: In section 2.1 Qualifications of Respondent in the RFP, it states that the vendor's proposed staff shall collectively have a list of 22 different certifications. Would you please clarify that the Authority expects all of those certifications to be represented by the proposed staff? Many of them do not seem to be germane to the scope of the project.

Answer- THEA expects at least 10% or more of the certifications listed, or their equivalent, to be represented by proposed staff

Q 2: In section B Insurance Requirements on page 37 of the RFP, Fiduciary Liability Insurance is listed as a requirement. This does not appear to be related to completion of the scope of work. Would the Authority consider removing this requirement?

Answer- Yes.

Q 3: Is this a single award or multiple award contract?

Answer- This is a single award contract.

Q 4: What is the anticipated date of award and contract execution?

Answer- Board approval for the final ranking per the Schedule of Events is on February 27th, 2023. Scope Clarification and Negotiations with the final ranked Respondent will be held in March 2023. Once Negotiations are complete, THEA can move forward with coordination efforts on contract execution.

Q 5: Is there any budget allocated for this contract? If yes, can you please let us know the same?

Answer- Yes

Q 6: Is there an incumbent on the contract? If yes, could you please let us know the incumbent name and spending done on contract so far? And are they eligible to be awarded this contract?

Answer- No

Q 7: What is the total number of resources who are currently working on this project? Please let us know their position name and hourly rate.

Answer- We do not have a current contract for these services

Q 8: Considering the current COVID-19 pandemic situation, if the proposed candidates are not available at the time of award, will the agency allow us to provide replacement personnel with similar or more skill sets?

Answer- Yes

Q 9: Is there any limitation on providing resumes of the personnel, i.e., if the requirement is for two candidates; do we need to submit only two resumes or can we propose resumes of more than two candidates for agency's consideration?

Answer- As this is a qualifications-based procurement there is no limitation on resumes for any appropriate staff you are proposing for key personnel.

Q 10: Is it entirely onsite work or can it be done remotely to some extent / Does the services need to be delivered onsite or is there a possibility for remote operations and performance?

Answer- The Scope of work is not expected to be entirely onsite. See scope of work for specified onsite tasks. Remote is acceptable for some tasks

Q 11: Are hourly rate ranges acceptable for proposed personnel including key?

Answer- Yes.

Q 12: Are all monitoring services managed by THEA staff or are some of these operations outsourced?

Answer- Some of these are out-sourced

Q 13: Has the new network architecture already been designed?

Answer- These are existing networks

Q 14: Task 3 is called "Website Assessment and Penetration Testing." However. the description includes vulnerability scans but not penetration tests. Are you expecting the performance of a penetration test or an assessment of the web application, including the scanning for additional vulnerabilities?

Answer- We are expecting vulnerability and penetration testing

Q 15: How many external active IP addresses are in scope?

Answer- 15-25

Q 16: Can we assume that the total number of internal active IP addresses in scope are the numbers provided in the description of the THEA Admin and Operations environment? If not, can you provide the approximate number of internal active IP addresses?

Answer- As described in the scope is a fair estimate

Q 17: Can you please confirm that all the qualifications outlined on pages 14 and 15 of the RFP are mandatory? The Microsoft Certified IT Professional (MCITP): Data Base Administration (MCITP) is based on older Microsoft products, and most MCITP certifications were retired in 2014.

Answer- See answer to question one above

Q 18: How many IP addresses are in scope for External Vulnerability Scanning?

Answer- See answer to question 15 above

Q 19: How many IP addresses are in scope for Internal Vulnerability Scanning?

Answer- See answer to question 16 above

Q 20: How many live web pages are in scope for tamap-xway.com? How many forms are on each page?

Answer- Number of pages – 64; Number of Forms - 7

Q 21: Are we required to propose staff meeting every certification listed or are we required to just meet some of these certifications?

Answer- See answer to question one above

Q 22: Please confirm that references are requested in both sections.

Answer- The three (3) references will not be counted within the 5-page ELOR. You can mention your past performance/references within the ELOR; however, we will expect the references to be located on additional pages included in the combined package.

Q 23: The Checklist in Form 6 does not seem to match with Forms requested in Section B OR the forms provided in the RFP document. Could you please indicate which forms we have to complete in order to provide a complete response?

Answer- The Checklist (Form 6) is the way THEA requests the packages to be organized based on the requirements from this solicitation. These are also the required forms to be completed to be found responses. Please include the following forms per page 22.
Form 1 - Declaration of Respondent

Form 2 - Public Entity Crimes Form

Form 3 - Conflicts of Interest Statement

Form 4 - Certification Regarding Scrutinized Companies List

Form 5 - Acknowledgement of Receipt of Addendum

Q 24: Is THEA looking for pricing information with the proposal?

Answer- This is a qualifications-based procurement. Cost/pricing is not an evaluation criterion of this procurement. The Procurement Office will request Hourly Wage Rate information during the negotiations process with the final selected Respondent.

Q 25: Are you open to proposers offering alternative insurance levels? For example, removing Fiduciary Liability Insurance and Environmental Impairment Liability.

Answer- Yes

Q 26: Is the place of performance on-site or remote? If on-site, how many locations?

Answer- Both. 2 onsite locations and remote for some tasks.

Q 27: Specify the VLAN details how many are included in the Scope?

Answer- 4-8 VLANs

Q 28: How much (%) of the infrastructure is in the cloud?

Answer- Only Microsoft 365 is used in the cloud

Q 29: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Answer- No 3rd party/co-location facilities are used

Q 30: Do you require a cost proposal along with the proposal submission, or just a technical proposal?

Answer- Per the Request for Proposal, THEA requires an Expanded Letter of Response, Organizational Chart, Resumes, Staff Hour Estimate, References, and the required forms per Section B.

Q 31: Is there a regulatory requirement for all of these certifications? If not, is there some other justification for all of these certifications?

Answer- See answer to question one above

Q 32: Is there some flexibility on these requirements, as some are redundant (e.g. Security + and CISSP) and some seem very peripheral to a Cybersecurity Assessment (e.g. Grant Professionals Certification Institute (GPCI) & Sophos Sales Engineer)?

Answer- See answer to question one above

Q 33: Does THEA currently follow any cybersecurity best practice framework or standard such as the NIST Cybersecurity Framework? If no, please indicate the preference of cybersecurity best practice framework or standard that the consultant should use?

Answer- NIST Cybersecurity Framework is preferred

Q 34: In the Gap Analysis section of the Audit of Network Architecture and Internet Connectivity section, are those listed bullets the only areas upon which THEA would like the consultant to find gaps or is it expected that other cybersecurity controls are reviewed and assessed such as those in the preferred best practice framework or standard?

Answer- It is expected that other cybersecurity controls are reviewed and assessed such as those in the preferred best practice framework or standard.

Q 35: Under the Penetration Testing Deliverables sections, it states a "…narrative of employee security awareness…" is required. What exactly is THEA expecting for this? Would it be a finding and recommendation around the state of security awareness and needed training for the workforce?

Answer- Yes

Q 36: For the Audit of Website tampa-xway.com, does THEA desire credentialed scanning to be performed?

Answer- Yes

Q 37: For the Audit of Website tampa-xway.com, what is the number of user roles that THEA would like us to test with?

Answer- ALL

Q 38: For the Audit of Website tampa-xway.com, what is the number of APIs that are in use and is documentation available for each?

Answer- Number of APIs - 1

Q 39: What is the number of external target systems or subnets for the THEA Operations & THEA Admin Network Environment that we should anticipate for external penetration testing?

Answer- See answer to question #15 above

Q 40: What is the number of internal target systems or subnets for the THEA Operations & THEA Admin Network Environment that we should anticipate for internal penetration testing?

Answer- See answer to question # 16 above

Q 41: Are all internal target systems or subnets for both the Operations and Admin Network Environments accessible from a centralized location or is it expected that travel to other sites will be necessary?

Answer- Accessible from a centralized location

Q 42: What is the number of wireless networks (distinct SSIDs) for each of the Network Environments that are in scope for penetration testing?

Answer- 2

Q 43: For the various types of penetration testing requested by THEA, does THEA expect that a risk-based approach will be used to identify the target systems with identified vulnerabilities most plausible for gaining and maintaining access ("attack and exploit") tasks OR is it THEA's expectation that the consultant attempt attack and exploit tasks on all in-scope target systems?

Answer- THEA expects a risk-based approach

Q 44: How many of the IT staff within the THEA Admin & Operations Network Environment should the consultant anticipate interviewing?

Answer- Approximately 4

Q 45: How many department end users and management representatives should the consultant anticipate interviewing?

Answer- 2-5

Q 46: When is the desired completion date for this engagement with THEA?

Answer- Per the Request for Proposals, the contract duration will be for six (6) months from the Notice To Proceed (NTP).

Q 47: Will internal network access be provided during phase 1, or will internal testing only be performed during this phase if access is achieved during external testing?

Answer- No Access is provided in Phase 1

Q 48: Based on employee security awareness reporting being an objective, are social engineering exercises such as email and phone phishing in scope?

Answer- See Page 4 of RFP "Tasks Excluded"

Q 49: In the Declaration of Respondent form, the bidder is required to note compliance with terms such as insurance and indemnification. In Section 1.21 – Award of the Contract within the RFP, it states that the top ranked firm will have the ability to negotiate terms, including insurance requirements and any other negotiable terms and conditions. We would like the opportunity to negotiate those terms if we are the top ranked firm. Would THEA be open to removing the confirmation requirement on the Declaration of Respondent form given the statements regarding the willingness to negotiation in Section 1.21 of the solicitation?

Answer- Insurance requirements are subject to negotiations with the top ranked Respondent following award.

Q 50: In Section 1.11.2 of the RFP, it states that bids may be deemed non-responsive bids if they include a limitation of liability. We would anticipate this would be handled as part of the overall negotiation of the terms and conditions. If a firm wishes to include a limitation of liability as part of the negotiation process, would they be deemed non-responsive?

Answer- See Answer to # 49.

Q 51: The Declaration of Respondent form asks for "the project manager assigned to this contract has a current professional license number of_____ issued by the state of____? What type of professional license number is THEA looking for?

Answer- See answer to question one above

Q 52: Can the team members work offshore?

Answer- No

Q 53: In section 2.1 EXPANDED LETTERS OF RESPONSE (ELOR) PACKAGE: subsection Content point 3 we need to include an organizational chart. Are you requesting an organizational chart for the prime & subcontractor? Do we have to provide an organizational chart with the key personnel for the subcontractor? or is it only for the prime? Does the organizational chart only include the key members who will work on the project or does need to include information regarding prime & subcontractor company organization?

Answer- Per the Request for Proposals, the Organization Chart should include the following:

- Identify key members of Respondent's team including the proposed Project Manager, and names and roles of other key personnel
- State firm name for key members of Respondent's team (if from a Subcontractor);
- Denote if Respondent firm or Subcontractor firms are a SBE;
- State office location (city and state) for key members of Respondent's team.

Only those members of the team who will actively participate under the potential work assignments should be included. Individuals who would be available on an "as-needed" basis should be omitted.

Q 54: Is it required to have a local office in Florida?

Answer- No

Q 55: Does THEA have any other preferred pricing format different than the example included in section 6? Staff hour Estimate?

Answer- No, cost/pricing is not an evaluation criterion of this procurement. As this is a qualifications-based procurement, a Staff Hour Estimate sheet with the proposed staff and hours estimated to perform this scope of work is required. The Procurement Office will request Hourly Wage Rate information during the negotiations process with the final selected Respondent.

Q 56: Do the forms need to be submitted by the prime contractor? Or is it required for the subcontractor to submit them as well?

Answer- Yes, the forms are to be submitted by the Prime Respondent with their Response Package.

Q 57: In the form declaration of the respondent is mentioned that we need to provide the Professional License Number. Are you referring to a Professional License Number for the Project Manager or the company?

Answer- Yes, the Professional License Number for the Project Manager.

Q 58: Does it have to be a Florida License number?

Answer- No.

Q 58: If it is mandatory for the firm to have a license number, Does it have to be a Florida License number?

Answer- No, the Professional License Number for the Project Manager.

Q 59: Regarding the presentation format. Is there a preferred font type?

Answer- No, there is not a specific font style required.

Q 60: Can the 3 references be from our subcontractor or do they have to belong to the prime contractor?

Answer- It is preferred that the majority of references represent work performed by the Prime Respondent.

Q 61: Could you please grant an extension on the due date?

Answer- At this time we will not be making changes to the Schedule of Events.

Q 62: Is it required to provide the COI alongside the proposal response?

Answer- The COI will be required of the Final Selected Respondent.

Q 63: The ELOR Packages must not exceed 8 MG in size in Adobe PDF format and unzipped.

Answer- To clarify, the size limitation for the Response Package is 8 MB.

Q 64: Does THEA have any mandatory goal for SBE/WBE/LBE/MBE for this particular contract?

Answer- No.

Q 65: Do we need to be certified as an SBE to be awarded?

Answer- No.

Q 66: Would an SBE Certification and work plan receive additional points during the evaluation process?

Answer- No, Grading Criteria for the Responses are listed under section 1.17 RESPONSE EVALUATIONS within the Request for Proposals.

Q 67: Do you have any local preferences?

Answer- No