**Appendix 2**

**TECHNICAL QUESTIONNAIRE**

**RFP ETD0060**

**Information Technology Audits and Consulting**

**This Technical Questionnaire section is scored. (500 total points)**

The purpose of this questionnaire is to provide the Department with a basis for determining the Proposer’s capability to undertake the Contract.

All Proposers must respond to the following by restating the identifying number of each question (for example, 2.1), restating each question or statement, and providing a detailed written response. The Proposal, at a minimum, must address the items listed below and be organized and labeled in the order indicated below. Instructions for formatting the written response to this section are found in RFP Section 2 Preparing and Submitting a Proposal.

Include all requested documents at the end of the section in your Proposal that corresponds to the RFP Section in which the document is requested. Label the document provided with the section number it applies to.

You (Proposer) must be able to perform Services according to the requirements contained in this RFP.

You must provide sufficient detail for the evaluation committee and the Department to understand how your organization will comply with each requirement. If you believe your organization’s qualifications go beyond the minimum requirements or add value, indicate those capabilities in the appropriate section of your Proposal. **Associated costs should ONLY be listed in the Cost Proposal. Do not include cost/pricing information in any other section of your Proposal.**

## **1. Specific IT Audit and Consulting Approach**

Provide a work plan for the performance of the Services for each audit and consulting engagement listed in RFP Sections 5.1.A and 5.1.B, including an explanation of your audit and consulting methodology to be followed. In developing the work plan, include a breakdown of major segments of the audit and consulting services, and hours for each team member.

At a minimum, provide the following information in the work plan:

1. **Summary:** State the overall approach to meeting the objectives and satisfying the scope of work to be performed, sequence of activities, and a description of methodology or techniques to be used. Include the approach to be taken to gain and document an understanding of the Department’s IT internal control structure.
2. **Program Schedule:** Provide projected milestones or benchmarks for completing the FY25 and FY26 projects (to include reports) within the total time allowed.
3. **Project Organization:** Describe the proposed management structure, program monitoring procedures, and organization of the proposed team. Provide a statement detailing Proposer’s approach to the project, specifically address the Proposer’s ability and willingness to commit and maintain staffing to successfully complete the project on the proposed schedule for FY25 and FY26.
4. **Assigned Contractor Personnel** – Provide the following information about the Contractor staff to be assigned to the project:
5. List all key personnel assigned to the project by level, name, and location. Provide a resume or similar statement describing the background, qualifications and experience of the lead person and all persons assigned to the project.
6. Provide a statement of education and training programs provided to, or required of, the staff identified for participation in the project, particularly with reference to management consulting, governmental practices and procedures, and technical matters.
7. Provide a summary of the Proposer’s general qualifications to meet required qualifications and provide the Services.
8. **Planned Use of Audit Software Programs:** Describe the Proposer’s system(s) or approach to document project findings and artifacts.
9. **Department Personnel** – Provide a summary and profile of the type of Department resources you expect to interface with during the engagements.

## **2. Qualifications**

a. Provide a statement of your firm’s background and related experience in performing services similar to those listed in the RFP in the past five years for clients, preferably, governmental, insurance or pension organizations, including technical capabilities and approach. At a minimum, provide the following information in the response:

1. Evidence of how your firm has successfully conducted similar contractual audit and consulting services. Include a description of the services provided and the size and type of client the services were provided for.
2. A description of how the services were provided successfully (or otherwise) according to project objectives, timelines and within the allocated budget, and any other positive effects.
3. A description of any standardized or repeatable service delivery methods and capabilities learned in providing the services.

b. Describe your firm’s approach to service delivery management and working relationships with clients and other providers in the client's service ecosystem.

c. Provide a summary of your firm’s service delivery methodologies and adherence to industry standards related to IT auditing.

d. Provide work samples or artifacts your firm has developed for similar engagements commonly associated with the types of services described in this RFP. You are encouraged to include example report formats or templates exclusive of any confidential or proprietary information which should be redacted.

## **3. Conflict of Interest**

Address possible conflicts of interest your firm may have with other clients should you be awarded a Contract.

## **4. Engagement Issues**

Describe your firm’s approach to resolve any audit engagement difficulties. Identify and describe any anticipated difficulties in performing audits for the Department.

## **5. Additional Work**

The Department and the Contractor may agree on additional Services not specified in the RFP. Examples of additional work may include a Risk Assessment Update for Audit Planning, Project Management, Bug Bounty Program development, and Cloud Services Review. These services will not be included in the initial Contract, however, the ability of the Contractor to perform these services will be a factor in the Contractor selection process. Describe your firm’s capabilities and experience in providing the services described in RFP Section 5.

The Department will provide written requirements for any additional work requested. A project plan must be reviewed and approved in writing by the Department and the Contractor prior to the Contractor commencing any additional work.

# **6. Information Technology**

6.1 Describe in detail the computer and data processing facilities, IT applications and/or IT Technologies you will use to process and deliver data results as part of the audit process.

6.2 Describe if/how your system (related to the provision of Services) will integrate with other public cloud solutions, including where your organization will host the Services, such as:

a. If your organization is headquartered in the US provide state of incorporation.

b. If your organization is headquartered outside the US provide country of incorporation.

c. For your organization and all vendors and Subcontractors you intend to use, provide the location of all cloud infrastructure where Department data will be stored, processed, transmitted that is located outside of the contiguous US (this excludes Hawaii, Alaska and US Territories).

d. For your organization and all vendors and Subcontractors you intend to use for this engagement, provide all locations outside the contiguous US where employees/vendors/ Subcontractors will have access to Department data.

6.3 Provide policies or other documentation that demonstrate your firm’s compliance with the storage and transfer of data that is protected by federal, state, or private-sector regulations.

## **7. Computer And Data Processing Facilities, Data Policies**

7.1 Provide your organization’s policies/guidelines related to security/privacy (e.g., annual training, confidentiality agreement, privacy policy).

7.2 Describe in detail the measures your organizations uses to protect the security and privacy of records, forms, and data processing operations.

7.3 Describe internal controls that are in place to reduce loss of data, records, forms, and data processing operations that may occur through fraud, negligence, incompetence, or system errors. Include information about the physical security measures you use to control access to your organization’s systems.

7.4 Provide data retention procedures/policies for client data evidencing that retention is in accordance with federal and state laws and regulations.

7.5 Describe what software applications and supporting platform will be used to secure Department records and data. Provide information on how information is secured in transit and at rest.

7.6 List all current IT and IT Security certificates your organization may hold and provide current copies of those certifications.

## **8. Information Security**

8.1 Does your organization have limited administrative / elevated rights to only those technology personnel with the need to maintain your systems based upon the principle of least privilege and supported through technical controls?

8.2 Does your organization logically segregate a client’s data from other clients’ data?

8.3 Can client data be deleted upon request?

8.4 Does your organization utilize a centralized log management system that alerts appropriate staff when an incident occurs?