**Appendix 2**

**TECHNICAL QUESTIONNAIRE**

**RFP ETI0049**

**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 2.4 Proposal Organization and Format.

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.

The Proposer must be able to perform Services according to the requirements contained in this RFP.

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

**1.0 Services and Deliverables Required**

The Department’s Office of Internal Audit (OIA) is seeking information technology (IT) auditing services in the areas of information security, IT organizational effectiveness, legacy application support and business continuity management. The Contractor shall objectively and systematically examine the Department’s IT systems (hardware and software) and procedures to provide an independent assessment. The Contractor shall use its judgment, experience and creativity in conducting these IT audits.

**The Department is seeking to outsource the following IT audit and non-audit consulting, advisory and review services:**

**A. Audits in FY20 (July 1, 2019 – June 30, 2020):**

1. **IT Governance Assessment** – The Contractor shall review the leadership, organizational structure, processes, policies, and procedures that ensure the Department’s IT department supports and carries out the Department’s IT Strategic Plan and objectives. This review will be performed by evaluating the five domains of IT governance as defined by COBIT 5.
2. **Network Security Assessment** – The Contractor shall conduct an internal and external vulnerability assessment to determine if processes, procedures, and configurations are adequately designed and implemented to provide reasonable protection against malicious attacks.
3. **IT General Controls** – The Contractor shall confirm the operating effectiveness of the Department’s IT general controls for a sample of applications related to security, change management / system development, batch scheduling, and backup and recovery.

**B. Audits in FY21 (July 1, 2020-June 30, 2021), FY22 (July 1, 2021-June 30, 2022), FY23 (July 1, 2022-June 30, 2023):**

1. **Vulnerability Management Program** – The Contractor shall evaluate the design of the agency’s vulnerability management strategy and review policies and procedures relating to vulnerability management.
2. **Social Engineering Assessment** – The Contractor shall conduct a social engineering exercise to review and assess staff security awareness and ability to withstand social engineering attacks. The objective of this testing is to obtain information that should not be disclosed and that could facilitate gaining unauthorized access to confidential data. This will include an electronic social engineering assessment and a physical security social engineering assessment.
3. **Breach Response Readiness Audit** – The Contractor shall evaluate the processes in place to react to a data breach or security incident including reviewing policy and mechanisms for detection and reporting of security incidents, determining if organizational structure/governance is appropriate for incident response, reviewing the breach response plan for appropriate steps regarding incident containment, eradication, recovery and follow-up.
4. **Business Continuity/Disaster Recovery Audit –** Evaluate the Department’s existing Business Continuity Plan and Disaster Recovery Plan to determine the Department’s preparedness for system outages. This will include business impact analyses, the Department’s training process, review of defined response plans, and review of recent testing results.
5. **NIST CSF Maturity Assessment** – The Contractor shall evaluate the information security environment (i.e., policies, processes, procedures, tools and organizational structure) against the five functions and corresponding categories/subcategories of the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST).
6. **IT Vendor Management** – The Contractor shall evaluate the existing vendor management processes including due diligence, security, contract review, financial stability, and contract compliance. Additionally, the Contractor shall provide an assessment of the quality of and the ability to rely upon the Contractor’s attestations regarding internal controls.
7. **IT Interfaces** – The Contractor shall evaluate the controls between interfaces to confirm that data transmissions are complete and accurate. The audit will focus on reviewing interface documentation, data transmissions, completeness and accuracy validation, and monitoring.

**C. Non-audit consulting, advisory and review services in FY20:**

1. **Systems Development Lifecycle (SDLC) Review** – The Contractor shall evaluate whether the Department’s System Development Life Cycle (SDLC) methodology is followed and sound project management and change management disciplines are utilized and validate the sample system to determine if it is designed with appropriate internal controls for requirements, design, implementation, code, test, deploy, etc.
2. **Endpoint Imaging Review** – The Contractor shall consult on the Department’s process and controls that comprise the desktop imaging process, including but not limited to, reviewing hardening standards, patching, change management process and third-party involvement.
3. **Data Management Review** – The Contractor shall consult on the process and controls regarding the Department’s data management plan. The Contractor shall review the Department’s overall data strategy and supporting processes and controls for data inventory, data inputs, edit checks, data quality and data interfaces between a sample of in-scope systems.

**D. Non-audit consulting, advisory and review services in FY21, FY22, FY23:**

1. **System Implementation Review** – The Contractor shall consult on the ongoing implementation activities for the Department’s legacy application replacement. OIA will confirm key stakeholder involvement. This review will focus on the Department’s adherence to project management principles, defined project milestones, comprehensive business requirements, user acceptance testing, ongoing monitoring of key project metrics and other key organizational considerations.
2. **Data Loss Prevention Review** – The Contractor shall identify where sensitive data is located on the network and when transmitted outside of the organization. The Contractor shall determine how sensitive data is controlled and leverage automated scanning tools to assist in confirming the location and transmission of sensitive data and determine if current-state configurations and processes are designed and implemented to effectively manage risks associated with data transfer/data transmission.
3. **Data Privacy Review** – The Contractor shall consult if policies, operating procedures, and controls are in place and operating effectively to protect sensitive information.
4. **Identity Access Management (IAM) Review** – The Contractor shall consult on the Department’s current state and plans for its identity access management program including management’s policies, procedures and governance activities. Additionally, the Contractor shall consult on the existing setup of roles in the Department’s applications to be determined at the time of the audit and identify per discussion and per review of the system any separation of duty (SoD) conflicts and mitigating controls.
5. **eDiscovery Program Review** – The Contractor shall consult on the Department’s preservation and disposition processes with a focus on establishing a litigation hold, preservation of documents and artifacts, removal of litigation holds; and communication and administration of the litigation hold portfolio.
6. **Records Management Review** – The Contractor shall consult on the Department’s existing record retention process and confirm any regulatory requirements for retaining or removing data. The Contractor shall perform a gap analysis of the Department’s current process versus regulatory record retention requirements. For the gaps identified, the Contractor shall identify remediation plans and work with Department management to get these implemented.

**1.1 Timing, Location and Conduct of Audit Work**

Audit work will be conducted at the Department’s headquarters at mutually agreeable times, follow up may be conducted remotely. The Department will provide laptops and network/systems access for Contractor’s auditors.

**1.2 Project Deliverables**

**For each project agreed to by the Contractor and the Department in a signed statement of work, the Department requires the Contractor to deliver the following:**

**Project Plan**: A project plan for each engagement, including objective, scope of work, project staffing, approach for the engagement, estimated timeline of key milestones, such as planning, fieldwork and reporting, as well as estimated hours by staff level, must be prepared and approved by the OIA Director before work is initiated. Project plans will be incorporated into the statements of work for each engagement.

**Workpaper:** The quality of Contractor’s workpapers must be in compliance with the Institute of Internal Auditors International Standards for the Professional Practice of Internal Auditing and made available to the Department upon the Department’s request.

**Report: Contractor’s a**udit and consulting reports shall be provided to the Department on the dates specified in the project plan. Any changes to the specified dates must have prior written approval by the OIA Director. Reports must be submitted in a format approved by the OIA Director.

**Presentation:** Key Contractor engagement staff shall present engagement results to the Board Audit Committee or Board, or both as requested. Contractor shall participate in exit conferences with the Department’s management team to discuss engagement results prior to attending the Board Audit Committee meetings.

**1.3 Acceptance Criteria**

## The Department’s evaluation and acceptance criteria of the aforementioned deliverables shall include but not be limit to completeness, accuracy, and quality of the deliverable. Acceptance criteria will be specified in the statement of work for each specific engagement as needed.

**1.4 Changes to Engagement**

**Changes with no impact on cost and/or timeline:** Any changes to the engagement requirements that have no impact on either the cost or the timeline must be mutually agreed upon by the Department and the Contractor and shall be documented by e-mail or other written means between the OIA Director and the Contractor.

**Changes with impact on cost and/or timeline:** Any changes to the engagement requirements that have impact on cost, either an increase or a decrease, or alter the timeline for any deliverables will require the following:

1. A new or revised statement of work setting forth the requirements of the proposed changes
2. A written summary of the facts that led to the decision
3. An impact analysis on related tasks, budget, and the overall Services to be delivered by the Contractor
4. Approval signature from the Department and the Contractor

Costs not included in the agreed upon engagement project plan or statement of work signed by the Department and the Contractor through the above process shall not be eligible for reimbursement.

**2.0 Questionnaire**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **2.1** | **FY20 Project Timeline**  The following is the Department’s proposed IT audit schedule and associated tasks for fiscal year 2020 (July 1, 2019-June 30, 2020):   |  |  | | --- | --- | | **Date** | **Event** | | October 1, 2019 | Estimated Contract start Date | | October 1-October 15, 2019 | Preplanning Work and Vendor Onboarding | | October 16, 2019 - June, 2020 | Complete the FY2020 engagements defined in the FY2020-FY2021 biennial audit plan.  Finalize engagement reports after consultation with the Department and present the final reports to the ETF Board Audit Committee at the March 2020 and June 2020 Audit Committee meetings. The Department and the Contractor will jointly determine the timeline for completion of Services.  Conduct 3 Audits and prepare deliverables:   * IT Governance Assessment * Network Security Assessment * IT General Controls   Conduct 3 Non-Audit Consulting, Advisory and Review Services:   * Systems Development Lifecycle (SDLC) Review * Endpoint Imaging Review * Data Management Review | |  | The schedule for audits and consulting work planned for FY21 and beyond will be jointly determined by the Department and the Contractor, included in a statement of work signed by both parties, and appended to the Contract. | |
| **2.2** | **Specific IT Audit and Consulting Approach**  Provide a work plan for the performance of the Services for each audit and consulting engagement identified in Section 2.6.1 above for FY20, including an explanation of the Proposer’s audit and consulting methodology to be followed. In developing the work plan, include a breakdown of major segments of the audit, consulting 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 FY20 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 FY20. 4. **Assigned Contractor Personnel** – Provide the following information about the Contractor staff to be assigned to the project:  * 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. * 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. * Provide a summary of the Proposer’s general qualifications to meet required qualifications and provide the Services.  1. **Planned Use of Audit Software Programs:** Describe the Proposer’s system(s) or approach to document project findings and artifacts. 2. **Department Personnel** – Provide a summary and profile of the type of Department resources you expect to interface with during the engagements. |
| **2.3** | **Qualifications**  i) Provide a statement of the Proposer’s background and related experience in performing services similar to those listed in Section 1.0 A-D above in the past five years for Proposer’s 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 Proposer 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. .   ii) Describe Proposer’s approach to service delivery management and working relationships with clients and other providers in the client's service ecosystem.  iii) Provide a summary of Proposer’s service delivery methodologies and adherence to industry standards related to IT auditing.  iv) Provide work samples or artifacts Proposer has developed for similar engagements commonly associated with the types of services described in this RFP. Proposer is encouraged to include example report formats or templates exclusive of any confidential or proprietary information which should be redacted. |
| **2.4** | **References**  Using FORM F – Vendor References, provide a minimum of four references for engagements the Proposer has performed during the last five years that demonstrate the Proposer’s ability to successfully complete engagements similar to those described in this RFP. Include the name of the reference’s organization, the contact name, title, telephone number, and engagement title/type of services provided for all references listed. |
| **2.5** | **Conflict of Interest**  Address possible conflicts of interest with other Proposer clients should Proposer be awarded a Contract. |
| **2.6** | **Engagement Issues**  Describe Proposer’s approach to resolve any audit engagement difficulties. Identify and describe any anticipated difficulties in performing audits for the Department. |
| **2.7** | **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, Business Intelligence, and Cloud Computing. 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 Proposer’s capabilities and experience in providing each of the above named services.  ETF will provide written requirements for any additional work needed. A project plan as described in Section 1.2 above, must be reviewed and approved by the OIA Director prior to the Contractor commencing any additional work. |