|  |
| --- |
| **STATEMENT OF REQUIREMENTS (SOR)** **SOR # VDH-240118-01-CAI**  ***(2024 VDH IT Security Audits)*** |

1. **Date:** January 18, 2024
2. **Authorized User**: Virginia Department of Health (VDH)
3. **Authorized User Contact Information:**

Tasha Owens

Internal Audit Director

Virginia Department of Health

109 Governor Street, Room 1021

Richmond, VA 23219

Phone: 804-864-7450

Email: [tasha.owens@vdh.virginia.gov](mailto:tasha.owens@vdh.virginia.gov)

1. **Solicitation Schedule:**

|  |  |
| --- | --- |
| **Event** | **Date** |
| Release SOR | 1/19/2024 |
| Supplier Response Due | 2/1/2024 |
| Award Decision | 2/2/2024 |
| Estimated Project Start Date | 2/9/2024 |

PLEASE NOTE: ALL questions related to this SOR should be directed to the CAI Account Manager. Suppliers may NOT contact the Authorized User.

1. **Evaluation and Scoring**

Supplier’s Response must be submitted in the specified Statement of Work (SOW) format and will be evaluated for format compliance.

Supplier’s Response will be evaluated for technical merit based on its appropriateness to the performance of Authorized User’s requirements, its applicability to the environment, and its effective utilization of Supplier and Authorized User’s resources.

Supplier’s Response will also be evaluated for the extent to which it demonstrates:

* An in-depth understanding of Commonwealth of Virginia (COV) Information Security Standards including IT Security Standards (SEC530), and IT Security Audit Standard (SEC502).
* An understanding of the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 - Recommended Security Controls for Federal Information Systems and Organizations
* Previous experience auditing IT security and compliance with commonwealth IT Security Standards at COV agencies.
* Ability to perform IT audits in accordance with the Generally Accepted Government Auditing Standards (Yellow Book) evidenced by a current, independent Quality Assurance/Peer Review report with an overall opinion of “generally conforms.” Suppliers responding to this SOR should provide this report with their SOW.

1. **Project/Service:**

2024 VDH IT Security Audits

1. **Specialty Area** (Check one)**:**

|  |  |
| --- | --- |
| Application Development | Information Security |
| Business Continuity Planning | IT Infrastructure |
| Business Intelligence | IT Strategic Planning |
| Business Process Reengineering | Project Management |
| Enterprise Architecture | Public Safety Communications |
| Enterprise Content Management | Radio Engineering Services |
| Back Office Solutions | IV&V Services |
| Geographical Information Systems |  |

1. **Contract Type:** Fixed Price, Deliverable-based
2. **Introduction:**

Virginia Department of Health (VDH)’s mission is to protect the health and promote the well-being of all people in Virginia with the vision of becoming the healthiest state in the nation.

VDH consists of the Central Office located in Richmond, VA with five (5) Regional Districts and a total of 35 local health districts located within the five regions.

Project History

VDH has about 45 sensitive critical systems and a Fiscal Year 2023 and Fiscal Year 2024 IT Audit Plan on file with VITA/Commonwealth Security and Risk Management (CSRM). VDH wants to ensure compliance with the current versions of the COV’s IT Security Standards (SEC530) as well as ensure compliance with COV’s IT Security IT Audit Standards (SEC502). The Commonwealth of Virginia’s Information Security Standard, SEC 530 (Security Standard) adopts the Information System Security Control Families (families) from the National Institute of Standards and Technology (NIST). The Security Standard uses these families to organize the controls that the Commonwealth is required to apply to its information systems.

According to NIST, a family “contains security controls related to the general security topic of the family. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems and devices.”

Business Need

The Office of Internal Audit’s IT Department, VDH Office of Internal Audit requires auditing of its systems in accordance with the FY24 IT Audit Plan on file with VITA.

The systems in scope for this SOR are:

* OEPI – ELR Database (ELR)
* OEPI – HIV Counseling, Testing & Referral (HIV-CTR)
* OEPI – VASE/VASE+
* OFHS – Care Connection for Children System Users Network (CCC-SUN) – if time permits

The data owners, system owners, and VDH’s Office of Compliance and Security have identified these systems as sensitive. As such, the Commonwealth’s IT Security Standard requires a SEC530 IT Security Compliance audit once every three years.

VDH requires final audit deliverables by June 30, 2024.

Project Complexity

Project complexity and risk are assessed as moderate.

Project Management and Organizational Structure

VDH Internal Audit Director will be the lead for this effort. The Supplier will provide deliverables to the Audit Director.

1. **Scope of Work:**

This SOR defines the services required by Authorized User in support of the Project/Service. In connection with the Services, the Supplier will perform the following tasks in the course of the audit:

A. IT Security Audit Process

1. Perform the IT Security Audit in a manner to comply with the American Institute of Certified Public Accountants (AICPA) Standard for Consulting Services as it relates to this specific IT Security Audit activity, such that general work processes, documentation standards, work paper formats, and report contents are required to comply with the above professional standards.
2. The Supplier will provide evidence of most recently completed external peer review that demonstrates general compliance with auditing standards.
3. Work directly with Authorized User staff to collect the information necessary to complete the IT Security Audit. For tracking and reporting of audit requests, maintain a list of items requested from Authorized User with item description, date requested, name of requestor, name of responsible Authorized User staff, due date agreed to, date received, and additional comments.
4. Conduct an entrance conference with appropriate Authorized User management to discuss IT Security Audit scope, limitations, expectations, and timeframes.
5. Compile a list of findings including the IT Security Audit Program step number, number, and title of the audit point in the IT Security Audit report in which the finding is included, a description of the finding, and the control number tested.
6. Prepare and provide a draft IT Security Audit report to Authorized User. Detailed findings may be grouped into a higher-level audit point in the report if they share a common subject. Audit points must include easily identifiable elements of a finding: condition, criteria, cause, effect, and recommendation.
7. Schedule and hold an exit conference with Authorized User management to present the draft IT Security Audit report. Within 10 business days after providing the draft report, meet with Authorized User staff responsible for corrective actions to discuss the draft report and findings and to obtain a written corrective action plan with responsible parties and estimated date of completion for inclusion in the final report.
8. Complete and submit the final report to Authorized User.

B. Approach

1. IT Security Audit Program: Supplier should develop an IT Security Audit Program for review and approval by Authorized User. The approved program will become the scope document and supersede any scoping in this document. The program should include a planning phase, which will be used to perform discovery of systems and devices in scope and subsequently, the development or updating of the Test Plan. If discovery identifies additional scope information that changes the Supplier’s SOW and any subsequent Change Orders are required, they will supersede this document as the agreed upon scope.
2. Control Frameworks:
   * VITA IT Security Standard SEC 530 should be used as the guideline for this IT Security Audit.
   * Only application specific controls from SEC 530 be considered in the scope. Agency level IT General Controls will not be included in the scope.
3. Period of Scope: From July 1, 2023 to June 30, 2024
4. Population Sampling: It is expected that the Supplier should perform IT Security Audit procedures based on a minimum of the lesser of 10% or 30 items sampling approach and therefore, 100% of the population should not be expected to be tested. For example, if 50 servers are within the overall scope, Supplier may sample 10% of servers to perform testing.
5. Control Testing Methods: Testing should confirm the design of controls in place. Supplier may perform the following activities to evaluate IT security controls: interviews, observation of control activities, inspection of control evidence. inspection of policies and procedures, and utilize automated testing tools to verify technical information.
6. **Period of Performance:**

Delivery of all products and services defined in the Statement of Work will occur within 5 months of project execution date and must be completed by June 30, 2024.

1. **Place of Performance** (Check one)**:**

Authorized User’s Location

Supplier’s Location

Authorized User’s and/or

Supplier’s Location

Some of this work can be performed off-site; however, space will be available at Authorized User’s office.

1. **Project Staffing**
2. **Supplier Personnel** (Check One)**:**

The roles listed in the table below represent the minimum Supplier personnel requirements for this engagement. The Supplier shall provide resumes for all proposed personnel.

The selected personnel should be independent in attitude and appearance in all matters related to the audit. In addition, the auditor should be organizationally independent of the area being audited. The selected personnel will ensure that the audit results are supported by work papers with sufficient, competent evidential matter to support the report conclusion. The final report should include a description of the work that was performed and audit results.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Key Personnel (Y/N)** | **Years of Experience** | **Certifications (any of the below)** | **References Required (Y/N)** |
| IT Security Audit Mgr | Y | 4-8 | CISA, CRISC, CISSP, & CISM | Y |
| IT Security Auditor | Y | 2-4 | CISA, CRISC, CISSP, & CISM | Y |

Supplier shall propose the roles and skillsets of the resources needed to deliver the scope of work as defined in this SOR. Supplier shall provide resumes for all proposed personnel.

PLEASE NOTE: The use of offshore resources for any SOW is prohibited.

1. **Authorized User Staff**

The roles listed in the table below represent Authorized User’s staff and the estimated time each will be available to work on the project.

|  |  |  |
| --- | --- | --- |
| **Role** | **Description** | **% Project Availability** |
| VDH Internal Audit Director | POC for the engagement. | As required. |
| VDH Chief Information Security Officer | Primary contact for audit information requests. | As required. |
| Risk and Review Analyst | Contact for audit information requests | 12 |
| VDH System Owners | Contact for audit information requests | 8 |
| Data Owner | Contact for audit information requests | 8 |

1. **Milestones and Deliverables:**

The minimum required milestones and deliverables, and the estimated completion date for each deliverable, are listed in the following table. Some aspects of each of the audits may be performed simultaneously to ensure completion of all audit work by June 30, 2024.

| **#** | **Milestone**  **Event(s)** | **Deliverable(s)** | **Estimated Completion Date** |
| --- | --- | --- | --- |
| 1 | Project Initiation | Project Plan  Entrance conference agenda.  Develop project plan, audit scope, limitations, expectations, and timeframes with VDH management and staff involved with the system under audit. Documentation of the entrance meeting date, time, attendees, and summary of the discussion. | Supplier to propose dates |
| 2 | Audit Scope Program/Procedures | Documentation Requests: Submit a comprehensive audit evidence request list for distribution to key VDH personnel with the understanding that follow-up questions may arise.  Submit IT audit procedures/program for review and approval by VDH Project Stakeholder. | Supplier to propose dates |
| 3 | Conduct IT Audit Fieldwork | Execute IT audit procedures to perform an IT Security Audit for SEC530 for **each** of the systems listed in Section 9, as approved by client. | Supplier to propose dates |
| 4 | Detailed audit findings | Provide briefing/ detailed list of failed controls including the audit program step number, a description of the finding, and the SEC530 control number tested. | Supplier to propose dates |
| 5 | Draft Audit Report | Submit a draft audit report detailing the background of the system and audit, scope of the audit work, findings (including the 5 elements of a finding), recommendations, and overall conclusion/ opinion. | Supplier to propose dates |
| 6 | Exit Conference | Exit conference agenda.  Review (at VDH location or remotely) audit results, findings, recommendations, and conclusions to objectives with VDH management and staff involved with the system under audit. Documentation of the exit meeting date, time, attendees, and summary of the discussion. | Supplier to propose dates |
| 7 | Final Audit Report | Submit a final audit report for each audit listed in Section 9 that incorporates VDH management responses and corrective action plans. | Supplier to propose dates |
| 8 | Audit Work Papers | Provide an editable (unlocked) electronic copy of all audit work papers and evidence used to complete the audits. | Supplier to propose dates |

The Supplier should provide all deliverables in electronic form, using the following software standards (or lower convertible versions):

|  |  |
| --- | --- |
| **Deliverable Type** | **Format** |
| Reports and Audit Documentation | Microsoft Office Products |

1. **Travel Expenses** (Check one)**:**

Supplier travel expenses, if required, must be included in the total fixed price of the solution

1. **Payment** (Check all that apply)**:**

Payment made based on successful completion and acceptance of deliverables

All payments, except final payment, are subject to a 10% holdback

1. **Acceptance Criteria:**

The Project Manager will have 10 business days from receipt of the deliverable to provide Supplier with the signed acceptance receipt.

Final acceptance of services provided under the SOW will be based upon (Check one):

User Acceptance Test

Acceptance Criteria for this solution will be based on a User Acceptance Test (UAT) designed by Supplier and accepted by Authorized User. The UAT will ensure that all the functionality required for the solution has been delivered. The Supplier will provide the Authorized User with a detailed test plan and acceptance checklist based on the mutually agreed upon UAT plan. This UAT plan checklist will be incorporated into the SOW.

Final Report

Acceptance criteria for this solution will be based on a final report. In the SOW, Supplier and Authorized User will agree on the format and content of the report to be provided to Authorized User for final acceptance.

Other (specify): Acceptance criteria shall include that the deliverable (i) is in a format and has, minimally, the content required by the Authorized User, (ii) satisfies all associated requirements; and (iii) accomplishes the purpose(s) for which the deliverable is intended. Additional acceptance criteria may be added as determined by the Authorized User.

1. **Project Roles and Responsibilities:**

| **Responsibility Matrix** | **Supplier** | **Authorized User** |
| --- | --- | --- |
| Network Connectivity (i.e. VPN, Email, Active Directory) | ✓ | ✓ |
| Meeting space and other resources as needed |  | ✓ |
| Provide project management oversight |  | ✓ |
| Parking |  | ✓ |
| Review audit plan, work papers and final report |  | ✓ |
| Prepare audit plan and scope, conduct audit fieldwork, provide documentation of testing of controls, and other audit work papers. | ✓ |  |
| Prepare status reports, audit related meetings, draft audit report and final audit report. | ✓ |  |
| Provide access to VMS Software to facilitate deliverable / milestone submissions and approvals | ü |  |
| Monitor milestone / deliverable submission schedule | ü |  |
| Subcontractor onboarding | ü |  |
| Facilitate invoicing to Authorized User and payment to Subcontractor | ü |  |
| Escalate issues with 24 hours | ü | ü |

1. **Criminal Background Checks and Other Security Requirements (**Check all that are required):

Standard CAI Required Background Check

Agency Specific Background Check – FBI fingerprinting

1. **Performance Bond** (Check one)**:**

Required for *(XXX)*% of the SOW value

Not Required

1. **Reporting** (Check all that are required):

**Weekly Status Update**

The weekly status report, to be submitted by Supplier to Authorized User, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

**Other(s)** (Specify)

1. **Federal Funds** (Check one):

Project will be funded with federal grant money

No federal funds will be used for this project

1. **Training and Documentation:**
2. **Training is:**

Required as specified below

Not Required – except as indicated in item number 25.a, Additional Terms and Conditions.

1. **Documentation is:**

Required as specified below

Not Required

Documentation Requirements: As outlined in Section 14. Milestones and Deliverables.

1. **Instructions Regarding Freedom of Information Act and Public Availability/Inspection of Records**

Authorized User reserves the right to use, copy, and reproduce all submitted documents, data, and other information in any manner Authorized User may deem appropriate in evaluating the fitness of the solution(s) proposed, and in complying with applicable law. All data, materials, and documentation originated and prepared for Authorized User shall be subject to public inspection in accordance with the *Virginia Freedom of Information Act*.

Consistent with the Code of Virginia, Authorized User will, as permitted by law, hold confidential trade secrets or proprietary information that is submitted by a Supplier in connection with the transaction contemplated by this SOR if the Supplier, to Authorized User’s satisfaction:

1. invokes the protections of the Code of Virginia in writing prior to or upon submission of the data or other materials,
2. identifies specifically the data or other materials to be protected, and
3. states the reasons why protection is necessary.

**FAILURE TO COMPLY WILL RESULT IN THE DATA OR OTHER MATERIALS BEING RELEASED TO SUPPLIERS OR THE PUBLIC AS PROVIDED FOR IN THE VIRGINIA FREEDOM OF INFORMATION ACT.**

The Supplier will use this form to identify the information that they deem trade secrets or proprietary information. T**he designation of an entire proposal or SOR as proprietary or trade secret is not acceptable, and pricing may not be designated as a trade secret or proprietary information.**

**Supplier Trade Secrets / Proprietary Information Designations Table**

| **SOR/Other Document** | **Section/Page** | **Trade Secret / Proprietary Information** | **Reason** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **Additional Terms and Conditions:**

The services to be provided are subject to the following additional provisions:

1. Effective July 1, 2020, the Code of Virginia requires contractors with the Commonwealth who spend significant time working with or in close proximity to state employees to complete sexual harassment training.  As a result of the new code, VITA and the Department of Human Resource Management (DHRM) are requiring that all contractors working through the CAI contract complete DHRM's "Preventing Sexual Harassment" training.  This training is available as either a short video or a written transcript on the DHRM website: <https://www.dhrm.virginia.gov/public-interest/contractor-sexual-harassment-training>. The selected Supplier must agree that any assigned resource will complete the training.
2. The selected Supplier must agree that any assigned resource will review and conform to the IT Contingent Labor Program (ITCL) Contractor Code of Conduct. The Code of Conduct can be reviewed on VITA’s website at the following link:

<https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/Contingent-Worker-Code-of-Conduct.pdf>

1. **Scheduled Work Hours:**

Authorized User is operational Monday through Friday during the business hours of 8am to 5pm (except state holidays).

1. **Facility and equipment to be provided by Authorized User:**

Provided by VDH:

* Visitor badge access to the building and work area
* Temporary guest wireless internet access upon request
* Work area (office/cube and desk) upon request
* Parking Central Office provided
* Access to all VDH Sensitive System related information, including, but not limited to, technical documentation and project status and financial data and to project and contractor personnel for information related to the project.
* Furniture and equipment within workspace on a temporary basis. Permanent office space, furniture and equipment are the responsibility of the Supplier. While on-site at the project location(s), the Authorized User will provide access to a copier, the agency LAN and the internet. Authorized User will also provide temporary desk/cubicle space.

Not provided by VDH:

* Desktop/laptop computer
* Office Supplies
* Phone
* The Supplier must provide any cell phones, personal computers or laptops required by their Team. The VITA technical staff supporting the agency’s network must verify that any personal computers or laptops meet minimum-security configuration standards (e.g., current virus protection) before any equipment may be connected to the agency’s LAN.