Contract Number *(VA-210625-CAI)*

Contents

[**STATEMENT OF REQUIREMENTS (SOR)** 2](#_Toc283151016)

[**STATEMENT OF REQUIREMENTS TEMPLATE INSTRUCTIONS** 9](#_Toc283151017)

|  |
| --- |
| **STATEMENT OF REQUIREMENTS (SOR)** **SOR # SCC-241004-01-CAI**  ***SCC Information Security Assessment*** |

1. **Date:** October 4, 2024
2. **Authorized User**: State Corporation Commission
3. **Authorized User Contact Information:**

Amanda Nies-Berger, Manager, Strategic Sourcing

1300 E Main Street

Richmond, VA 23219

Phone: 804.371.2123

E-mail: amanda.nies-berger@scc.virginia.gov

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

1. **Solicitation Schedule:**

|  |  |
| --- | --- |
| **Event** | **Date** |
| Release SOR | 10/08/2024 |
| Supplier Questions Due to CAI | 10/14/2024 |
| Authorized User Responds to Questions | 10/17/2024 |
| Supplier Response Due | 10/31/2024 |
| Clarification Session  Award Decision | 11/19/2024  12/16/2024 |
| Estimated Project Start Date | 01/06/2024 |

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.

1. **Project/Service:**

Information Security Assessment

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:**

Project History

The Virginia State Corporation Commission (SCC) has an Office of Information Security (OIS) that reports to the Chief Administrative Officer. The SCC-OIS is responsible for securing the agency IT assets, and protecting, ensuring confidentiality and integrity, and controlling access to SCC data in compliance with internal and external system security policies and procedures.

The OIS is staffed with eleven members that have various OIS responsibilities as assigned by the OIS Chief Information Security Officer.

The SCC IT environment includes on-prem and cloud computing, personal computing assets, supporting over 60 applications developed and maintained in-house or by application supplier partners.

Business Need

The SCC is interested in a complete assessment of the current OIS organizational structure, applicable policies and procedures, and compliance with established policies and procedures

The SCC expects the successful supplier to provide its opinion of the SCC’s information security posture identifying those activities, services, implemented policies, procedures and processes that are best practices and identify areas where improvements should be made with recommendations.

Project Complexity

Information security is a complex area within any organization. The successful supplier will be interacting with SCC staff, reviewing documentation, understanding the current SCC information security environment, and other assessment activities as the supplier determines necessary.

1. **Scope of Work:**

This SOR defines the services required by Authorized User in support of the Project/Service.

Supplier shall perform an Information Security assessment which includes the following:

Obtain a list of all Office of Information Security (OIS) policies and standards. Determine if documented policy and standard topics addressed by OIS are considered to be best practices. Identify information security best practice topics not addressed in current polices and standards, if any. Perform a cursory review of the content in each OIS policy and standard and recommend any edits to be made and/or additional security topic content to include.

Trellix SIEM Platform

* Assess Patch Management Compliancy
* Assess capability to perform all System Administrator Roles
* Assess capability to use the tool to perform Incident Management
* Assess capability to use the tool to conduct Forensic Investigations
* Assess that the SIEM is properly configured for prioritized alerts and logging
* Assess that the SIEM is properly tuned to generate usable reports
* Assess the quality of log data collection and reports

Trellix IPS Platform

* Assess Patch Management Compliancy
* Assess capability to perform all System Administrator Roles
* Assess capability to use the tool to perform Incident Management
* Assess capability to use the tool to conduct Forensic Investigations
* Assess that the IPS platform is properly configured for prioritized alerts and logging
* Assess that the IPS platform is properly tuned to generate usable reports

CyberArk

* Assess Patch Management Compliancy
* Assess capability to perform all System Administrator Roles
* Assess capability to use the tool to perform Incident Management
* Assess capability to use the tool to conduct Forensic Investigations
* Assess that the CyberArk platform is properly configured for prioritized alerts and logging
* Assess that the CyberArk platform is properly tuned to generate usable reports

OIS Team Project Management/System Development activities

* Assess ability to guide projects, in collaboration with SCC infrastructure, application, and project management office teams, to deliver needed IT solutions that comply with OIS established policies and standard

OIS Best Practices:

* Assess, as compared to IT industry best practices, the OIS approach to:
  + Security Policy, Process and Procedures development and documentation
    - Are these documented, up to date, implemented, appropriate?
  + Advising Senior SCC Leadership on Information Security strategy for the SCC
  + Advising Senior SCC Leadership on emerging security threats for the SCC and recommendations to defend
* Evaluate OIS Security Incident response procedures
* Interaction/collaboration/coordination between OIS, information technology infrastructure, applications, and project management offices
* Incident Management:
  + Assess capability to effectively use existing SCC security tools and applications to perform Incident Management and quickly resolve security issues.
  + Assess whether there are appropriate personnel resources with the appropriate capabilities available to address various incidents

1. **Period of Performance:**

Delivery of all products and services defined in the Statement of Work will occur within *(4)* months of project execution date.

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

Authorized User’s Location

Supplier’s Location

Authorized User’s and/or

Supplier’s Location (see below explanation) –

Work will likely need to be performed on-site and at the supplier’s location. On-site activities may include interviews with IT or other SCC staff, review of documentation, inventory of SCC computing assets and other activities that require on-site review as determined by the supplier.

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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Technical**  **Skills Required** | **Years of Experience** | **Certifications**  **Required** | **References Required**  **(Y/N)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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** |
| Engagement Manager | Will provide leadership to advance the engagement at the executive level in compliance with the final agreement. | As needed |
| Engagement Project Manager | Will ensure the requirements of the final agreement are met, coordinate between the supplier and SCC resources to set meetings, coordinate documentation transfer, obtain access to systems as authorized, maintain the project schedule. | 100% |
| Subject Matter Resources | Those individuals within the SCC that have any role or interest in the agency’s information security condition. | As needed |

1. **Milestones and Deliverables:**

The minimum required milestones and deliverables, and the estimated completion date for each deliverable, are listed in the following table.

| **#** | **Milestone**  **Event(s)** | **Deliverable(s)** | **Acceptance Criteria** | **Estimated Completion Date** | **Deliverable Payment** |
| --- | --- | --- | --- | --- | --- |
| 1 | Project Kick-off meeting | Meeting presentation | * Supplier schedules and conducts pre-kick off meeting (logistics and customer POC identification) * Supplier schedules and conducts kick-ff meeting | 10 days from final SOR execution |  |
| 2 | Interim findings and recommendations | Report document  Meeting presentation | * Supplier documents interim findings and recommendations for all aspects of assessment * Supplier schedules and leads meeting to present interim findings and recommendations to the SCC for all aspects of assessment * Supplier provides copy of meeting presentation to SCC | 60 days from Project Kick-off |  |
| 3 | Draft final report | Report document  Meeting presentation | * Supplier documents draft findings and recommendations for all aspects of assessment * Supplier schedules and leads meeting to present draft findings and recommendations to the SCC for all aspects of assessment * Supplier provides copy of meeting presentation to SCC * Supplier allows SCC to provide feedback and revisions to draft report | 90 days from Project Kick-off |  |
| 4 | Final report | Report document  Meeting presentation | * Supplier documents final findings and recommendations for all aspects of assessment * Supplier schedules and leads meeting to present final findings and recommendations to the SCC for all aspects of assessment * Supplier provides SCC a copy of meeting presentation to SCC | 120 days from Project Kick-off |  |

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

|  |  |
| --- | --- |
| **Deliverable Type** | **Format** |
|  |  |
|  |  |

1. **Travel Expenses**

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 *(XX)*% holdback

1. **Acceptance Criteria:**

Deliverable Acceptance Process

Each deliverable created under this Statement of Work will be delivered to Authorized User with a Deliverable Acceptance Receipt. This receipt will describe the deliverable and provide the Project Manager with space to indicate if the deliverable is accepted, rejected, or conditionally accepted. Conditionally Accepted deliverables will contain a list of deficiencies that need to be corrected in order for the deliverable to be accepted by the Project Manager. The Authorized User/SCC Designee will have 15 business days from receipt of the deliverable to provide Supplier with the signed Acceptance Receipt.

Acceptance Criteria

The review period for each Deliverable will be 15 business days after delivery. The Supplier will assist SCC as SCC reasonably requires in review and or testing. Prior to the expiration of the applicable review period, SCC will provide the Supplier a written statement indicating acceptance or rejection of the Deliverable. In the event of rejection, SCC will provide reasonable details of the nonconformity If the Supplier fails to deliver any Deliverable by its required delivery date or if any Deliverable is rejected, then SCC may, in its sole discretion exercise any other rights and remedies provided in the master agreement. When submitting each Deliverable, the Deliverable Submission and Review Form must be submitted along with the Deliverable artifact. Supplier will complete the top section “Deliverable Submission Statement” and email both the form and Deliverable artifact to the designated Authorized User personnel by the due date documented within this SOW. Once SCC has reviewed and decisioned the Deliverable, the Deliverable Submission and Review Form will be sent back to Supplier with the bottom section, “Deliverable Review Statement”, completed.

1. **Project Roles and Responsibilities:**

| **Responsibility Matrix** | **Supplier** | **Authorized User** |
| --- | --- | --- |
| Project Management | X |  |
| Meeting Facilitation | X |  |
| Attend meetings as necessary |  | X |
| Provide requested documentation/information | X |  |

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

Standard CAI Required Background Check

Agency Specific Background Check

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

Training Requirements:

None

1. **Documentation is:**

Required as specified below

As specified in SOR paragraph number 14.

Documentation Requirements:

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. **The 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:**

Access to the SCC facility for on-site work will be limited to 830 AM to 4:30 PM, Monday through Friday. No access to the facility on weekends or holidays.

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

Laptop