|  |
| --- |
| **STATEMENT OF REQUIREMENTS (SOR)** **SOR # VITA-240318-01-CAI**  ***VITA State and Local Cybersecurity Grant Program – Cybersecurity Plan Capability Assessment Support*** |

1. **Date:** March 18, 2024
2. **Authorized User**: Virginia Information Technologies Agency (VITA)
3. **Authorized User Contact Information:**

Kelley Kapsak, kelley.kapsak@vita.virginia.gov

1. **Solicitation Schedule:**

|  |  |
| --- | --- |
| **Event** | **Date** |
| Release SOR | April 12, 2024 |
| Supplier Questions Due to CAI | April 19, 2024 |
| Authorized User Responds to Questions | April 24, 2024 |
| Supplier Response Due | May 8, 2024 |
| Award Decision | May 22, 2024 |
| Estimated Project Start Date | June 10, 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 resources. The basis and reasonableness of proposed pricing will also be evaluated.

1. **Project/Service:** State & Local Cybersecurity Grant Program Cybersecurity Plan Capability Assessment Support
2. **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** (Check)**:**

Fixed Price, Deliverable-based

1. **Introduction:**

Project History

VITA and VDEM are administering Virginia’s participation in the State and Local Cybersecurity Grant Program (SLCGP), under which a combination of federal grant money and state-provided matching funds will be used to assist state and local public entities with improving their cybersecurity posture. 80% of the grant fund will be allocated for local public entities and within that 80%, 25% is specifically designated for rural localities (defined by federal law as a population less than 50,000 that has not been designated in the most recent decennial census as an “urbanized area” by the Secretary of Commerce). For further information on the SLCGP generally, see CISA and FEMA's websites:

[State and Local Cybersecurity Grant Program | CISA](https://www.cisa.gov/state-and-local-cybersecurity-grant-program)

[State and Local Cybersecurity Grant Program | FEMA.gov](https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program)

For further information on Virginia’s participation in the SLCGP, see VITA’s website:

[Federal Cybersecurity Grants | Virginia IT Agency](https://www.vita.virginia.gov/information-security/grant-programs/)

The [Virginia Cybersecurity Planning Committee](https://www.vita.virginia.gov/information-security/cyber-awareness/cybersecurity-programs/federal-cybersecurity-grants/virginia-cybersecurity-planning-committee/) has developed a [Virginia Cybersecurity Plan](https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/meetings/2022-Virginia-Cybersecurity-Plan.pdf), which has been approved by the federal government and is a prerequisite for using SLCGP funding. The Plan contains Virginia’s objectives for the program and also identifies a set of priority objectives.

Year one funding is already available to Virginia. The intent is to prioritize localities conducting a needs / gap assessment against the program objectives.

The intent of this SOR is to identify and vet suppliers who will perform a needs / gap assessment of specified locality’s environment resulting in an artifact (the Findings and Recommendations Report described below). The produced artifact is expected to be utilized as a baseline for the locality and as a guide and precursor for determining what cyber security services will be implemented through the SLCGP as further funding uses are approved. VITA reserves the right to make multiple awards as a result of this SOR and our expectation is that at least one hundred five (105) assessments will be completed by one or more suppliers. However this is an estimate, and the actual quantity of assessments awarded may be more or less than those shown.

Authorized User will determine the in-scope localities for assessments before executing any resulting SOW(s).

Business Need

This SOR requires:

* an overall review of a specified locality’s current capabilities as compared to the goals and objectives described in the Virginia Cybersecurity Plan,
* An assessment of the capability level of the organization in its current state and,
* Development of recommended security artifacts to support operationalization of the Virginia Cybersecurity Plan.

**10. Scope of Work:**

This Statement of Requirements (SOR) defines the Cybersecurity Plan Capability Assessment Support required by the Virginia IT Agency (VITA). This SOR requires an overall review of specified locality’s current approach for meeting the goals and objectives outlined in the Cybersecurity Plan, as well as development of recommended security artifacts to support operationalization of the Cybersecurity Plan.

The Supplier will review specified locality’s current state capability against the following capabilities using a standard list of topics provided by VITA:

* Inventory and control of technology assets, software and data
* Threat monitoring
* Threat protection and prevention
* Data recovery and continuity
* Security assessment

In order to complete the current state assessment, the Supplier will be expected to conduct interviews with the locality’s personnel, and request and review a locality’s existing documentation and policies that support the Virginia Cybersecurity Plan goals and objectives. Supplier is expected to use its security expertise to ask the right questions and follow-ups so as to ensure a useful review. Supplier is *not* being engaged to conduct technical tests of security systems or measures.

After this initial evaluation, the Supplier will generate a Findings and Recommendations Report using a standard template provided by VITA. The draft report is provided as an attachment to this SOR. The report will describe the current state and also recommend actions to improve the locality’s capabilities, such as initial development of missing governance artifacts (e.g., Security Management plan, updated policies, updated standards, controls frameworks, capabilities, charters, etc.) as prioritized by senior leadership for this initial phase of this effort. Prioritizations should focus on greatest impact, while keeping in mind feasibility of near-term and program objectives, and may include but are not limited to:

* Manage, monitor, and track information systems, applications, and user accounts;
* Monitor, audit, and track network traffic and activity;
* Enhance the preparation, response, and resiliency of information systems, applications, and user accounts;
* Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk;
* Adopt and use best practices and methodologies to enhance cybersecurity (references NIST);
* Implement multi-factor authentication, implement enhanced logging, data encryption for data at rest and in transit, end use of unsupported/end of life software and hardware that are accessible from the Internet, prohibit use of known/fixed/default passwords and credentials, ensure the ability to reconstitute systems (backups), migration to the .gov internet domain;
* Promote the delivery of safe, recognizable, and trustworthy online services, including using the

.gov internet domain;

* Ensure continuity of operations including by conducting exercises;
* Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity);
* Ensure continuity of communications and data networks in the event of an incident involving communications or data networks;
* Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the specified locality;
* Enhance capabilities to share cyber threat indicators and related information between the eligible locality and the Authorized User;
* Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;
* Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.

Suppliers should provide a **fixed price per assessmen**t in their response. As in-scope localities will be determined prior to SOW execution, Suppliers should also include any assumptions that could impact their price per assessment. The final total price of the SOW(s) will be finalized during Supplier negotiations once the number of in-scope assessments is determined. Please review the attached Appendix – Locality Characteristics for estimates of size and type of public bodies that have requested the assessments. Respondents may propose a tiered pricing approach per assessment based on factors provided.

1. **Period of Performance**

The period of performance for any resulting SOW(s) will be determined based on the number of assessments in scope to the SOW(s) and finalized during supplier negotiations. VITA’s initial vision is to have all of the assessments completed within an estimated 12 week timeframe or as mutually agreed upon during supplier negotiations. Suppliers responding to this solicitation should provide estimates for the number of assessments they can complete in a 12 week period and any associated assumptions.

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

Authorized User’s Location ­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(City, VA)*

Supplier’s Location \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(City, State)*

Specified Locality and/or \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(Explain)*

Supplier’s Location

Suppliers should assume that all the work can be performed remotely when pricing their proposals. However, VITA wants to offer localities the flexibility of requesting onsite visits by the Supplier if needed. In their proposals, responding Suppliers should detail any limitations on travel if requested by a locality. Final determinations about travel and any associated costs will be made during supplier negotiations. Any travel involved will be required to adhere to Commonwealth travel expense regulations.

1. **Project Staffing:**
2. **Supplier Personnel**

The roles listed in the table below represent the minimum Supplier personnel requirements for this engagement.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Key Personnel (Y/N)** | **Years of Experience** | **Certifications** | **References Required (Y/N)** |
| Security Executive Sponsor and QA | Y | 20+ years | N/A | N |
| Senior Security Lead | Y | 15+ years | N/A | N |
| Junior Security Support | Y | 2-5 years | N/A | N |

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 |
| VITA Chief Information Security Officer | Project Sponsor work product approval | 5% |
| Various VITA Support Staff | Support discovery, provide expertise on current processes, provide feedback on recommendations and deliverables as appropriate | 10% |
| VITA Project Manager | Primary POC for the project and support project coordination and discovery | 85% |

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** | **Estimated Completion Date** |
| --- | --- | --- |
| Project Initiation | Project Planning and Kickoff Presentations | May 2024 |
| Acceptance of Final Findings and Recommendations Report | Final Findings and Recommendations Report | TBD |
| Phase 1 Completion | Completion of Phase 1 Supporting Artifacts per sponsor agreement | TBD |

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

|  |  |
| --- | --- |
| **Deliverable Type** | **Format** |
|  |  |
| Spreadsheets | Microsoft Excel |
|  |  |

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

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

Respondents should assume no travel when providing their pricing per assessment. Travel requirements and the associated costs, if any, will be determined during Supplier negotiations.

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:**

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 of 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 submission of completed assessments for each interviewed locality.

Other (specify): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Project Roles and Responsibilities:**

| **Responsibility Matrix** | **Supplier** | **Authorized User** |
| --- | --- | --- |
| *Prepare Capability Assessment plan* |  |  |
| *Review and Accept Plan* |  |  |
| *Perform Capability Assessment and Review* |  |  |

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

Standard CAI Required Background Check

Agency Specific Background Check – VITA 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): As defined in the Scope of Work and Deliverables sections of this SOR.

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:**

Required as specified below

Not Required

Training Requirements:

*(Specify specific training requirements)*

1. **Documentation:**

Required as specified below

Not Required

Documentation Requirements:

As detailed in Section 10 (Scope of Work) and Section 14 (Milestones and Deliverables) of this SOR

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

VITA will protect the confidentiality of cybersecurity information, including assessments of public bodies, as permitted under Virginia law.

As between VITA and Supplier:

Authorized User (VITA) 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 may be requested 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:**

On an as needed basis, to be coordinated with the Authorized User’s Project Sponsor and Project Manager.

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

The Authorized User may provide furniture and equipment within limited workspace on a temporary basis. Permanent office space, furniture and equipment are the responsibility of the Supplier. If required, while on-site at the project location, the specified locality will provide access to a copier, fax, the agency LAN and the internet (for up to two connections). Specified locality will also provide temporary desk space. The Supplier must provide any cell phones, personal computers or laptops required by the Supplier team. The specified locality’s technical staff supporting the specified locality’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.

Specified locality will also provide access to all documentation for the referenced projects.