**STATEMENT OF REQUIREMENTS (SOR)**

**SOR # DRPT-220405-01-CAI**

**DRPT Web Application Penetration Testing**

1. **Date:** April 5, 2022
2. **Authorized User:** Virginia Department of Rail and Public Transportation
3. **Authorized User Contact Information:**

Jennifer L. Mayton, CGFM, VCO

Virginia Department of Rail and Public Transportation

Email: Jennifer.mayton@drpt.virginia.gov

Phone: (804) 786-5756

[www.drpt.virginia.gov](http://www.drpt.virginia.gov)

1. **Solicitation Schedule:**

|  |  |
| --- | --- |
| **Event** | **Date** |
| Release SOR | 04/25/2022 |
| Supplier Response Due | 05/09/2022 |
| Award Decision | 05/10/2022 |
| Estimated Project Start Date | 05/16/2022 |

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 agency requirements, its applicability to the Commonwealth Agency’s environment, and its effective utilization of Supplier and Commonwealth 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 requirements including:
* Information Security Standard (SEC501-11.3)
* Previous experience conducting penetration tests for similar organizations based on size, complexity, and regulatory requirements.

1. **Project/Service:** Web Application Penetration Testing
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: As an agency of the Commonwealth of Virginia, the Virginia Department of Rail and Public Transportation (DRPT) is required to follow COV ITRM Standard SEC501-11.4 (SEC501). DRPT has three (3) interactive web applications and six (6) public-facing websites that are required to undergo penetration tests as mandated by control CA-8 of SEC501.

Project Complexity: This project is medium complexity and low risk.

Business Need: DRPT is committed to complying with SEC501 and as such, penetration testing of the above-referenced applications is required. In addition to complying with SEC501, DRPT is committed to ensuring the ongoing security posture of these web applications. Therefore, the Supplier shall perform penetration tests of these applications on a monthly basis for twelve (12) contiguous months.

Project Management and Organizational Structure

DRPT’s Information Technology Manager and/or designee(s) will be the leads for this effort. The Supplier will provide deliverables to the Information Technology Manager.

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:

* Conduct a baseline penetration test of the following web applications:
  + Online Grant Administration (OLGA)
  + Financial and Procurement System (Bobcat)
  + DRPT Intranet
  + DRPT public website
  + Telework!VA website
  + CommuteVA website
  + VanpoolVA website
  + BikeToWorkVA website
  + TransitVA website

Prior to testing, the Supplier shall work with DRPT to develop written Rules of Engagement to confirm the scope of the testing, including specific Uniform Resource Locators (URLs), the type of attacks that may be out of scope (e.g., intentional denial of service), assumptions and limitations, authorized test windows, and points of contact during the testing.

The Supplier shall deliver a baseline report that covers each of the above-referenced web applications. The report shall include:

* + Overview of activities performed and testing methodology
  + Summary of findings
  + Detailed findings narrative
  + Suggested remediations for findings and/or enhancements to improve the security posture of the web application

The Supplier shall provide a briefing of the findings to the DRPT IT Manager and others as determined by DRPT leadership.

* Conduct monthly testing of the above-referenced applications to determine whether newly exploitable vulnerabilities were introduced in the intervals between tests. DRPT may, at its discretion, request that the monthly test for an application be conducted prior to release of an enhancement to one of the web applications referenced above.

The Supplier shall report out the results to DRPT after each test in a written summary and briefing.

1. **Period of Performance:**

DRPT requires that these services are performed from the Project Start Date and for the 12 contiguous months thereafter.

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

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

☒ Supplier’s Location Richmond, Virginia *(City, State)*

☐ Authorized User’s and/or

Supplier’s Location

1. **Project Staffing**

A. Supplier Personnel

The roles listed in the table below represent the minimum Supplier personnel requirements for this engagement. The Supplier will propose its staffing solution in the Statement of Work.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Key**  **Personnel**  **(Y/N)** | **Years of Experience** | **Certifications** | **References Required (Y/N)** |
| IT Security Analyst | Y | 3-5 | CISA, CISSP, eCPPTv2 or Similar certification preferred | Y\* |

\*References must be from a Virginia state agency

Respondents to this SOR must include the experience and skills of representative staff who the

respondent would propose to perform penetration testing.

At a more detailed level, the Team personnel must collectively demonstrate the knowledge and

experience to:

* Lead the execution of and manage penetration testing projects.
* Conduct penetration tests of web applications, including receiving credit for original vulnerabilities issued a Common Vulnerabilities and Exposures (CVE) number by Mitre Corporation.

B. 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** | **Hours/Week** |
| DRPT IT Manager | Primary contact for coordination to ensure the availability of web applications during testing; primary recipient of test reports and results | As required |
| Chief Administrative Officer | Authorization authority, as needed, of Rules of Engagement; Recipient, as needed, of test results | .25 |

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)** | **Estimated Completion Date** |
| 1 | Project Initiation | Approved project plan of action and milestones | Supplier to Propose |
| 2 | Baseline Penetration Testing Completed | Penetration Test Report | Supplier to Propose |
| 3 | First 2 Months of Recurring Tests Completed | Two (2) monthly test result summaries | Supplier to Propose |
| 4 | Second 2 Months of Recurring Tests Completed | Two (2) monthly test result summaries | Supplier to Propose |
| 5 | Third 2 Months of Recurring Tests Completed | Two (2) monthly test result summaries | Supplier to Propose |
| 6 | Fourth 2 Months of Recurring Tests Completed | Two (2) monthly test result summaries | Supplier to Propose |
| 7 | Fifth 2 Months of Recurring Tests Completed | Two (2) monthly test result summaries | Supplier to Propose |
| 8 | Final Month of Recurring Tests Completed | One (1) monthly rest result summary | Supplier to Propose |

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

|  |  |
| --- | --- |
| **Deliverable Type** | **Format** |
| Documents or spreadsheets created or completed by the tester. | Editable (unlocked), electronic format compatible with the Microsoft Office 2016 suite or higher (Word, Excel). |
| Working papers, documentation/email provided to the assessor | Retain in the original format as provided by DRPT. |

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

☒ No travel will be required for this engagement

☐ Travel must be included in the total fixed price of the solution. Travel outside the metro

Richmond, VA area will not be required to complete this project.

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 a final report. In the SOW,

Supplier will define 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** |
| *Conduct Penetration Tests* | ✔ |  |
| *Prepare Rules of Engagement document* | ✔ |  |
| *Sign Rules of Engagement document* |  | ✔ |
| *Ensure availability of web applications during agreed upon test windows* |  | ✔ |
| *Review and approve deliverables* |  | ✔ |
| *Escalate issues within 24 hours* | ✔ | ✔ |
| *Prepare deliverables* | ✔ |  |

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: estimate of completion of the overall project, progress toward fulfillment of each risk assessment, anticipated findings, and risks to project deadlines or requests for changes to agreed-upon project deadlines.

☒ **Other(s)** (Specify) Baseline and Monthly Penetration Test Reports

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

☐ Project will be funded with federal grant money (Standard Federal match rate)

☒ No federal funds will be used for this project

1. **Training and Documentation:**

**A. Training is:**

☐ Required as specified below

☒ Not Required

Training Requirements: COV required contractor training

**B. Documentation is:**

☒ Required as specified below

☐ Not Required

Documentation Requirements: *Please see scope of work and deliverables*

1. **Additional Terms and Conditions:**

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

* 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.
* 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:**

Normal business hours are 8:30 a.m. to 5 p.m., Monday through Friday.

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

* N/A