|  |
| --- |
| **STATEMENT OF REQUIREMENTS (SOR)** **SOR # VATAX*-*231020-01*-*CAI**  ***Virginia Department of Taxation Information System Audits – CACSG, PASS, FileNet, SailPoint*** |

1. **Date:** October 20, 2023
2. **Authorized User**: Virginia Department of Taxation
3. **Authorized User Contact Information:**

Robert Watts

600 E Main St

Richmond, VA, 23220

Phone: 804-371-0503

E-mail: [robert.watts@tax.virginia.gov](mailto:robert.watts@tax.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 | 11/03/2023 |
| Supplier Questions Due to CAI | 11/10/2023 |
| Authorized User Responds to Questions | 11/13/2023 |
| Supplier Response Due | 11/27/2023 |
| Award Decision | 11/29/2023 |
| Estimated Project Start Date | 12/06/2023 |

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 requirements including:

 Information Security Standard (SEC530)

 IT Security Audit Standard (SEC502)

 IT Risk Management Standard (SEC520)

• An understanding of the National Institute of Standards and Technology (NIST) Special Publication 800-53 - Recommended Security Controls for Federal Information Systems and Organizations.

• Previous experience auditing information technology security and compliance with Commonwealth Information Technology Security Standards at COV agencies.

• Ability to perform IT audits in accordance with the Generally Accepted Government Auditing Standards (GAGAS, Yellow Book) or Institute of Internal Auditors International Standards for Professional Practice of Internal Auditing.

• Suppliers who have performed IT security projects (other than audits) for VA TAX related to systems in scope must use audit staff and management independent of the staff and management for the IT security projects. The supplier shall include documentation describing how the supplier will achieve this independence with their response. These arrangements are subject to approval by VITA Commonwealth Security, which may result in delays to the start of the project.

• Preference given to firms with COV IT Audit experience or similar.

1. **Project/Service:**

VITA SEC530 IT Audits for the following Virginia Tax systems:

* CACSG
* PASS
* FileNet
* SailPoint

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

This SOR includes the following four separate SEC530 IT security audits:

*CACSG*

Computer Assisted Collections System for Government ("CACSG") is a software application that routes delinquent debts/cases through various collection states based on predefined business rules and procedures. CACSG is used by Virginia Tax to facilitate the collection of delinquent tax fees from individual taxpayers and businesses.

CACSG automates the collection and case management workflow, automatically performing functions such as generating correspondence to taxpayers, monitoring the status of payment plans, and generating daily work lists detailing those collection items that require further activity by Collections personnel. CACSG has also centralized case management by consolidating information regarding taxpayer contacts, debts, assets, payment plans, and past collection activities.

The Computer Assisted Collections System for Government for Court Debt Collections (“CACSG-CDCO”) is an associated application that is similar to CACSG but uses a separate database. The two applications share server platforms and operate in the same Information Security controls environment. CACSG-CDCO is used by the Court Debt Collections Office (“CDCO”). CDCO has been charged with collecting outstanding court debts on behalf of the Commonwealth’s judicial branch.

Access to CACSG, and CACSG-CDCO, is handled by the single sign-on process, Tax Authority, which grants users the capability to access multiple IRMS applications through a central authentication application. The CACSG system architecture consists primarily of Linux servers and utilizes an Oracle database.

*PASS*

PASS is an Audit Selection Application. PASS allows auditors to create, manage and initiate the creation of audit cases. PASS evaluates information in the Compliance Repository and identifies potential audit candidates. PASS uses models to define the criteria that should be used to evaluate the data in the Compliance Repository. As a sub-system of PASS, Return Reconstruction uses Federal and State data from the Compliance Repository to build a proposed audit return. Return Reconstruction contains the logic necessary to reconstruct a state return from the federal and state data sources.

The PASS application has a PowerBuilder-based front end interface that is installed on the desktop or laptop computer for data entry/model definition. The backend PASS processes runs on a Unix server. The batch processes that run on the Unix server are written in C++ and Oracle stored procedures. Return Reconstruction jobs are processed via the Tivoli job scheduler in production. Return Reconstruction distributes the proposed audit return information to AR as an XML file through the return processing (RP) process. The Return Reconstruction application is stand-alone program written using Oracle packages, stored procedures and functions. The Return Reconstruction processes are launched via calls to Unix scripts that in turn invoke the Return Reconstruction Oracle packages. Source data for Return Reconstruction consists of Federal data (1040, CP2000, EOAD) and State data (760,763,760PY forms),

*FileNet*

FileNet is used by the Virginia Department of Taxation as the content repository of paper tax returns, taxpayer correspondence, and tax audit workpapers and contains both state and federal tax data. FileNet content can be accessed directly via FileNet Image Retrieval, but images from FileNet are most commonly accessed by selecting a link within the Advantage Revenue, Siebel or CACSG systems which accesses images using FileNet Image Viewer. The application is a commercial of-the-shelf (COTS) system supported by IBM.

The DataCap team performed an upgrade to the system to version P8 in 2017, with the help of CGI. FileNet P8 provides a COTS web-based presentation layer, IBM Content Navigator (ICN), that replaces the agency-developed Image Retrieval and Image Viewer applications. Image Retrieval uses an ICN stock search desktop. Image Viewer uses a custom desktop developed in Java. The agency has source code for this custom desktop and maintains it.

FileNet utilizes an Oracle database server to store image data.

*SailPoint*

The SailPoint Identity IQ application system is an identity access management application that provides a means for users to request and when approved, receive access to various systems used by Virginia Tax employees. SailPoint provides compliance controls that help define and enforce user access policies, such as separation-of-duties (SOD) and automates the process of reviewing user access rights across the organization by requiring business managers to approve or revoke access as part of a centralized governance program. SailPoint user provisioning makes it easy to manage access changes throughout a user’s lifecycle. By applying governance to all provisioning processes, this allows users to acquire the appropriate access to systems and applications across the data center, the cloud, and mobile environments.

SailPoint IdentityIQ also provides a solution for enterprise customers that delivers a wide variety of identity and access management (IAM) processes including automated access certifications, policy management, access request provisioning, password management, and identity intelligence. Furthermore, IdentityIQ has a flexible connectivity model that simplifies the management of applications running in the data center or the cloud.

The SailPoint system architecture consists primarily of Linux servers and utilizes an Oracle database.

Business Need

As part of the Internal Audit process, the CACSG, PASS, FileNet, and SailPoint system audits are included in the CY24 IT audit plan.

The data owners, system owners, and VA TAX’s Information Security Officer have identified each of these systems as sensitive. As such, the Commonwealth’s IT Security Standard requires a SEC530 IT Security Compliance audit.

VA TAX requires final audit deliverables for all four audits by June 1, 2024.

Project Complexity

This project is medium complexity and high risk.

Project Management and Organizational Structure

VA TAX’s Internal IT Audit Supervisor and/or designee(s) will be the leads for this effort. The

Supplier will provide deliverables to VA TAX’s Internal Audit Director, Internal IT Audit

Supervisor, and other VA TAX staff required.

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 over the course of the audits:

Work papers will need to be reviewed by Virginia Tax Internal Audit prior to the exit conference. Inquiry cannot be used as the primary source of evidence for tests of controls. Access control testing should confirm the **timely** termination of access and not just termination of access. The final audit report should be written in the format provided by Virginia Tax Internal Audit. The audit should be performed in compliance with SEC530 standards. Consultants must maintain appropriate licenses and perform all assignments in accordance with the International Standards for the Professional Practice of Internal Auditing (IIA standards).

1. Develop an IT audit program based on the requirements of VITA’s SEC530 for the systems identified in Section 9 of this document.
2. Arrange for and conduct an audit entrance conference to review the project plan, audit scope, limitations, expectations, and timeframes with appropriate VA TAX management and Internal Audit staff. Document the agenda, attendees, and summary of discussion for inclusion in audit work papers.
3. Document and execute IT audit procedures to perform an IT Security Audit for SEC530 for each system listed in Section 9. Supplier will assess and ensure compliance in accordance with the Commonwealth’s Information Technology Security Audit Standard (ITRM Standard SEC502) and the Generally Accepted Government Auditing Standards or Institute of Internal Auditors International Standards for Professional Practice of Internal Auditing. IT general controls and controls that are the responsibility of VA TAX IT infrastructure service provider (VITA) or other third party vendors such as physical and environmental controls are not in scope for this audit.
4. Work directly with VA TAX business unit staff and management, VA TAX’s Internal Audit Director, Internal IT Audit Supervisor, and other VA TAX staff as required to collect the information necessary to complete the audit. For tracking and reporting of audit requests, maintain a list of items requested from VA TAX with item description, date requested, name of requestor, name of responsible VA TAX staff, due date agreed to, date received, and additional comments.
5. Compile and provide a detailed list of audit findings for failed controls including the audit program step number, the number and title of the audit point in the audit report in which the finding is included, a description of the finding, and the SEC530 control number tested.
6. Prepare and provide a draft audit report to the Internal Audit Director and IT Audit Supervisor, for review. Detailed findings may be grouped into a higher-level audit point in the report if they share a common subject. **Audit findings in the report must include easily identifiable elements of a finding: condition, criteria, cause, effect, and recommendation.**
7. Review audit findings and draft report with VA TAX’s Internal Audit Director, Internal IT Audit Supervisor, and other VA TAX staff and stakeholders as needed. Obtain a written corrective action plan including a responsible individual and estimated date of completion from responsible staff within 10 business days for inclusion in the final report.
8. Complete and submit the final report including the VA TAX corrective action plan to VA TAX’s Internal Audit Director, Internal IT Audit Supervisor, and other VA TAX staff required for review.
9. Conduct an exit conference with IT operational management, information security management, business process owners (system owners), data owners, and Internal Audit staff to present the final audit report. Document the agenda, attendees, and summary of discussion for inclusion in audit work papers.
10. Provide a complete set of work papers in the formats specified in item 14 of this SOR by the project completion date.
11. Upon completion of the project, provide the work paper template that is utilized for said project.
12. Ensure the protection of sensitive system and audit information by using a secure method for obtaining audit evidence and using encrypted email to communicate sensitive information to and from VA TAX audit contacts.
13. **Period of Performance:**

Delivery of all products and services defined in the Statement of Work will occur by June 1, 2024.

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

Authorized User’s Location

Supplier’s Location

Authorized User’s and/or

Supplier’s Location (see below explanation)

Interviews and discussions with VA TAX Staff and reviews of sensitive documentation should take place remotely, or at VA TAX Headquarters at 600 East Main Street Richmond, VA 23219. Field work and other work may be performed either at VA TAX Headquarters or at supplier’s location if reasonable measures are taken to secure sensitive VA TAX documents and data.

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** |
| VA TAX Internal IT Audit Supervisor and/or designee | Primary contact for audit information requests | 100% |
| System Owners | Contact for audit information requests | 50% |
| System Administrators | Contact for audit information requests | 50% |
| Data Owners | Contact for audit information requests | 50% |

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 | Project Plan  Entrance conference agenda.  Develop project plan, audit scope, limitations, expectations, and timeframes with VA TAX management and staff involved with the system under audit. Documentation of the entrance meeting date, time, attendees, and summary of the discussion. | Within 10 business days of signed SOW/SOR |
| 2 | Audit Scope Program/Procedures | Documentation Requests: Submit a comprehensive audit evidence request list for distribution to key VA TAX personnel with the understanding that follow-up questions may arise.  Submit IT audit procedures/program for review and approval by VA TAX Internal Audit team. | Within 5 business days of entrance conference |
| 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. | Within 45 business days of Internal Audit approval of the scope of the audit procedures |
| 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. | Upon completion of audit test work or with draft audit report |
| 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 |
| 6 | Exit Conference | Exit conference agenda.  Review (at VA TAX location or remotely) audit results, findings, recommendations, and conclusions to objectives with VA TAX management and staff involved with the system under audit. Documentation of the exit meeting date, time, attendees, and summary of the discussion. | 5 to 10 business days after VA TAX receipt of the draft audit report |
| 7 | Final Audit Reports | Submit a final audit report for each audit listed in Section 10 that incorporates VA TAX management responses and corrective action plans. | Supplier to propose |
| 8 | Audit Work Papers | Provide an editable (unlocked) electronic copy of all audit work papers and evidence used to complete the audits. | Prior to audit exit conference |

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 auditor | Editable (unlocked), electronic format compatible with the Microsoft Office 2016 suite or higher (Word, Excel). |
| Audit evidence provided to the auditor | Retain in the original format as provided by VA TAX or other audit contact. For hardcopy documentation provided as evidence, provide scanned PDF 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:**

The Project Manager will have 10 business days from receipt of each 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 and Authorized User will agree on the format and content of the report to be provided to Authorized User for final acceptance.

Acceptance of all individual deliverables

1. **Project Roles and Responsibilities:**

| **Responsibility Matrix** | **Supplier** | **Authorized User** |
| --- | --- | --- |
| *Conduct Audit* | ✓ |  |
| *Coordinate audit evidence gathering and*  *meetings with operational and management staff* | ✓ |  |
| *Prepare audit report and summary of findings* | ✓ |  |
| *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: 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:

N/A

1. **Documentation is:**

Required as specified below

Not Required

Documentation Requirements:

Please see scope of work 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. **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. All audit evidence and working materials provided to the Contractor by VA TAX remain the property of VA TAX.
2. All work products and deliverables produced by the Contractor for this project become the property of VA TAX.
3. **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:**

Provided by VA TAX as needed and upon request:

* Visitor badge access to the building and work area
* Work area (office/cube and desk)
* Phone
* Desktop/laptop computer
* Office supplies