REQUEST FOR QUOTES
INFORMATION TECHNOLOGY SECURITY RISK ASSESSMENT SERVICES
OFFICE OF THE STATE COURTS ADMINISTRATOR

STATE ALTERNATE CONTRACT SOURCE 252-GSA-SCHEDULE 70,
Cyber Security and IT Professional Services

STATE TERM CONTRACT NUMBER 973-000-14-01,
Management Consulting Services

RFQ No.: 2200-1718-OIT-1

I. OVERVIEW

A. Purpose

Pursuant to the above-referenced state term contract and alternate contract source, Office of the State Courts Administrator (Customer) requests quotes from state term contract vendors for Information Technology (IT) security risk assessment services (the Services).

The Office of the State Courts Administrator seeks a vendor to provide the services outlined in this RFQ, delivered pursuant to the methodology and approach identified in this Request for Quotes (RFQ).

B. Office of the State Courts Administrator-Specific Information

This section contains OSCA-specific information, current as of the time this RFQ was released, relevant to a vendor providing the services described in this RFQ.

CURRENT STATE INFORMATION	
TOTAL AGENCY BUDGET:	55,000
NUMBER OF AGENCY EMPLOYEES:	215
CORE MISSION AREAS:	To protect rights and liberties, uphold and interpret the law, and provide for the peaceful resolution of disputes
LIST AND NUMBER OF OFFICE LOCATIONS:	Florida Supreme Court OSCA Annex
NUMBER OF SERVER ENDPOINTS:	100+
NUMBER OF USER ENDPOINTS:	200+

NUMBER OF APPLICATIONS:	20+
OTHER	The OSCA supports and maintains the data center held within the Florida Supreme Court building. OSCA is culpable for providing information systems that allow the six state courts (Florida Supreme Court, First District Court of Appeals, Second District Court of Appeals, Third District Court of Appeals, Fourth District Court of Appeals, and Fifth District Court of Appeals) to communicate and execute the core functions of the Florida Judicial Branch.

II. ELIGIBLE RESPONDENTS

This RFQ is being issued to vendors on the two above-referenced contracts. Only vendors who have been awarded contacts on one or both may submit a response.

III. TERM

The estimated term of the contract resulting from this RFQ will be two months with an anticipated contract start date of June 27, 2018 and a firm-fixed end date no later than September 1, 2018. There will be no renewals available under the prospective contract.

IV. TIMELINE

Important dates/times related to RFQ events are listed below. All times are Eastern Standard Time, and are subject to change.

DATE	TIME	EVENT
May 29, 2018		Release of RFQ
June 1, 2018		Questions due
June 5, 2018		Response to questions provided
June 12, 2018		Quotes due
June 13-21, 2018		Selection process
June 22, 2018		Selected Respondent identified
June 27, 2018		Anticipated start date
August 27, 2018	5:00 pm	All final deliverables / services provided to OSCA for completed IT Security Risk Assessment.

V. RFQ QUESTIONS AND CONTACT WITH THE STATE

Questions regarding this RFQ shall be submitted in writing (e-mail preferred) to the procurement officer identified in Section XII, by the date and time specified in Section IV or as amended by OSCA. Questions will NOT be answered via telephone or fax. OSCA will e-mail the answers to the questions by the close of business on the date stated in Section IV. The Contractor shall only contact the Procurement Officer for information regarding this RFQ.

VI. MODIFICATIONS

OSCA reserves the right to modify any requirement in the Scope of Work if OSCA deems it to be in the best interest of the State of Florida. Also, OSCA reserves the right to withdraw and/or cancel this RFQ at any time with no obligation to the vendor if withdrawn prior to services being performed.

VII. SCOPE OF WORK

A. TASKS

1. **IT SECURITY RISK ASSESSMENT**

The vendor shall perform a comprehensive IT security risk assessment of OSCA, meeting the requirements of this RFQ. The results of the services provided shall be in conformance with National Institute of Science and Technology (NIST) standards, particularly:
1) NIST SP 800-30 (Rev. 1) Guide for Conducting Risk, September 2012,
2) NIST SP 800-53 (Rev. 4) Recommended Security Controls for Federal Information Systems and Organizations, January 2015.
3) NIST Framework for Improving Critical Infrastructure Cybersecurity (Rev. 1)

The assessment shall be used to evaluate the processes, policies and procedures for all of the following functions:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness & Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes & Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies & Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning

		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The IT security risk assessment shall include evaluation of all resources as identified in Section I.B. above.

B. METHODOLOGY

In performance of the Risk Assessment, the Vendor shall utilize the following Risk Assessment Methodology:

1. Risk Assessment Process. The risk assessment process is broken down into three distinct parts:

    a. Prepare for the assessment (see NIST SP 800-30, Section 3.1):
        a. Identify the purpose
        b. Identify the scope
        c. Identify the associated assumptions and constraints
        d. Identify the sources of information to be used as inputs
        e. Identify the risk model and analysis approach

    b. Conduct the assessment (see NIST SP 800-30, Section 3.2):
        a. Identify threat sources and events
        b. Identify vulnerabilities and predisposing conditions
        c. Determine likelihood of occurrence
        d. Determine the adverse impacts
        e. Determine the information security risk

    c. Communicating the assessment results (see NIST SP 800-30, Section 3.3)
        a. Communicate the risk assessment results
        b. Share resulting information in support of risk management activities

2. The Risk Model. This model is a threat-based model that considers threat sources, likelihoods of occurrence, and impacts (see NIST SP 800-30, Section 2.3.1).

3. Assessment Approach. This approach uses ranges (0-15, 16-29, 30-50) and scales (1-10) to assign risk severities, and is semi quantitative (see NIST SP 800-30, Section 2.3.2).

4. Analysis Approach: The analysis approach is vulnerability-oriented (see NIST SP 800-30, Section 2.3.3).

C. DELIVERABLES

Under the prospective contract, the vendor shall provide all services and deliverables pursuant to OSCA requirements identified in this SOW.

Deliverable	Acceptance Criteria/Performance Standards	Schedule/Due Dates
Project Management Schedule & Support Services	Develop and provide a project schedule and associated project documentation to include the following: • Describe your security assessment methodology • List the tools used in the security assessment process • List milestones/deliverables with estimated delivery dates • Describe how you ensure the quality and the timeliness of the above deliverables All documents shall be submitted in a format compatible with Microsoft Office 2013, or higher, and/or Project 2013, or higher software.	July 9, 2018
Initial Draft of IT Security Risk Assessment Report	After completion of the risk assessment as detailed above, the Vendor shall complete and submit drafts of the below documents: **IT Security Risk Assessment Report** At a minimum, this report shall narrate the vendor's methodology for completing the IT security risk assessment and must address each of the below requirements: • Identification and assessment of security risks using a uniform criteria based on industry best practices. • Identification of any risks with severity. • Recommendation for remediation strategies. • Prioritization of remediation activities. **Delivery**: An initial draft of the IT Security Risk Assessment Report shall be provided to OSCA for review to ensure the document conformance with the SOW. OSCA shall provide feedback within 7 days of receipt of the initial drafts. This feedback will include any changes or adjustments vendor is to make to the document prior to submission of the final deliverable.	August 20, 2018

Final Draft of IT Security Risk Assessment Report *(Attachment A)*	Based upon OSCA feedback of draft documents, Vendor shall revise and submit final versions of the below documents: **IT Security Risk Assessment Report** At a minimum, this report shall narrate the vendor's methodology used to complete the IT security risk assessment and must address each of the below requirements: • Identification and assessment of security risks using a uniform criteria based on industry best practices. • Identification of any risks with severity. • Recommendation for remediation strategies. • Prioritization of remediation activities. **Delivery**: The final documents shall be provided to OSCA. **Briefings**: Upon request of the OSCA, and at no additional cost to OSCA, the vendor shall be available to present and provide in-person briefings (limit 2) on the risk assessment and remediation strategies for a 60 day period after the OSCA's receipt and acceptance of the final Risk Assessment Report.	August 27, 2018

D. ACCEPTANCE OF WORK

All deliverables must be submitted to OSCA for review and approval (Acceptance) in accordance with the Section VII C above. OSCA will only accept each deliverable when it has been reviewed and acknowledged compliant with the applicable criteria specified within this SOW. OSCA may provide additional acceptance criteria during the contract period to be used for the deliverables. OSCA reserves the right to require the Contractor to revise deliverables previously approved at no additional cost for any inadequate or insufficient information. The invoice will not be paid for deliverables that fail to meet specifications until acceptable corrective action has been completed. Failure to accept a deliverable within twenty (20) calendar days means automatic non-acceptance unless stated otherwise by OSCA in writing.

VIII. USE OF SUBCONTRACTORS

In providing services under the prospective contract, the vendor is permitted to utilize subcontractors. However, in its response to this RFQ, the vendor shall identify all

subcontractors that the vendor will utilize and what services they will provide. During the term of the prospective contract, subcontractors may be substituted with the prior written approval of OSCA Procurement officer. AGENCY NAME and state term contract background check requirements will apply to subcontractors.

IX. QUOTE SUBMISSION

Electronic copy of the response to this RFQ shall be delivered to the Procurement Officer on or before the response deadline provided in Section IV, or as amended by OSCA. The vendor's quote shall be organized as follows:

TAB A COVER LETTER

A cover letter identifying the Contractor, Contractor representative and contact information. The cover letter MUST identify whether the vendor's response is submitted via Department of Management Services Management Consulting Services Contract No. 973-000-14-01; or the General Services Administration (GSA) Schedule 70 Contract. Submissions from vendors that are not on one of these contracts will be considered non-responsive and not reviewed or considered.

TAB B

PAST EXPERIENCE AND UNDERSTANDING OF CUSTOMER NEEDS

A. Describe your organization's experience with conducting IT security risk assessments, making sure to describe all contracts your organization has executed in the last five (5) years that required an analysis be conducted of the IT risks of the customer identified in the contract. Be sure to specifically identify when such services were provided to other State of Florida governmental entities. Also, identify all relevant similarities or differences to such contracts as compared to the services sought via this RFQ. The listing shall contain the organization name, contact name, address, telephone number and e-mail address of the entity that received the services from Respondent.

B. Provide an overview of your understanding of the service objectives sought via this RFQ.

C. Provide a brief description of the IT security statutes, rules and other standards that relate to OSCA's IT security model / systems.

D. Identify any other experience that is relevant to the services sought, using comparisons and distinctions where applicable.

E. Provide a sample IT Security Risk Assessment report that illustrates the deliverables OSCA will receive.

TAB C APPROACH TO PROVIDE THE SERVICES

A. **Scope of Work**. Describe in detail how the vendor intends on achieving the requirements identified in Section VII; specifically, vendor's approach to providing the deliverables identified in Section VII.C. Further, vendor shall detail workspace and any other additional resource needs for on-site and off-site services.

B. **Resources**. Provide resumes of each team member that your organization shall assign to this project and how their skill sets are relevant to the scope of work detailed in this RFQ. Vendors are welcome to identify certifications held by resources that will provide the services. Failure by vendor to provide the identified resources may result in OSCA selecting another vendor to provide the services.

C. **Superior Service**. Identify what makes your organization uniquely qualified to provide the services to OSCA. Be sure to identify how your organization is better able to provide the services compared to other vendors that provide IT risk management services, and the key advantages of the vendor's solution or value added to the OSCA.

TAB D PRICE SHEET.

The contractor shall provide a price sheet containing a single fixed price for all services to be provided under the prospective contract, **AND** a price for each deliverable that matches the percentage limitations provided in the table contained in Section XII. below. The fixed price shall be based on established rates set forth in the state term contract and no additional fees shall be charged for products or services other than the single fixed price.

NOTE: If the contractor considers any part of its response to this RFQ confidential or trade secret, it shall provide the OSCA with a copy of its response with such information redacted. The redacted copy shall be provided to the OSCA at the same time vendor submits its response and must only exclude or obliterate those exact portions which are claimed confidential, proprietary, or trade secret. The vendor must state the specific statutory exemption(s) for each redaction and shall be responsible for defending its determination that the redacted portions of its response are confidential, trade secret, or otherwise not subject to disclosure. Further, vendor shall protect, defend, and indemnify the OSCA for any and all claims arising from or relating to the vendor's determination that the redacted portions of its response are confidential, proprietary, trade secret, or otherwise not subject to disclosure. If the vendor fails to submit a redacted copy with its response, the OSCA is authorized to produce the entire documents, data, or records submitted by the vendor in response to a public records request for these records.

OSCA reserves the right to reproduce and disseminate proposal materials, as it deems necessary. All materials submitted become the property of OSCA. The OSCA reserves the right to use any information contained in a quote unless prohibited by law.

X. ORAL INTERVIEWS AND NEGOTIATON

Prior to issuance of a purchase order, OSCA may conduct oral discussions and / or negotiate pricing, terms, and / or conditions with quoting vendors.

XI. BASIS OF SELECTION

Pursuant to the State Courts System Purchasing Directives, the OSCA will base its decision on which vendor offers the best value.

XII. PAYMENT

Upon written acceptance of the deliverables identified in Section VII.C. payment, in the form of a percentage of the single fixed price vendor provides in **TAB D** of their quote, will be made as follows:

	DELIVERABLE	PAYMENT AMOUNT
1.	**PROJECT SCHEDULE**	5%
2.	**INITIAL DRAFTS** IT Security Risk Assessment Report (**Attachment A**)	25%
3.	**FINAL DELIVERABLES** IT Security Risk Assessment Report – Final (**Attachment A**)	70%

XIII. PROCUREMENT OFFICER AND PROJECT MANAGER

The Procurement officer for this RFQ is:

Steven Hall
Office of the State Courts Administrator
500 South Duval Street
Tallahassee, FL 32399
halls@flcourts.org

The Project manager for this RFQ is:

Gavin Green
Office of the State Courts Administrator
500 South Duval Street
Tallahassee, FL 32399
greeng@flcourts.org

XIV. APPLICABLE TERMS AND CONDITIONS

The following terms and conditions will apply to the prospective contract:

This RFQ and any resulting purchasing order or contract is bound by the State Courts System General Contract Conditions for Services, which are incorporated by reference and can be found at: http://www.flcourts.org/administration-funding/contract-conditions-for-services.stml. Any disagreement between the general conditions and this RFQ or resulting contract or purchase order, the RFQ, contract or purchase order will govern.

A. **ANNUAL APPROPRIATION**

The State of Florida's performance and obligation to pay under this contract is contingent upon an annual appropriation by the Florida Legislature.

B. **COMPLIANCE WITH ALL APPLICABLE LAWS**

The vendor shall provide all services in accordance with all applicable federal and state laws, rules and regulations. All such laws, rules, regulations, and procedures, current and/or as revised, are incorporated herein by reference and made a part of this RFQ and the resulting contract.

C. **STATE TERM CONTRACT TERMS AND CONDITIONS**

All terms and conditions of the above-mentioned state term contract shall apply to the prospective contract.

D. **INTELLECTUAL PROPERTY**

OSCA will own the intellectual property rights to all deliverables provided to OSCA as part of the prospective contract.

E. **RECORDS MANAGEMENT**

In providing services under the prospective contract vendor will receive, review and / or will come in contact with information that is or may be considered confidential and exempt under law. Vendor shall manage such information appropriately.

F. **FAILURE TO PERFORM**

Failures to perform will be handled in accordance with 60A-1.006, Florida Administrative Code, and as specified in the purchase order.

G. **FINANCIAL CONSEQUENCES**

The vendor shall perform the services in a proper and satisfactory manner as determined by the RFQ. Vendor failure to comply with the terms and conditions of this RFQ and any resulting contract will result in the OSCA taking the following actions, as appropriate:

1. If the vendor does not meet the deliverable deadline for any reason, 15% of the total contract payment will be deducted from final payment.

XV. REFERENCE MATERIALS

The following documents may have applicability to this project and are hereby incorporated by reference into this RFQ.

- NIST Guide for Completing Risk Assessments:
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

- Risk Management Framework (RMF) Site:
  http://csrc.nist.gov/groups/SMA/fisma/framework.html

- RMF Overview:
  http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

- Security and Privacy Controls for Federal Information Systems and Organizations
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf