RFQ 2200-1715-OIT-1 Q&A

Questions and Answers, in the order received.

Question	Answer
Does the system have an existing SSP?	No
Do they use a system like Xacta or CSAM to generate the SSP.	N/A
Will they provide us the current POAM list?	N/A
Will they provide scanning tools or we have to bring our own?	The vendor will be allowed to utilize their own scanning tools during business hours. OSCA will not provide access to their scanning solutions.
What's the number of OS servers, DB servers, Web Application servers we have to scan?	10-15 OS Servers / 5-10 DB Servers, 5-10 Web application servers
Is there a format they prefer for the Security Assessment Report? Will previous SAR's be provided for reference?	No format preferred. Previous SAR is N/A
Are there insurance requirements specific to this contract that are in addition to that required by the Term Contract?	No.
Will the Assessment Team have access to the locations during non-business hours and during business hours for conduct of the assessments?	The assessment team will have access during business hours only which are Monday-Friday, 8Am to 5PM Eastern Standard Time.
Can the vendor bring their own equipment into the OSCA environment?	Yes
Is there an expectation for Penetration Testing to be part of the Vulnerability Assessment solution?	Penetration testing is not part of this assessment.
Does the Customer have a vulnerability scanning and pen testing program already in place? Or does it have access to scan results from vendors if outsourced?	Yes, OSCA utilizes a vulnerability scanning solution. The vendor may utilize their own vulnerability scanning solution. OSCA will not provide access to their vulnerability scanning solution.
If no vulnerability scan program, is the Contractor expected to conduct a vulnerability scan?	Yes.
Has a similar assessment or audit been performed in the recent past?	No.
Is the budget of $55K listed on page 1 the budget for this project? If not, what is the estimated budget?	Yes, the budget for this project is $55,000
Please confirm that the Florida Cybersecurity Standard – Risk Assessment Tool is not included in the scope of this RFP.	Correct, the Risk Assessment Tool is not within scope.

Please confirm vulnerability assessment scanning is not included in the scope of this RFP.	Vulnerability assessment scanning is within scope.
The Initial Draft due 8/20/2018 states, "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." If OSCA takes the full 7 days to provide feedback to the draft, it will not be possible to provide the Final Draft by 8/27/2018. Will OSCA consider changing the Final Draft of IT Security Risk Assessment Report due date from August 27, 2018 to a later date to allow the contractor to receive and integrate comments from OSCA into the Final Draft Report?	The OSCA is willing to adjust the dates as follows: The initial draft will still be due on 8/20/18. The OSCA will provide changes and/or adjustments to the vendor by 8/25/18. The final draft will be due from the vendor by 5pm on 8/30/18.
Given the limited budget for this project, will OSCA waive the requirement for "in-person briefings (limit 2)" and consider Webex/teleconference as an acceptable method to meet this requirement for remote participants to reduce/limit the cost of travel?	Yes.
The RFQ states there are 100+ server endpoints, please specify the exact number	268
Specify the number of actual servers, both physical and virtual.	63 Physical Servers / 205 Virtual Servers
The RFQ states there are 200+ user endpoints, please specify the exact number.	Estimated 208
The RFQ states there are 20+ application, please specify the exact number. Are they off-the-shelf or in-house developed? Please specify the numbers for each.	OSCA administers over 80 in house and third party applications. Within the scope of this RFQ is 20-25.
Is this risk assessment to be in compliance with Rules 74-1 and 74-2 of Florida Administrative Code?	No
Are we expected to use the AST Florida Cybersecurity Standards-Risk Assessment Tool V1.0 as part of this engagement?	No
Total Agency Budget is listed as $55K. Can OSCA please clarify if this is the total budget available for this risk assessment?	$55,000 is the total budget available.
Will the vendor be required to compile risk assessment results in the FCS 74-2 template that was developed by AST for similar Agency risk assessments in 2016-2017?	No

Is the scope of work limited to assets that are supported and maintained by OSCA at the data center located within the Florida Supreme Court building? If not, what other assets are in scope?	Yes
Are the user and server endpoints and applications in this table all considered in scope? If so, are they all supported and maintained by OSCA at the data center located within the Florida Supreme Court building?	Yes
Will the vendor have access to OSCA threat intelligence feeds?	OSCA will not provide access to their threat intelligence feeds.
Will the vendor have access to OSCA vulnerability scan and assessment reports?	OSCA will not provide access to their vulnerability scan and assessment reports.
Is technical configuration/vulnerability testing included as part of the overall NIST CSF framework and in scope for this assessment?	Yes
Is the vendor performing the assessment expected to complete the AST CSF spreadsheet?	No
Will the Office consider a 30-day extension to the assessment timeline (final due 10/1 instead of 9/1)? Based on prior experience with this assessment is other State for Florida entities, we anticipate the Office will need a couple of weeks minimum to prepare, collect documentation, schedule SME interviews, etc.	OSCA will consider a 30 day extension to the assessment timeline.
What is the Office's budget for this project?	$55,000
What is the total Agency total budget? The RFQ states 55,000 and is unclear what this figure is intended to communicate.	$55,000
Please confirm the number of physical locations in scope of this RFQ are two (2). In Section 1.B of the Overview, the Florida Supreme Court and OSCA Annex are indicated.	The physical location of the Florida Supreme Court is only within scope.
Please indicate if this is a governance-only assessment?	The scope of this risk assessment is outlined in Section VII in which states that the assessment shall evaluate the processes, policies, and procedures of OSCA and how they align with the resources identified as part of the NIST Cybersecurity Framework. This assessment is not governance only.
For this RFQ is OSCA considering network vulnerability assessments and network penetration testing within scope?	Network vulnerability assessments are within scope. Network penetration is not.

If yes, then several additional items will be needed to understand the services the complexity of the environment.	OSCA's infrastructure primarily consists of Microsoft solutions (desktop O/S, Server O/S, Active Directory, IIS). OSCA primarily uses Microsoft SQL and Oracle for database functions. OSCA consists of many in-house web applications to facilitate services but manages web applications developed by a third party. Within the scope of this RFQ is the data center housed in the Florida Supreme Court building that serves the Florida Judicial Branch and the information technology assets that provide the services.
For this RFQ does OSCA require a full project management plan?	Yes
If yes, will templates be made available prior to the start of the project?	No. Vendor may use their own template.
Will OSCA provide a copy of a previous assessment or template at the start of the project?	No.
Failure to accept a deliverable within twenty (20) calendar days means automatic non acceptance… Please indicate the scenario where this could occur? This statement appears to indicate that a deliverable could inadvertently be rejected if a reviewer were to be out for illness.	This is standard language and OSCA does not have a scenario where this would be applicable.
Please indicate if conference rooms will be available for required meetings such as kick-off and final presentations. Will OSCA schedule these on the vendor's behalf?	Yes, OSCA will be able to accommodate the vendor for required meetings and final presentations. OSCA can schedule meetings on behalf of the vendor if necessary.
Please indicate OSCA's expectations for on-site meetings and/or status reports?	OSCA expects on-site meetings with staff to be timely and precise. OSCA also expects that status reports provide a summary of completed actions, and subsequent action items with estimated timeframes for future activities. OSCA will accept meetings via video or web conferencing solution(s) in lieu of in-person meetings.
Please confirm the vendor should use pricing under GSA Schedule 70. The cover page lists these two contracts: 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	The vendor should providing best and lowest pricing available, whether based on the contract(s) or otherwise. The contract(s) provide maximum pricing.
Does OSCA currently have vulnerability and compliance assessment tools deployed to the enterprise (e.g. Tenable Nessus, HP Web Inspect, etc…)?	Yes

Does OSCA currently have System Owners, ISSOs, Technical leads currently in place for the system?	Yes
Has the system been categorized as High, Moderate or Low? Does the system have PII?	No, there is no current data classification defined. Yes, PII does exist.
Does the assessment include any hot failover or continuity of operations facilities?	No
Does OSCA utilize a system of record manager such as CSAM, XACTA, or ARCHER?	No
Section I. Para B Current State Information. First row. What does 55,000 on first row represent? Does this mean the total agency budget is $55,000?	Yes, $55,000 is the total agency budget.
For Section VII Para A.1 The listed functions to be assessed do not seem to include all the NIST SP 800-53 security controls. Please confirm that the security controls listed are only required for the OSCA assessment	The security controls listed are the only required for the OSCA assessment.
Section IX Quote Submission. Tab B. Para C. Only info provided about the OSCA IT system is provide in Section 1, Para B. Respectfully request government provide a more detailed overview of the current OSCA IT security model/systems and business rules/data. This would help in scoping a response to this area.	OSCA serves as the administrative arm of the Florida State Courts which include the Florida Supreme Court and the five Appellate Courts. OSCA IT staff administer a data center within the Florida Supreme Court building. OSCA IT infrastructure includes, but is not limited to - Microsoft Active Directory, Exchange, Windows Servers, Windows Desktops, in-house developed applications, criminal justice information systems (CJIS) systems of which are governed by the FBI CJIS security policy and FDLE.
Is this the first time a risk assessment of this nature has been conducted within this environment?	Yes
Past Experience and Understanding of Customer Needs (Page 7, Tab B (A)). Is it required that the offeror has had direct past experience with OSCA or the State of Florida?	No
Price Sheet (Page 8, Tab D). Can we use our prices that are established in our GSA Schedule 70 if we are not on the State Term Contract?	Yes. Pricing should be the best and lowest available pricing for the services to be rendered. The contract(s) providing maximum pricing for services; if lower pricing is available, that pricing should be quoted.
Section XIV (B). Is this project funded?	Yes

Is there a provided Price Sheet from the State or should each vendor use their own price templates?	Own templates.
What is the time deadline on 6/12/18 to submit? Will this submission be to email or in a portal?	The OSCA will accept submissions through 11:59pm on 6/12/18.
Can this work be completed remotely?	OSCA will accept meetings via video or web conferencing solution(s) in lieu of in-person meetings. However, vendors will not be provided remote access for technical actions of the assessment and will require the vendor to be onsite.
Are all Access Points in the same location?	Yes
After the vulnerabilities have been identified. (a) Are additional tasks or testing required? (b) Only a report is required?	No
Although much of the wording of the RFQ reads as if this is a policy and procedure assessment, do you also want technical verification that the various processes are in place? This would require some technical testing.	No. Technical verification is not necessary, identification is. Within the scope of this RFQ is that the vendor have the capability of identifying vulnerabilities of critical systems. Not within the scope of this RFQ is verifying that the vulnerabilities can be verified by pen testing.
Questions inadvertanly left off the original response list:	
Section IX. Quote Submission, Tab B (PAST EXPERIENCE AND UNDERSTANDING OF CUSTOMER NEEDS) "List all contracts for last 5 years especially Florida State and list organization name, contact name, address, telephone number and e-mail address of the entity that received the services. Also, identify all relevant similarities or differences to such contracts as compared to the services sought via this RFQ." We have completed hundreds of such assignments in the last five (5) years. Will it suffice to provide a list of 5 to 6 examples with the information requested and provide the total number of overall similar projects completed in the last five years?	Yes

Section IX. Quote Submission, Tab C (APPROACH TO PROVIDE THE SERVICES) “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.” Would it be acceptable to provide a pool of resource bio’s for the project that identifies the skills required by each member to complete the work as well as certifications and education. Then once selected and upon contract execution, provide full resume for OSCA records?	Yes