The Supreme Court of Ohio

ADDENDUM #1

RFP No. 401

CYBERSECURITY RISK ASSESSMENT AND GOVERNANCE CONSULTING SERVICES

Date of Issuance: October 27, 2026

Response Due Date and Time:

November 20, 2026 at 12:00 p.m. EST

The Supreme Court of Ohio

Addendum #1 - Vendor Questions and Clarifications Related to RFP #401:

QUESTION #1:
Could you confirm whether the Court would accept a proposal in which a qualifying prime contractor meets the experience requirements of Section 6.2 and a respondent takes part as a subcontractor?

ANSWER:
The proposal response must be completed and submitted by a qualifying prime contractor. Respondents shall identify any subcontractors that they intend to use, and the subcontractor's specific work or services they will perform. All subcontractors shall work at the sole expense of the Contractor, and the Contractor shall be solely responsible for ensuring proper payment to the subcontractors. The Contractor shall assume responsibility for all work performed by subcontractors and ensure that all subcontractors comply with all contractual terms and conditions and policies of the Court. Proposed subcontractors shall also be considered and reviewed as a portion of the evaluation criteria. The Court reserves the right to review information regarding all proposed subcontractors and reject any identified before a contract is awarded.

QUESTION #2:
Must all five comparable projects requested in Section 6.2 be cybersecurity risk assessments completed by the proposing legal entity, or may key personnel and subcontractor projects qualify?

ANSWER:
Respondents are free to submit a proposal response that includes relevant experience of its proposed principals and key personnel, including work performed with previous employers, or named as an attributed subcontractor. As per Section 10, the Court reserves full discretion to determine the competence and capabilities of any Respondent who has submitted a proposal response, including contacting any customer or previous employer of the proposed principals.

QUESTION #3:
Do all five references need to be public-sector entities, or can private-sector references be included as well?

ANSWER:
The respondent must have documented experience with public-sector entities, however private-sector entities may be included provided they fit within a similar scope outlined in the RFP.

QUESTION #4:
Does the bidding process follow preference rules that the State uses, Such as buy Ohio and veteran owned?

ANSWER:
There are no preference rules.

QUESTION #5:
Are any minimum certifications or independence restrictions mandatory for key assessors?

ANSWER:
No certifications are mandatory, but any relevant certifications should be highlighted. Any relevant independence restrictions should be disclosed, including any prior contracts that the entity or individuals have been awarded with the Supreme Court of Ohio.

QUESTION #6:
May certain analysis tasks be performed by Contractor personnel located outside the United States, provided all Court data remains on U.S.-hosted systems?

ANSWER:
Respondents may use their discretion in choosing which members of their organization are involved in the project. Per Section 6.4 of the RFP, the Court is requesting a current resume and detailed information regarding experience for all key personnel that would be involved in the project, and the location of all key personnel should be noted in that information. Location of all key personnel may be considered in the evaluation process described in Section 7 of the RFP if it is reasonably determined that it may cause potential challenges in completing the project successfully.

QUESTION #7:
Is the Court able to accept proposals from a Canadian corporation with no United States place of business? Specifically, for Section 13.6, would the Court accept an IRS Form W-8BEN-E in place of a United States Federal Taxpayer Identification Number, or is a US EIN required before contract execution?

ANSWER:
The Court prefers the primary team to be based in the USA as some on-site visits are preferred. Location of the corporation and all key personnel may be considered in the evaluation process described in Section 7 of the RFP if it is reasonably determined that it may cause potential challenges in completing the project successfully. The Court can legally contract with a vendor out of the United States provided they have an active account with OhioPays, the official online financial portal managed by the State of Ohio's Office of Budget and Management (OBM) at the time of contract execution.

QUESTION #8:
May a non-US supplier or approved subcontractor may deliver remotely from England, and which registration, clearance, data-access and insurance requirements would apply?

ANSWER:
See answer to Question #7.

QUESTION #9:
Does the Court require proof of insurance at proposal submission or only before contract execution?

ANSWER:
Per Section 13(15) of the RFP, the Court reserves the right to request confirmation of insurance at any time throughout the evaluation and/or contractual negotiation process.

QUESTION #10:
Appendix D: If the Contractor has no Ohio-based employees, is Ohio workers' compensation coverage still required?

ANSWER:
Ohio workers' compensation coverage is not required if there are no employees living or working in Ohio.

QUESTION #11:
Appendix D(4) applies Professional Liability coverage "if Contractor is performing services as a licensed trade or profession." Please confirm whether E&O coverage is required for this engagement, or would a cyber/technology E&O policy satisfy the requirement, and if so, at what limit?

ANSWER:
A cyber/technology E&O policy can satisfy the requirement with the same limits outlined in Appendix D(4).

QUESTION #12:
Will contractor personnel be subject to background checks, NDAs, or specific data-handling requirements before accessing Court contracts and policies?

ANSWER:
An agreement for services with the awarded contractor will contain the following language: Contractor agrees not to disclose to any person, other than an employee of the Court, any documents marked confidential or proprietary or any nonpublic information that is identified as confidential at the time of disclosure that is obtained through or results from work performed under this Agreement.

QUESTION #13:
Will the Court provide the relevant contracts and supporting vendor security documentation for review? Will contracts, insurance policies, and policy documents be provided electronically before or at kickoff?

ANSWER:
The Court anticipates they will be provided electronically shortly after initial kickoff.

QUESTION #14:
Appendix D requires insurance placed with insurers authorized to conduct business in Ohio with an A.M. Best rating of A:VII or better, "unless otherwise agreed in writing." Would coverage placed through Lloyd's of London underwriters (A.M. Best rated A), written on a surplus lines basis, satisfy this requirement?

ANSWER:
If a foreign-domiciled insurance company is desiring to write insurance in Ohio on a nonadmitted/surplus lines basis, they must be registered and appear on the list of Eligible Surplus Lines Companies and Risk Retention Groups with the State of Ohio Department of Insurance, found here: https://insurance.ohio.gov/companies/surplus-lines/resources/ohio-eligible-sl-companies-risk-groups .

If the company is not registered, they must meet the requirements and follow the instructions provided with the State of Ohio Department of Insurance at this link: https://insurance.ohio.gov/companies/surplus-lines/resources/nonadmitted-surplus-lines-insurer-approval-annual-fee

The Supreme Court of Ohio reserves the right to require documentation of the registration and coverage at any point in the evaluation process, and it must be completed before contract execution.

QUESTION #15:
Will the awarded Contractor be eligible to compete for future implementation work arising from the roadmap and recommendations?

ANSWER:
Yes, provided that any future implementation work is procured in accordance with the Court's procurement policies and does not prejudice other prospective vendors.

QUESTION #16:
Are on site visits mandatory, and if so, how many are anticipated?

ANSWER:
The Court strongly prefers at least 2-3 on site visits, preferably for project kickoff and presentation of deliverables at the end of the project.

QUESTION #17:
Is there a budget ceiling or estimated fee range the Court may disclose?

ANSWER:
The Court does not wish to share an estimated budget for this project and encourages respondents to submit their most competitive proposal.

QUESTION #18:
Should Appendix B be priced per deliverable or as a single fixed fee? Does the contractor have the ability to specify its own payment schedule, for example, milestone-based or hourly? Does the court expect a fixed price proposal with costs for any travel built into pricing for the required deliverables?

ANSWER:
The Court is requesting a not-to-exceed fixed price proposal inclusive of all expected respondent costs incurred, including possible travel expenses, and encourages respondents to categorize and

itemize proposed costs in Appendix B. The Court will reimburse the awarded Contractor on a monthly basis for all costs incurred during that period, once an invoice and supporting documentation is provided. Delivery costs will be reimbursed after they are incurred.

QUESTION #19:
May respondents include a change management process in their proposal to address (a) Court-requested changes to the scope or deliverables, and (b) schedule or cost impacts if Court-dependent activities (e.g., providing documentation, scheduling interviews, or completing reviews and approvals) are delayed beyond agreed timeframes? If so, should these terms and any associated rates be stated in the "Price Assumptions" column of Appendix B, or elsewhere in the proposal?

ANSWER:
Respondents are free to include a change management process for any costs incurred that are Court-dependent and not outlined in the scope of the RFP and/or executed agreement. These should be included in the Price Assumptions and also can be explained and expanded upon on a separate document if necessary.

QUESTION #20:
How will "Budget and Cost Effectiveness" (25%) be scored — lowest price, value relative to scope, or another method?

ANSWER:
Value relative to scope.

QUESTION #21:
The notice on page 1 refers to a "Request for Qualifications." Please confirm this solicitation is a Request for Proposal requiring a cost proposal.

ANSWER:
This is a Request for Proposal requiring a cost proposal.

QUESTION #22:
Please confirm there are no page limits, specific templates, reporting formats, deliverable standards or font/formatting requirements beyond those stated in Section 6.

ANSWER:
There are no page limits or formatting requirements for the proposal response beyond what is stated in Section 6. There are no specific templates, formats or deliverable standards for any deliverables provided the information can be reasonably accessed and interpreted.

QUESTION #23:
Could the Court please provide the anticipated project timeline, including key milestones and the overall expected duration of the engagement?

ANSWER:
The project timeline can be found in Section 2.3 of the RFP.

QUESTION #24:
Has the Court established an anticipated project start date and key milestones within the June 30, 2027 completion deadline?

ANSWER:
As per Section 2.3 of the RFP, the Court anticipates a contract award by the end of December 2026. Key milestone dates are dependent on the details of the response, and a proposed schedule should be outlined as per Section 6.3 of the RFP with an assumption of a January 1, 2027, start date.

QUESTION #25:
Would a focused 4–8-week delivery schedule be acceptable, subject to the agreed scope?

ANSWER:
Any proposed schedules should be outlined as per Section 6.3 of the RFP with an assumption of a January 1, 2027, start date.

QUESTION #26:
Could the Court please clarify whether it intends to award this RFP to a single vendor or multiple vendors? If multiple awards are anticipated, could the Court specify the expected number of vendors to be selected?

ANSWER:
Per Section 7 of the RFP, the Court will award one contract for this project.

QUESTION #27:
Which Court staff will be designated points of contact, and approximately how many individuals from administrative leadership, the Office of Legal Counsel, and the Office of Information Technology will participate in interviews?

ANSWER:
While specific staff members have not yet been determined, respondents can expect up to ten staff members from the Office of the Administrative Director, Office of Legal Counsel and the Office of Information Technology to participate in the evaluation process.

QUESTION #28:
Is there an existing incumbent vendor currently providing cybersecurity risk assessment and governance consulting services to the Court. If an incumbent vendor is in place, could you kindly share the vendor's name and any available details regarding the existing contract, including its duration and contract value?

ANSWER:
There is no incumbent vendor currently in place for these specific services.

QUESTION #29:

Are cybersecurity policies and governance centrally managed, or will the assessment require review of separate policies and governance structures across multiple offices or courts?

ANSWER:
They are centrally managed.

QUESTION #30:
Does "audit" mean the Court requires a formal audit opinion, or is a consultative assessment with findings and recommendations sufficient?

ANSWER:
A consultative assessment with findings and recommendations is sufficient.

QUESTION #31:
Does the scope cover the Supreme Court and its administrative offices only, or does it also include the lower courts (courts of appeals, common pleas, municipal) and other judicial branch entities or shared systems?

ANSWER:
The Supreme Court of Ohio and its administrative offices only.

QUESTION #32:
Approximately how many Court staff, offices, and locations are in scope?

ANSWER:
See answer to Question #31. There are approximately 300 staff members at the Supreme Court of Ohio.

QUESTION #33:
Approximately how many contracts and agreements are in scope for the Contract Risk Assessment Review (Section 4.1(5)), broken out by IT vendor contracts, insurance policies, and other agreements?

ANSWER:
There are approximately 20 IT vendor agreements and less than five insurance policies for review. Other agreements would be minimal and would likely include less than ten agreement templates.

QUESTION #34:
For vendor contracts, please confirm the review is limited to cybersecurity and vendor-risk terms (e.g., data protection, breach notification, security requirements, right to audit), and that legal review of contract terms, liability, and enforceability is excluded and remains with the Court's Office of Legal Counsel.

ANSWER:
The review is limited to cybersecurity and vendor-risk terms (e.g., data protection, breach notification, security requirements, right to audit).

QUESTION #35:
What level of assessment is expected for these contracts? Should the contractor conduct a detailed cybersecurity risk assessment of each vendor, or primarily review contractual security requirements, obligations, and associated risks?

ANSWER:
See answer to Question #34.

QUESTION #36:
For insurance policies, please confirm the review is limited to whether the Court meets the policy's security requirements and whether its incident response plan aligns with the policy's notification and vendor requirements, and that evaluation of coverage adequacy, limits, exclusions, and legal interpretation of policy terms is excluded.

ANSWER:
Coverage adequacy, limits, exclusions, and policy terms should be evaluated provided they are relevant to the risk assessment, vulnerability identification, and gap analysis of the Respondent as per Section 4.1.

QUESTION #37:
Approximately how many existing written policies, procedures, and protocols are in scope to be evaluated? Approximately how many pages total?

ANSWER:
There are approximately 25-30 policies, procedures, and protocols in scope to be evaluated. Page totals vary widely from 5-25.

QUESTION #38:
Are there existing cybersecurity risk assessments, audit reports, or gap assessment results that will be made available to the contractor?

ANSWER:
Previous vendor technology assessments and penetration testing results will be made available to the awarded contractor.

QUESTION #39:
Can we assume that as part of a discovery request the Court will provide any and all requested cybersecurity documentation including application configuration, prior assessments, penetration test results, security risk analyses, previously completed cybersecurity insurance carrier questionnaires?

ANSWER:
See answer to Question #38. Any previously completed assessments within scope will be provided to the awarded contractor.

QUESTION #40:
Do "other applicable agreements" include agreements with other courts or agencies for systems the Court hosts on their behalf?

ANSWER:
No.

QUESTION #41:
Since penetration testing is excluded, is the review of "technological capabilities" in the Gap Analysis (Section 4.1(6)) limited to documentation and interviews, or does the Court expect any technical validation of security tools or configurations?

ANSWER:
Technical validation of security tools or configurations are not in scope.

QUESTION #42:
The gap analysis includes identifying weak or missing "technological capabilities," while the RFP states that penetration testing is not intended. Please clarify the intended scope of the technology component. For example, is the Court expecting (a) a review of whether security tools and controls exist and are documented, based on interviews and documentation, (b) a review of system architecture or configuration, (c) a review of existing scan or assessment results, or (d) something else? Please also confirm whether vulnerability scanning and technical configuration testing are out of scope.

ANSWER:
The scope would concentrate on a review of whether security tools and controls exist and are documented, and a review of existing scan or assessment results. Vulnerability scanning and technical configuration testing are out of scope.

QUESTION #43:
How many IT applications are in scope? By IT applications we mean any multi-user system, whether hosted in-house or via a third-party vendor, that stores and processes information important to the Court. Please estimate the number of external users (that is, not Court staff) who use these systems.

ANSWER:
Technical review of the applications is not in scope.

QUESTION #44:
How many IT infrastructure tools are in scope? By IT infrastructure tools we mean a software application that does not store the Court's business data but is important for the security of the Court's information, including for example password managers, anti-malware software, vulnerability management tools, or web application firewalls.

ANSWER:

Technical review of the applications is not in scope.

QUESTION #45:
How many enterprise applications are included in the scope for the risk assessment or GCC?

ANSWER:
Technical review of the applications is not in scope.

QUESTION #46:
Although penetration testing is excluded, may the contractor perform nonintrusive vulnerability scanning or configuration reviews?

ANSWER:
The Court is not opposed to the awarded contractor performing nonintrusive vulnerability scanning or configuration reviews provided it is discussed and planned in collaboration with the Court's stakeholders.

QUESTION #47:
Are the Court's disaster recovery plan and incident response plan currently documented, and when were they last tested? Is a tabletop exercise expected as part of this engagement?

ANSWER:
The plans are documented and will be shared with the awarded contractor. Testing is determined by a wide variety of factors and will be disclosed to the awarded contractor. A full tabletop exercise with all staff is not expected.

QUESTION #48:
What cybersecurity policies, plans, and documentation exist today (for example, policy set, incident response plan, disaster recovery/business continuity plan, risk register)? Are they current, and in what format are they maintained? When were they last reviewed and updated?

ANSWER:
Disaster recovery, incidents response plans, and continuity plans do exist and are maintained internally. Reviews and updates vary widely by policy and will be shared with the awarded contractor.

QUESTION #49:
Are your organization's IT policies aligned with a best-practice security or control framework, such as the NIST CSF, NIST SP 800-53, or ISO 27001/2? If so, which one(s)?

ANSWER:
Framework is generally aligned with NIST standards.

QUESTION #50:
When was the last time an assessment of this nature was performed?

ANSWER:
This specific service has never been solicited.

QUESTION #51:
How many IT staff members does your organization have? Of these individuals, how many are dedicated to cybersecurity? Are cybersecurity roles formally assigned to individuals within the IT organization?

ANSWER:
The Court can share that there are approximately 300 total staff members at the Supreme Court of Ohio. Details regarding dedicated cybersecurity roles will be discussed with the awarded contractor.

QUESTION #52:
Is a formal security awareness training program in place? How often is training provided to users?

ANSWER:
Yes, training is required once a year and provided by the Ohio Department of Administrative Services.

QUESTION #53:
To what degree is cybersecurity integrated into the overall business strategy or mission?

ANSWER:
Cybersecurity is an integral part of the Supreme Court of Ohio and its overall operations.

QUESTION #54:
Is a virtual dashboard optional, or a required deliverable?

ANSWER:
It is not a required component, but respondents should be able to demonstrate how all deliverables will be presented to the Court.

QUESTION #55:
How is the optional virtual dashboard scored? Does the Court want pricing for ongoing access to this platform beyond the June 30, 2027 term of the contract? How many users will require access?

ANSWER:
Approximately 10-15 users may require access. The Court recommends a pricing proposal submitted under the assumption that access will not be required past June 30, 2027.

QUESTION #56:
For the optional virtual dashboard (Sec. 4.1(7)(a)), does the Court prefer a solution hosted in its own environment (e.g., Microsoft 365/Power BI) or will a contractor-hosted platform be acceptable? Are there data-hosting or security requirements for any tool that stores Court information?

ANSWER:
The Court prefers a contractor-hosted platform. The platform should be a tool for sharing deliverables data and hosting Court data should not be applicable.

QUESTION #57:
Does the Court prefer the gap analysis be benchmarked against NIST CSF 2.0, or should other frameworks (for example, the CJIS Security Policy or NIST SP 800-53) also be referenced? Should the analysis include current and target profiles?

ANSWER:
A primary framework may be used as a benchmark, as the Court has familiarity with multiple options. The awarded contractor can choose the framework based on what they deem most applicable to current Court operations and needs.

QUESTION #58:
Is the use of NIST CSF 2.0 a preference or a requirement, given that the RFP says the contractor "may use" it?

ANSWER:
See answer to Question #57.

QUESTION #59:
Section 6.3(c) asks for examples of written reports, dashboards, and training plans. May these be sanitized samples, and will the Court accept redacted examples under the Appendix E process?

ANSWER:
The Court will accept redacted and sanitized samples, however they must still clearly illustrate examples of the capabilities of deliverables the respondent is able to provide for evaluation purposes. The Court will **not** be responsible for redaction of any samples submitted in a proposal response, as Appendix E should disclose proposed redactions of information from **the primary respondent only**. Any samples submitted must already have redactions in place.

QUESTION #60:
Section 4.1(7)(c) (Staff Training) appears under "Recommendations for Updated Governance and Procedure Plan." Please confirm whether the Contractor is expected to deliver training sessions and provide training materials to Court staff during this engagement, or to recommend and plan training as part of the written recommendations.

ANSWER:
Delivery of training sessions is not required. The awarded contractor should recommend and plan training as part of the written recommendations.

QUESTION #61:
If the contractor is expected to deliver training sessions, approximately how many staff will be trained, how many sessions are expected, and should training be delivered virtually or in person?

ANSWER:
Delivery of training sessions is not required.

QUESTION #62:
Is the contractor expected to revise and produce final policy documents, or is the requirement limited to identifying gaps and providing a policy/procedure development and revision plan?

ANSWER:
The awarded contractor should provide frameworks for policy documents and development if gaps are identified.

QUESTION #63:
Are the policies and procedures currently documented and available, or will the contractor also be expected to develop new policies and procedures where documentation is missing?

ANSWER:
See answer to Question #62. Current policies and procedures are currently documented internally and will be made available to the awarded contractor.