JUDICIAL COUNCIL OF CALIFORNIA

QUESTIONS AND ANSWERS

RFP Title: Information Systems Security Outreach Program
RFP-IT-2023-03-LP

May 22, 2023

==========

1. **QUESTION**: Are the approximately 45 courts listed in the RFP all located within northern California or throughout the state?

   ANSWER: The Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California, and this would take place throughout the state.

2. **QUESTION**: Is the Judicial Council planning to award to a single vendor or is an award to multiple vendors possible | likely?

   ANSWER: Single vendor.

3. **QUESTION**: How much notice will the Judicial Council provide before a project is anticipated to start?

   ANSWER: Please refer to RFP for the anticipated start date of the contract. Regarding the start date of assessments, the approximate advance notice time frame is typically two (2) to four (4) weeks. However, there may be a longer lead time if existing assessments are underway, resulting in new assessments being scheduled further out into the future.

4. **QUESTION**: Is small business certification with the Los Angeles County Metropolitan Transportation Authority sufficient for Judicial Council's small business declaration?

   ANSWER: To receive the small business preference, the Proposer must be either (i) a Department of General Services ("DGS") certified small business or microbusiness performing a commercially useful function, or (ii) a DGS-certified small business nonprofit veteran service agency. Please refer to Request for Proposals, Section 13, Small Business Preference for additional information.

5. **QUESTION**: Can work be performed remotely or does it have to be performed from Sacramento, San Francisco JCC sites?

   ANSWER: The assessments and other Outreach Program services are typically performed directly with the courts and are encouraged to be performed "in-person" whenever practical, and within budget. There is a "capped" budget of $40,000 per year for reimbursable travel expenses. For travel to qualify for reimbursement, Judicial Council travel guidelines must be followed, including pre-authorization. Billable work, such as report preparation, and other non-in-person work activities supporting the Outreach program may be performed remotely but must be within the continental United States.

6. **QUESTION**: Can personnel be remote working through jump hosts onsite in Sacramento? (i.e., We have CJIS certified penetration testers in multiple states and want to know if they can be utilized on the project)

   ANSWER: Please refer to the response to question 5.

7. **QUESTION**: The RFP states that the dollar cap 1,040,000 per year. Does this mean you agree to cap the hours worked at the 1,040,000 / Blended Rate?

   ANSWER: The dollar cap of $1,040,00.00 has two components. $1,000,000.00 for services at the blended rate, and $40,000.00 for travel.

8. **QUESTION**: Are you looking for part-time personnel or full-time personnel to support this effort?

   ANSWER: There is no requirement. Staffing is up to the vendor.

9. **QUESTION**: What type of remediation work is being requested in the following statement "…includes meaningful assistance in the implementation of recommendations and / or remediation findings rather than the simple performance of a discovery/review process and the reporting of findings without follow-on support"?

   ANSWER: Consultative services on a variety of security program topics (e.g., policy development, strategic planning, playbook development, and tabletop exercises).

10. **QUESTION**: What is the percentage of work being requested by job title / job level / function?

    1. Information security consulting services
    2. Information systems policy and procedure development, review, and revision
    3. Standards-based risk assessments, controls reviews and testing
    4. Both Black and Grey Box Penetration testing.
    5. Information systems process reviews and process engineering
    6. Information technology project reviews in support of the identification of potential points of failure
    7. Prepare and deliver information security-related training.
    8. Program and project management services in support of the Information Systems Security Outreach Program.

    ANSWER: Cannot be defined because each assessment varies, and the post assessment work will vary based on the outcome of each assessment. The work will be consulting services 100% of the time and job titles, roles and levels will vary based on the assigned assessment.

11. **QUESTION**: Are there any controls implementations that have been identified that have a deadline for implementation?

    ANSWER: No.

12. **QUESTION**: Does the JCC have an existing security checklist that can be shared?

    ANSWER: The checklist may vary at each entity but is based upon or derived from the NIST, ISO 27000, CJIS, and CIS controls.

13. **QUESTION**: Can the JCC provide an estimate of the number of professional service hours per year?

    ANSWER: Approximate number of hours can be derived from $1,000,000.00 divided by the blended rate.

14. **QUESTION**: We can cover the scope with CALNET-NG. Will the JCC accept CALNET-NG in place of the terms and conditions of the RFP?

    ANSWER: No.

15. **QUESTION**: If we redline the RFP terms and conditions and if our requested changes are accepted by the JCC, will we still receive 10 points for this line item in the evaluation and scoring? If not, how many points would be given?

    ANSWER: The JCC will not "accept" any redlined changes to the standard terms and conditions that are submitted with a bid. The redline will simply be reviewed and evaluated along with the other bid materials. A contract will be negotiated, if necessary, after a bid has been awarded. Whether the JCC deducts some or all of the available ten points will depend on the particular exceptions we receive from the bidder in any redline submitted with a bid.

16. **QUESTION**: Can we provide any of the security services remotely?

    ANSWER: Please refer to the response to question 5.

17. **QUESTION**: Has JCC engaged with a 3rd party to help write the RFP or provide materials for the RFP? If so, please share the name of the company.

    ANSWER: No.

18. **QUESTION**: Depending on the answers to our questions and the answers to questions from others we may need some time to update our response. For that reason, can you move out the proposal response deadline by 1 to 2 weeks?

    ANSWER: No.

19. **QUESTION**: For information security related training, how many total users does the Judicial Council have in scope for this training?

    ANSWER: The total number of users would range from 10 to 4,000 total users and be dependent on the requesting court.

20. **QUESTION**: Is the Judicial Council looking for the development of a formalized Security Awareness and Training program?

    ANSWER: No, the development of a formalized security awareness and training program would be out of scope for this RFP, but a court may ask for guidance with/or a review of their existing program.

21. **QUESTION**: Are phishing campaigns expected to be within scope of the security related training?

    ANSWER: No.

22. **QUESTION**: How many endpoints are each location?

    ANSWER: We don't have exact counts for each court but does vary from 10 to more than 4,000.

23. **QUESTION**: How many endpoints are in scope total for this Project?

    ANSWER: More than 20,000.

24. **QUESTION**: Are all accounts and main access controls managed from a centralized source (e.g., centralized Active Directory)?

    ANSWER: No, each entity manages its own centralized Active Directory.

25. **QUESTION**: Does the Judicial Council have a vulnerability management program in place today?

    ANSWER: Yes, the Judicial Council has a vulnerability management program in place.

26. **QUESTION**: Is the cost of the licenses for vulnerability scanning assumed by the Contractor?

    ANSWER: The Judicial Council already has a vulnerability scanning service in place. Regarding penetration testing the Contractor would supply and assume the cost for the penetration testing tool.

27. **QUESTION:** Does the Judicial Council have a patch management program in place today?

    ANSWER: Yes, the Judicial Council has a patch management program.

28. **QUESTION**: Is physical security expected to be within scope for this Program?

    ANSWER: Yes, but this will differ between entities being assessed. Some will want physical security assessed while others will not.

29. **QUESTION**: How many IT Risk assessments are expected per court per year?

    ANSWER: One.

30. **QUESTION**: Are application security scans expected to be within scope of the Project?

    ANSWER: Yes.

31. **QUESTION**: Does the Judicial Council have their own SIEM and SOC?

    ANSWER: Yes.

32. **QUESTION**: Is a SIEM and SOC expected to be within scope of the Project?

    ANSWER: No.

33. **QUESTION**: Is Incident Response, including Investigations, expected to be within scope of the Project?

    ANSWER: Yes, but this is limited to development and assessment of incident response and investigations of policies, process documentation, playbooks and or program materials.

34. **QUESTION**: Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?

    ANSWER: The current Contractor is eligible to bid on this project. To obtain the information requested, you need to request the records through Public Access to Judicial Administrative Records (PAJAR). However, this will not excuse you from submitting your proposal on time. Please refer to this link: https://www.courts.ca.gov/requestforms.htm.

35. **QUESTION**: Specify the VLAN details how many are included in the Scope?

    ANSWER: VLAN details will differ with each entity.

36. **QUESTION**: Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

    ANSWER: Infrastructure details differ with each entity and will be shared after the bid has been awarded.

37. **QUESTION**: How much (%) of the infrastructure is in the cloud?

    ANSWER: The majority of entities have a cloud presence, but the percentage varies for each.

38. **QUESTION**: In the IT department/environment, how many employees work?

    ANSWER: This varies for each entity from 1 to 200+ IT staff.

39. **QUESTION**: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    ANSWER: Each entity maintains its own on-premises data center or cloud environment.

40. **QUESTION**: Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

    ANSWER: Please refer to the response to question 7 and the Request for Proposals, Section 5, Payment Information.

41. **QUESTION**: Scope related. Of the 400 hours expected to establish the advising and implementation engagements, do these include the implementation and monitoring aspects around remediation services? Or above and beyond.

    ANSWER: Active monitoring is out of scope for the Outreach Assessment program but there may be involvement with implementation, and revisions to incident and remediation plans, policies, tools, and other related materials.

42. **QUESTION**: What is/are the current established framework(s) that the courts are utilizing? Program FW? Risk Management FW? and/or Control FW? Or will this be a greenfield opportunity to build a new program?

    ANSWER: All frameworks will be discussed and evaluated per each Judicial Branch entity assessed to determine if new opportunities exist.

43. **QUESTION**: Will Project Management from a court's perspective be a part of the implementation phase, to coordinate with the contractor's PM?

    ANSWER: The Contractor's project manager will manage, coordinate and document all phases of the security outreach assessments, but will partner/collaborate with an assigned court or JCC team member to carry out the assessment activities, schedule interviews, request documentation, perform requests, submit reports, etc.

44. **QUESTION**: Will the court's IT team be able to participate and coordinate with the contractor's team to implement and monitor in a collaborative fashion?

    ANSWER: Yes.

45. **QUESTION**: Is the advisory team expected to be on-site 100% of the time of can virtual meetings and discussions be available?

    ANSWER: Please refer to the response to question 5.

46. **QUESTION**: On average, how many IP addresses are expected to be penetration tested for a small/medium court?

    ANSWER: This will vary.

47. **QUESTION**: Will the Penetration tests take place on External Facing Networks or Internal Facing Networks?

    ANSWER: Both external and internal.

48. **QUESTION**: How many penetration test assessments are projected to be Gray Box Penetration Tests and how many are projected to be Black Box Penetration Tests?

    ANSWER: There will be approximately 12-15 entity assessments per year, and each assessed entity will have the option of requesting a pentation test. Gray Box or Black Box tests, if any, will be a determination made by each entity as part of the assessment scoping process.

49. **QUESTION**: Is the expectation that the vendor be performing assessments at all 45 courts over a 3-year period or 45 courts per year? If over the 3-year period, is it safe to assume 15 courts assessed per year?

    ANSWER: The Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California. We anticipate approximately 12-15 courts will be assessed per year, for each initial year of the contract and for each additional year of the contract if the contract is extended.

50. **QUESTION**: What is the total number of expected courts per year needing Penetration Tests?

    ANSWER: We anticipate approximately 15 penetration tests per year.

51. **QUESTION**: Is all of the assessment and penetration testing expected to be performed on site? Will any remote testing be allowed?

    ANSWER: Please refer to the response to question 5.

52. **QUESTION**: Will any clearances be required to perform this service for the Judiciary?

    ANSWER: Background checks will be required for all staff involved.

53. **QUESTION**: Will there be any travel to courts around the state or is the expectation to do 100% of the assessments from the Sacramento/SF offices?

    ANSWER: Please refer to the response to question 5.

54. **QUESTION**: What are the main topics to be included in the cybersecurity training?

    ANSWER: The topics of the Judicial Branch security awareness training program include, but is not limited to, all the security frameworks listed in the response to question 12, industry best practice as well as new and advanced threats.

55. **QUESTION**: Is there an expected amount of time allotted for each training course?

    ANSWER: This will be determined on a case- by-case basis.

56. **QUESTION**: How many learners are expected in each session of the cybersecurity training classes?

    ANSWER: This will vary based on if the training is in person or virtual, and also be determined based on room capacity and virtual platform attendee limits.

57. **QUESTION**: Is the training expected to be held virtually or on-site?

    ANSWER: Both.

58. **QUESTION**: If the training is to be conducted virtually, who is responsible for hosting the training environment?

    ANSWER: The Judicial Branch hosts.

59. **QUESTION**: If the training is to be held onsite, who is responsible for procuring the training location?

    ANSWER: The Judicial Branch provides the facilities.

60. **QUESTION**: Is the estimate of 400 hours of effort estimated per court engagement inclusive of all bulleted services in 2.2.4?

    ANSWER: The scope of engagement at each entity varies and may include any of the bulleted services in section 2.2.4.

61. **QUESTION**: Do the 45 smaller/midsize courts share the same networking backbone as Judicial Council ITO? If so, who is responsible for engineering/administering the shared network?

    ANSWER: No. The Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California. Each court maintains a network independent of the Judicial Council network. A common wide area network is shared by the branch.

62. **QUESTION**: Do the 45 smaller/midsize courts leverage the same security tools as each other? Same security tools as Judicial Council ITO?

    ANSWER: Yes, the Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California. Most of the courts as well as the Judicial Council leverage the same tools.

63. **QUESTION**: What security services (if any) does Judicial Council ITO provide to the courts? Incident Response? Architecture?

    ANSWER: The Judicial Council ITO makes available various security services including SOC, SIEM, endpoint protection, incident response, vulnerability scans, security assessments, phishing campaigns, and security awareness training.

64. **QUESTION**: Does the Judicial Council ITO provide email services to the in-scope courts?

    ANSWER: No. Each court manages its own email services.

65. **QUESTION**: Is the Judicial Council expecting one roll up report encompassing findings of the assessments of the 45 smaller/midsize courts? Or individual reports for each court?

    ANSWER: The Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California. Each court receives its own confidential assessment report. An additional anonymized rollup report is provided to the Judicial Council quarterly.

66. **QUESTION**: Does each court follow its own set of technology policies? Or do they adhere to policies published by the Judicial Council?

    ANSWER: Each court follows its own set of technology policies.

67. **QUESTION**: Beyond an Incident Response Policy, what is the anticipated quantity and type of policy documents that will need to be revised or implemented for each court?

    ANSWER: Policy documentation quantity may differ for each court and will be determined as part of the assessment or upon court request.

68. **QUESTION**: Will the Judicial Council consider extending the RFP deadline to June 9, 2023? What is the approximate size of the target address space to be assessed for each of the courts (e.g., one class B network, three class C networks, etc.)?

    ANSWER: No, the dates are firm until notified otherwise. Court staff size ranges from 10 to 4,000+ throughout the state. Target address space varies across the state.

69. **QUESTION**: Is there any overlap or shared resources between courts that would be in scope?

    ANSWER: Generally, there is no overlap.

70. **QUESTION**: Are your user workstations mostly Windows systems (if so, what version? 7 or 10?)? Are they Mac/Unix?

    ANSWER: Mostly Windows (the supported versions).

71. **QUESTION**: Approximately how many workstations and how many servers exist within the internal address space?

    ANSWER: This varies for each entity, from 25 to 5,000 total workstations/servers per court.

72. **QUESTION**: What is the scope of the penetration testing work. Will this be exclusively an assessment of the internal network? Or will there be an external component?

    ANSWER: Penetration testing will be both external and internal.

73. **QUESTION**: If an external test is requested, what is the approximate number of live IPs that would be in scope?

    ANSWER: Depends on the entity assessed.

74. **QUESTION**: Are there any assets hosted in the cloud that would be in scope? If so which cloud providers?

    ANSWER: Cloud assets are within the scope. Cloud providers vary. Contractor must be able to work with all major Cloud providers.

75. **QUESTION**: Vendor X prefers to perform this work remotely by either sending a virtual machine for remote deployment, shipping a physical device that connects back to Vendor X systems, or through provisioned accounts for the corporate VPN or other remote access system. Are you able to provide remote access to the internal network for this effort or does it require on-site work?

    ANSWER: This will be determined on a case-by-case basis, by the entity being assessed in accordance with their policies, standards, infrastructure, and security practices.

76. **QUESTION**: One of the deliverables JCC mentions in the RFP is a security checklist. Can you describe what JCC envisions for the Information Security Checklist in more detail?

    ANSWER: Please refer to the response to question 12.

77. **QUESTION**: Will the security team have to travel to various courts throughout the state during an engagement with a court? For example, will a technical resource need to be onsite at that court for implementation assistance?

    ANSWER: Please refer to the response to question 5.

78. **QUESTION**: We understand the engagement is a collaborative effort, so why grey or black box testing instead of white box testing? Are you open to different approaches if deemed appropriate by our staff working in collaboration with the JCC and court staff?

    ANSWER: We are only interested in black box and gray box testing.

79. **QUESTION**: Reference to support tickets & requests, is that in reference from the contractor to JCC?

    ANSWER: The mechanism to log and track assignments, projects, support tickets and requests will be maintained by the Contractor. This is not just applicable for the JCC. There may also be tickets and requests submitted by courts. The Contractor will provide reports to the JCC on all open tickets and the status of the tickets.

80. **QUESTION**: Do you have a current ticketing system?

    ANSWER: Not applicable. Please refer to the response to question 79.

81. **QUESTION**: Reference is made to "implementation assistance, please elaborate, is this strategic or implementation tools? If tools which tools?

    ANSWER: The Contractor will provide guidance on security strategies and frameworks. Additionally, the Contractor may assist with the development of security documentation. The Contractor will not implement security tools.

82. **QUESTION**: How mature are your current security program?

    ANSWER: The maturity level of Judicial Branch entities may vary.

83. **QUESTION**: Do you currently have any security tools or programs for your Threat Intelligence?

    ANSWER: Yes.

84. **QUESTION**: Do you have any monitoring security tools and if so please specify.

    ANSWER: Yes, the Judicial Branch has security monitoring tools. Specific tools will be reviewed and discussed as part of the outreach assessments.

85. **QUESTION**: Could the training be a once off per year or quarter, what is the expectation please?

    ANSWER: The Contractor may be asked to participate in the Judicial Branch webinar trainings that are currently held at least once per quarter. The Contractor will not be asked to assist with ongoing subscription/licensed based security awareness training. Additionally, on occasion the Contractor may be asked to present on site in meetings.

86. **QUESTION**: Any specific type of training you have in mind, i.e., security awareness or?

    ANSWER: Please refer to the responses to questions 54 and 85.

87. **QUESTION**: Is specific clearance required, if yes, which please?

    ANSWER: Yes. Background checks are required for all staff.

88. **QUESTION**: Do you have a asset management program or tool? if so which one

    ANSWER: This will vary for each entity.

89. **QUESTION**: Do you have a DLP program, if so, who is the vendor?

    ANSWER: This will vary for each entity.

90. **QUESTION**: What is the process to add staff/people to the contract to supplement staffing when needed

    ANSWER: This is up to the Contractor and should be specified in the proposal. Background checks for new staff are required. Advance notification to and approval from the Judicial Council is required.

91. **QUESTION**: Is US citizenship required for the staff on this contract?

    ANSWER: No, but staff must be lawfully permitted to work in the US. All Judicial Branch assets and data must be assessed and stored within the US.

92. **QUESTION**: Is there a limitation on the length, number of pages for the proposal response? If yes, what is the maximum number of pages for the proposal response?

    ANSWER: There is no limitation on proposal length.

93. **QUESTION**: Please clarify how many hours should be assumed within a given year? For example, should offerors assume 2080 hours, 1920 hours when determining the blended hourly rate.

    ANSWER: The Judicial Branch has 14 holidays a year. A Contractor cannot work on premise or access data without Judicial Branch personnel oversight, but a Contractor could possibly perform other reporting or administrative work without being onsite. The “offeror” may assume any number of hours necessary to prepare their bid. Bids should meet RFP cost and billable specifications for consideration.

94. **QUESTION**: May a contractor perform portions of this work off-site?

    ANSWER: Please refer to the response to question 5.

95. **QUESTION**: Is retainage applicable to an hourly rate bid? If applicable when is the retainage released? annually? Quarterly?

    ANSWER: Invoicing is done in arrears after work has been performed.

96. **QUESTION**: Security Check list and Policies available to bid participants before submission is due?

    ANSWER: Please refer to the response to question 12.

97. **QUESTION**: What are the existing security tools available to the courts? I.e., IT review questions….

    ANSWER: The Judicial Branch utilizes a variety of security tools that align with industry best practices and security frameworks; and the specific vendor/provider can vary by

court. The security programs, postures, and various tools used are all items that will be reviewed as part of the security outreach assessments that are performed.

98. QUESTION: Are current security tool data collection part of the consultant duties?

ANSWER: No.

99. QUESTION: Are consultants going to be issues Courts network/OS credentials for use during the project? Non pen testing.

ANSWER: No.

100. QUESTION: How many courts are there in total?

ANSWER: The Judicial Branch is made up of the Judicial Council plus 65 courts.

101. QUESTION: What is the status of larger and smaller courts that makes the (45) courts of 300 or less users the focus?

ANSWER: The Judicial Branch consists of 58 Trial Courts, 6 Appellate Courts, and the Supreme Court, plus the Judicial Council of California. The small to medium size courts are prioritized but all courts can request and obtain security outreach assessments which are typically scheduled on a first come first serve basis. If there is a scheduled conflict due to multiple requests, the Contractor will partner with the JCC to determine the schedule prioritization.

102. QUESTION: Please confirm that only the Project Manager is to be considered as the Key Personnel.

ANSWER: The Project Manager is one of the Key Personnel. Key personnel should be identified based on the job duties and responsibilities needed to perform the assessments and the contractual obligations that will be identified and assigned by the Contractor.

103. QUESTION: Is the Information Security Checklist available to the public, and if so, where can it be found?

ANSWER: Please refer to the response to question 12.

104. QUESTION: Are any additional compliance standards required, such as CJIS, for any system or sub-systems of this engagement?

ANSWER: Please refer to the response to question 12.

105. QUESTION: Is a contractor presence required in person at the primary or secondary location for the duration of the contract or have provisions been put in place to allow for remote work due to COVID and the nature of this work? If remote work is allowed, are there any functions requiring physical access other than on-site security assessments or Penetration Testing efforts?

ANSWER: Please refer to the response to question 5.

106. QUESTION: Are all councils and courts utilizing the same system impact-level?

ANSWER: Impact-level may vary by entity.

107. QUESTION: Does each council and court utilize the same policies and procedures?

ANSWER: No. Policies and procedures will vary by entity.

108. QUESTION: How many assessments or policy reviews could potentially be conducted at the same time?

ANSWER: The Contractor's resources and bandwidth will determine that.

109. QUESTION: Will specific 800-53 control assessments be required as part of the risk assessment or will control status be maintained elsewhere?

ANSWER: Please see the response to question 12.

110. QUESTION: For Black box testing, how do we verify the hosts are owned by the organization?

ANSWER: Testing will be coordinated with the entity and include the targeted hosts.

111. QUESTION: For Black box testing, does JCC want the testing to be evasive?

ANSWER: Evasive testing is not a requirement, but it may be desired by a court. If this is something that is offered in your penetration testing, please specify it in your proposal.

112. QUESTION: Does JCC want both perimeter and internal testing?

ANSWER: Both.

113. QUESTION: If you want perimeter testing, how many perimeter hosts do you want tested?

ANSWER: Amount varies for each entity.

114. QUESTION: Do we need to be onsite for every assessment or review?

ANSWER: Please refer to the response to question 5.

115. QUESTION: Can offshore resources be utilized?

ANSWER: No.

116. QUESTION: Can you provide the number of hours utilized per year on the previous contract?

ANSWER: No. It varies per year based on the type of work requested from the courts.

117. QUESTION: Can you provide an estimated number of full-time resources used at a given time on the previous contract?

ANSWER: No.

118. QUESTION: Can you provide an estimated number of part-time resources used at a given time on the previous contract?

ANSWER: The previous Contractor used 4-6 staff. However, new bidders should determine the number of staff (part-time and/or full-time) to be used based on their proposed plan to meet the requirements of the RFP.

119. QUESTION: RFP-IT-2023-03-LP-, Section 7.d (Pg 9/16). The RFP requires 3 references at a minimum with names, addresses, and telephone numbers. Given the sensitive nature of security work, and in certain cases confidentiality agreements, some of our clients do not allow us to disclose identifying information within proposals. Can the identifying information be anonymized in the proposal and provided directly to the Judicial Council of California's procurement official upon request?

ANSWER: Bidders must complete the requirement for references.