Office of the State Auditor

Kerri L. Hunter, CPA, CFE
State Auditor

April 5, 2024

A Request for Proposals for an IT Performance Audit of Cybersecurity Resiliency at the Judicial Department

Responses to Prospective Bidder Inquiries

<u>Questions from Firm #1:</u>

1. How many of the following are in-scope for this project?

   OSA Response: We are not completely clear on the inquiry; responses to inquiries 2-9 may provide additional information.

2. External Penetration Testing – if so, What is the total number of external IPs?

   OSA Response: External penetration testing would not be in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

3. Internal Network Vulnerability Testing – if so:
   a. Do you require credentialed scanning ?
   b. How are the assets separated - broadcast domains? By VPNs? By VLANS?
   c. What are the subnet sizes ?
   d. Do you utilize Microsoft Intune ?
   e. Do you utilize site-to-site VPNs ?

   OSA Response: The OSA is not subject to the audit procedures. As stated in the RFP the Judicial Department is subject to the audit procedures. Internal network penetration testing would not be in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

4. Web Application Security Testing – if so, how many applications are in-scope?

   OSA Response: Web application vulnerability assessment and penetration security testing would not be in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

5. Wireless Penetration Testing in-scope ? If so, how many sites ?

   OSA Response: Wireless penetration testing is not in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

6. Physical Penetration Testing, if so, how many facilities will be in-scope ?

   OSA Response: Physical penetration testing is not in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

7. Do you require an assessment of your Information Security (IS) Policies ?
   a. If so, how many are presently defined and implemented, and are there any that need to be developed from scratch ?

   OSA Response: The OSA is not subject to the audit procedures. As stated in the RFP the Judicial Department is subject to the audit procedures. According to the objective on page 9 of the RFP, "The objective of this IT performance audit will be to determine whether ITS has adequate cybersecurity practices in place to identify, protect, detect, respond to, and recover from cybersecurity events that could impact the Judicial Department's critical infrastructure, IT systems, data, and business operations. To achieve this objective, the Contractor shall use criteria established in accordance with Colorado statutes or other state requirements; ITS's adopted policies, procedures, or standards; and other industry leading practices or standards, as applicable."

   Once the engagement commences, this information should be requested, by the selected Contractor from Judicial. The selected Contractor should then assess and utilize the information, as necessary, during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

8. NIST CSF 2.0?

   OSA Response: We are unclear on this inquiry. NIST CSF 2.0 would fall under the statement made on page 9 of the RFP, in that it could be utilized by the Contractor, "as criteria established in accordance with Colorado statutes or other state requirements; ITS's adopted policies, procedures, or standards; and other industry leading practices or standards, as applicable."

9. Are any of the following assessments also in-scope ?
   a. Network Architecture Evaluation
   b. Firewall Configuration Assessment (VPN, DMZ, VLAN)
   c. Server Evaluation Assessment (Physical and Virtual)
   d. Data Store Review and Security Assessment
   e. Microsoft AD, Azure AD and O365 Configuration Assessment
   f. Mobile Device Management Assessment

   OSA Response: The objective of this audit will be to determine whether ITS has adequate cybersecurity practices in place to identify, protect, detect, respond to, and recover from cybersecurity events that could impact the Judicial Department's critical

infrastructure, IT systems, data, and business operations. As such, the intent of this audit will be to assess the cybersecurity practices that are overseen and managed by ITS, which may include practices to manage the areas or infrastructure components noted above. Upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to include obtaining any necessary information from Judicial to assess and utilize during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

Questions from Firm #2:

10. Is this the first time that you will contract a vendor for the services in question? If not, then would a copy of the final contract and amount of the previous successful vendor be available?

    OSA Response: To our knowledge, this is the first time for a contract request of these types of services at Judicial from our office.

11. Is there a not-to-exceed budget for this project that you can share?

    OSA Response: No budget information is available to share at this time. The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered. The OSA will consider all proposals submitted with the required total cost information.

12. Please provide a high-level overview of the technical infrastructure in place the organization so that we can get an idea of the complexity involved.

    OSA Response: While we understand the reason for the requested information, we do not plan to publicly release even high level technical infrastructure details that may be inappropriately used by a malicious actor. Therefore, upon the commencement and during the planning phase of the audit, the selected Contractor will need gain an understanding to obtain this type of information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

13. How many key individuals (approximately) would need to be interviewed?

    OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

14. How many different locations are in scope? How far are these locations from each other?

    OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the

information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

15. How comprehensive is the cybersecurity documentation of your organization? Do you have documented policies and procedures? Do you have a documented incident response plan? Do you have a documented business continuity plan? Do you have a documented cybersecurity program?

    OSA Response: The OSA is not subject to the audit procedures. As stated in the RFP the Judicial Department is subject to the audit procedures. Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

16. Is there a specific NIST publication that you would like to align this project's methodology with? Please provide.

    OSA Response: NIST specific publications would fall under the statement made on page 9 of the RFP in that it could be utilized by the Contractor, "as criteria established in accordance with Colorado statutes or other state requirements; ITS's adopted policies, procedures, or standards; and other industry leading practices or standards, as applicable."

    Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

17. Is there a specific driver (an incident, a litigation, any other event, etc.) for this project?

    OSA Response: No, there is not a "specific driver" for this engagement. According to Section 2-3-103, C.R.S., the Colorado State Auditor is granted broad authority to conduct performance IT audits of all state departments and agencies, public colleges and universities, the Judicial Branch, most special purpose authorities, any state entity designated as an enterprise, and other political subdivisions as required by law.

<u>Questions from Firm #3:</u>

18. Clarification on the scope of the audit –
    a. In the RFP, the Judicial Department's IT services area (ITS) is responsible for the Judicial department and the 10 independent agencies or potentially responsible?
    b. Can the 10 independent agencies govern their own and choose separate cybersecurity measures and processes?
    c. How many separate infrastructure environments (networks, VMs, etc.) are used to support the judicial departments and independent agencies for which ITS is responsible for cybersecurity resiliency?

OSA Response:

1. ***Yes, pages 4-8 of the RFP states this information.***
2. ***Once the engagement commences, the selected Contractor will need to gain an understanding of Judicial, including its 10 independent agencies, during the planning phase of the audit. The selected Contractor should then assess and utilize the information, as necessary, during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.***
3. ***While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. Once the engagement commences, the selected Contractor will need to gain an understanding of Judicial, including these 10 independent agencies, during the planning phase of the audit. The selected Contractor should then assess and utilize the information, as necessary, during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.***

19. With respect to the State chief information security officer (CISO) – Is the Judicial Department required to submit an Agency Cybersecurity Plan?

    OSA Response: As stated on page 6 and 8 of the RFP, the Judicial Department is defined as a "public agency," and therefore is required by Section 24-37.5-404 C.R.S., as a "public agency," to submit an Agency Cybersecurity Plan to the State's Chief Information Security Officer.

20. The RFP discusses definitions from NIST, should we consider reviewing and cybersecurity resiliency as defined in Colorado statutes and ITS policies and procedures specifically against the NIST Cybersecurity Framework 2.0?

    OSA Response: Once the engagement commences and during the planning phase of the audit, the selected Contractor will need to gain an understanding of Judicial to determine whether Judicial prescribes to the NIST Cybersecurity Framework 2.0. The selected Contractor should then assess and utilize the information, as necessary, during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

21. Do you have an anticipated budget/cost range that you can share for this project?

    OSA Response: No budget information is available to share at this time. The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered. The OSA will consider all proposals submitted with the required total cost information.

22. Do you have an automated workpaper tool that we should document our work in or is Microsoft products acceptable?

OSA Response: The contract template included in the RFP on pages 23-62 does not require a specific automated tool to be utilized by the selected Contractor. However, the selected Contractor should ensure it is able to comply with Section 9, Contractor Records, within the contract as well as any other sections of the contract related to workpaper documentation, including Exhibit E, Information Security Policy for Contractors.

Questions from Firm #4:

23. How many court buildings and Department offices does the ITS division provide services to?

    OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

24. How many end points are is the ITS division responsible for?

    OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

25. How many applications is the ITS division responsible for?

    OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

26. How many networks is the ITS division responsible for?

    OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when

planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

27. How far along is Judicial in the process of inventorying data types (e.g., SSN) across it's environment?

    OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

28. When was the last time Judicial had a business impact assessment (BIA) completed?

    OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

<u>Questions from Firm #5:</u>

29. Page 10 of the RFP states, "The intent of this audit will be to assess the cybersecurity practices that are overseen and managed by ITS. Page 6 of the RFP states that the ITS Information Security Team, "...is responsible for protecting the confidentiality, integrity, and availability of Judicial Department applications, systems, and networks, except for potentially the ten independent agencies of the Department noted above. Can you provide additional insight into the factors that could impact whether these ten independent agencies fall within the responsibility of ITS? Can you provide any additional insight into whether the cybersecurity practices of these independent agencies should be considered as overseen and managed by ITS?

    OSA Response: Although the Colorado constitution and relevant statutes would be the primary factors impacting whether Judicial's ten independent agencies fall within the responsibility of ITS, there may be other factors, such as formal or informal agreements between the various agencies, which could have additional impact. However, we are unclear as to what these factor are or may be. Thus, we have a specific audit objective related to this, and it is something we would expect the selected Contractor to determine through the course of the audit and in achieving the related audit objective.

30. Page of 10 of the RFP states, "If the Department has certain cybersecurity practices that are independent of ITS, these practices should be excluded from the scope of this audit. Can you provide any examples of Department cybersecurity practices would be independent of ITS?

    OSA Response: Examples of cybersecurity practices may include identity and access management, asset management, physical security, risk management, security planning,

configuration management, vulnerability and patch management, audit log management and monitoring, incident response, contingency planning, and training and awareness.

31. Are the ten independent agencies listed on pages 4 and 5 of the RFP also considered public agencies as defined in statute [Section 24-37.5-102.(26), C.R.S.], which was quoted on page 6 of the RFP?

    OSA Response: Based on our interpretation of the relevant statutes, Judicial's ten independent agencies would be included as public agencies. However, we are uncertain as to whether there may be any other factors that exclude them as such. Thus, we have a specific audit objective related to this, and this is something we would expect the selected Contractor to determine through the course of the audit and in achieving the related audit objective.

<u>Questions from Firm #6:</u>

32. Regarding the IT Performance Audit of Cybersecurity Resiliency solicitation, can you tell us if the OSA will want the vendor to fully own the audit and deliverables, or if they envision this as a co-sourcing arrangement in which the audit leverages the vendor as a subject matter expert?

    OSA Response: We expect the selected Contractor to "fully own the audit and deliverables."

33. What is OSA's budget for this project?

    OSA Response: No budget information is available to share at this time. The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered. The OSA will consider all proposals submitted with the required total cost information.

34. Is the Judicial Department aligned with NIST CSF or another security framework?

    OSA Response: NIST specific publications would fall under the statement made on page 9 of the RFP in that it could be utilized by the Contractor, "as criteria established in accordance with Colorado statutes or other state requirements; ITS's adopted policies, procedures, or standards; and other industry leading practices or standards, as applicable."

    Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

35. How many IT policies, procedures, standards, and guidelines are in place?

    OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this from Judicial, as necessary, during the planning phase of

the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

36. How many staff interviews are aniticipated as needed?

    OSA Response: See response to inquiry 13.

37. External Network
    a. Approximately how many external IPs are active in the Judicial Department's network?

       OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

38. Internal Network
    a. Approximately how many IPs or subnets are in scope?
    b. Can all internal network testing be done from a single location?

       OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

39. Firewall Configuration
    a. Are firewall configuration reviews in scope?
    b. Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?
       OSA Response: Firewall configuration reviews would not be in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

40. Router | Switch Configuration
    a. Is router | switch configuration review in scope?

       OSA Response: Router | switch configuration review would not be in scope for this engagement. Please refer to page 9 of the RFP for the audit objectives, scope and methodology.

41. Web Applications

a. How many web applications are in scope?
b. Are the web applications Internet-facing or internal only?

OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

42. Enterprise Applications
    a. How many enterprise applications are in scope?
    b. Are the enterprise applications COTS or internally developed?

OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

43. Database Security
    a. How many unique databases are in scope for database-specific testing?
    b. If databases are in different locations, can all locations be reached from one central location?

OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

44. Server Configuration Analysis
    a. How many servers and unique server brands are in scope for assessment?

OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

45. Wireless Network

   a. Is the wireless network controller-based or access-point-based?
   b. How many locations are in scope for wireless network assessments?

   OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

46. Mobile Device Management

   a. Is there an MDM solution; if so, what is the vendor?

   OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

47. Endpoint Security Review

   a. How many endpoints are in scope?

   OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to obtain this information from Judicial, if necessary. The selected Contractor should then assess and utilize the information during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

48. Cloud Security Configuration

   a. How much of the Judicial Department's environment is in the cloud?

   OSA Response: While we understand the reason for the requested information, we do not plan to publicly release details that may be inappropriately used by a malicious actor. Therefore, and upon the commencement of the engagement, the selected Contractor will need gain an understanding during the planning phase of the audit to include obtaining this information from Judicial. The selected Contractor should then assess and utilize the information, as necessary, during its risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

49. How many data centers are in scope?

OSA Response: Once the engagement commences, the selected Contractor will need to gain an understanding of this type of information from Judicial, as necessary, during the planning phase of the audit. The selected Contractor should then assess and utilize the information during the Contractor's risk assessment procedures and when planning the work necessary to satisfy the evaluation objectives, project deliverables, and timelines, as outlined in the RFP.

Questions from Firm #7:

50. Is the RFP for cybersecurity audit only including IT or does it include the OT (Operational Technology) environment as well?

OSA Response: The RFP is requesting services for the following: "The objective of this IT performance audit will be to determine whether ITS has adequate cybersecurity practices in place to identify, protect, detect, respond to, and recover from cybersecurity events that could impact the Judicial Department's critical infrastructure, IT systems, data, and business operations." The scope of the RFP does not include whether Judicial has an adequate operational technology environment in place.