May 17, 2019

A Request for Proposal for an Evaluation of Information Technology Security at the Colorado Department of Transportation

Response to Bidder Inquiries

1. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services?

   There is currently not an incumbent company or previous incumbent who has completed similar contract performing these services for the OSA.

2. If so - can you please provide incumbent contract number, dollar value and period of performance?

   N/A, see response to question 1.

3. Are you satisfied with incumbent performance?

   N/A, see response to question 1.

4. Does this opportunity contain local preference? If yes, please provide the details.

   We have no local preference. An OSA evaluation team will judge the merits of proposals received in accordance with the general criteria outlined in the RFP. The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered.

5. What is the budget of this opportunity? Is Budget approved?

   As noted in the RFP, bidders will propose total cost and a schedule for the work to be performed and to meet the project deliverables.

6. How many sample job description and/or resume, we have to provide?

   As noted in the RFP, the proposal must include a resume of all principal staff highlighting their professional qualifications and similar evaluation work that they have performed.

7. Can you allow the offer or use the past performances of teaming partners as valid past performance references?

   The intent is for proposals to include references from other clients for similar work performed, not from "teaming partners" with whom bidders collaborated or worked together to perform similar work or project deliverables.

8. Can you please provide current number of users and infrastructure details? (VMWare, MAN, # of Servers, # of Workstations)

   This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

9. Are any cloud providers used? Do you manage your own datacenter, or do you utilize any 3rd-party/colocation facilities?

   This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

10. Approximately how many live hosts, # of internal and external IPs are in scope for the Network Vulnerability Assessment?

    This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

11. Are any vendor products installed for Governance, Risk, and Compliance (GRC) tracking?

    This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

12. How often are information security policies updated? When it was updated last time?

    As noted on the OIT website (http://www.oit.state.co.us/about/policies), "Colorado Information Security Policies were updated in their entirety in February 2017 and supersede any policies posted prior to this date. Additional information related to the frequency of updates should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

13. What is the number of wireless controllers supporting the organization wireless networks?

    This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

14. Are IoT devices included as "assets" on the network?

As noted in the RFP, the engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during the planning phase of the evaluation, in partnership with the OSA, to align with the overall project timelines outlined in the RFP. This detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as the detailed approach and methodology used. As such, if IoT device are found to be present in the CDOT environment, they can be included in the scope of this evaluation, if deemed necessary, through the selected contractor's planning and risk assessment procedures, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

15. Are any vendor products installed for Security Incident & Event Management (SIEM)? If yes, please provide currently used SIEM product name.

    This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

16. Below is a request we are to provide.

    > "Provide a copy of the results of the organization's most recent external peer review if the organization will conduct an audit under generally accepted government auditing standards."

    However, we cannot provide a copy of results of an audit as such information is confidential. Can you please consider waiving this request – understanding confidentiality matters are important? Or maybe the request can be altered somewhat?

    For this evaluation engagement, there is no requirement to follow generally accepted government auditing standards (GAGAS). However, if bidders indicate in their proposals that they will conduct the engagement under GAGAS, a copy of the results of the organization's most recent external peer review must be included in their proposals.

17. General

    - Will a single report combining both the risk assessment and the penetration testing be required or can they be separate reports?

      A single public evaluation report containing findings, conclusions, and recommendations resulting from the work performed is required. However, as noted in the RFP, two reports may be necessary to report the findings, conclusions, and recommendations associated with this evaluation. As necessary, one report will be made public after being released by the Legislative Audit Committee (LAC), and another report will remain confidential and will not be released publicly by the LAC in order to protect any sensitive information that may need to be reported in it. The selected contractor will prepare the final evaluation report(s) in the format delineated in Exhibit H of our contract, which is attached to the RFP in template form. As such, all references to the evaluation "report" in the RFP, contractor proposals, the executed contract, etc. should include the possibility of two reports. In this sense, separate risk assessment and penetration testing reports would not necessarily need to be included in the public report, but may need to be *provided through a second confidential report, as necessary, depending on the information being reported.*

18. Security Program Risk Assessment

- Is an ISO 27001/2 risk assessment acceptable for a review of the security organization structure?

  The security policy structure aligns with the NIST SP 800-53 framework. However, other leading practices, such as ISO 27001/2, may be considered and applied if deemed necessary through the selected contractor's planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

- Does the DOT all follow a single standard of policies and procedures?

  As noted in the RFP, Colorado statute [Section 24-37.5-403, C.R.S.] requires the CISO to develop and update information security policies, standards, and guidelines to be followed by Executive Branch agencies, including CDOT, as well as any vendors or the service providers they use. OIT has published these policies and standards on its website: http://www.oit.state.co.us/about/policies.

- Is the entire department of Transportation considered a unified IT and security organization (one division)?

  The Colorado Department of Transportation (CDOT) is the State's transportation department responsible for operating and maintaining Colorado's state highway system, including more than 3,000 bridges, and maintaining the aviation system plan, under the policy direction of the eleven-member Transportation Commission. CDOT is also responsible for highway construction projects, implementing the State's Highway Safety Plan, repairing and maintaining roads, providing technical support to local airports regarding aviation safety, and administrating the reimbursement of aviation fuel tax revenues and discretionary grants to local airports. It does not have it's own IT and security organization or division within the Department. Rather, with the passage of Senate Bill 08-155 during the 2008 Legislative Session, the Governor's Office of Information Technology (OIT) was created to oversee, manage and operate the delivery of IT services across 16 executive branch agencies, including CDOT. For these consolidated state agencies, as they have been termed, OIT also maintains an Information Security Program to control risks associated with access, use, storage, and sharing of sensitive citizen and state information to achieve the requirements of the Colorado Information Security Act, as noted in C.R.S. 24-37.5-401 et seq. Again, all statewide information security policies for consolidated state agencies apply to every public agency as defined in C.R.S. 24-37.5-402(9) and also apply to any entity (i.e., vendors) providing information technology as defined in C.R.S 24-37.5-102(2) or any IT related products, goods, equipment, hardware, supplies, software, services, or any other IT related resource to any state agency.

- How many people are in the security department and how many people will need to be interviewed?

  This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

- How many people in IT and how many need interviewed?

  This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences. However, for the Fiscal Year 2018-2019 budget year, OIT was appropriated about 952 full-time equivalents.

- How many other people in DOT need to be Interviewed?

  This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

19. Penetration Testing Portion

- For the penetration testing component, we understand it is a risk based approach however is it possible to provide the following data:
  - Number of IP addresses (active) and are externally facing (on the internet)
  - Number of servers in the organization and is 10% a good sample size for testing
  - Number of workstations in the organization and is 10% a good sample size for testing
  - Number of other devices on the network (routers, switches) is 10% a good sample size for testing
  - How many web applications should be included in the sample size (e.g, 2 web applications)
  - How many web APIs should be considered in scope?
  - Is WIFI in scope and how many locations should be assessed?
  - Should a red team engagement be included in addition to Pen Testing?
  - Should a social engineering engagement (phishing, vishing, etc.) be included in the scoping?

  The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective, including any red team or social engineering procedures deemed necessary. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences. An appropriate sampling methodology will also need to be designed and applied by the selected contractor to achieve the evaluation objectives.

20. We understand there is approximately 9 weeks for the testing window(s) (July-September) (7/29-10/7) to perform all field-work. Should the Risk assessment, pen testing and all other work be grouped into this 9 week period and can they overlap.

    Yes, all evaluation work procedures that may be necessary to meet the evaluation objectives should be performed during the fieldwork phase of the project as noted. Various types of work procedures or testing can overlap during this time period, as necessary.

21. In our experience with similar requirements, we have found that it could take anywhere from $300-$500K depending on the scope of assessment. Does OSA have the required funding and can OSA share the budget for this assessment?

    The contract will be awarded to the bidder whose proposal will be most advantageous to the State of Colorado, price and other factors considered, as noted in the RFP. Thus, the OSA will consider all proposals submitted, along with their total cost information. The OSA plans to have the funding to support the awarded bidder. Budget information is not available to share for this assessment.

22. Would the selected vendor be excluded from performing any future remediation work for CDOT?

    No.

23. Can OSA confirm that the scope of the assessment should include the following?

    a. Security policies and procedures review
    b. Review of CDOT's security capabilities against CDOT and OIT policies and standards
    c. Network vulnerability scanning. Please provide number of IPs in-scope (internal and external public facing).
    d. Application vulnerability scanning (e.g. secure code, database scanning). Please provide number of external public facing and internal applications that will be in-scope.

    The scope of the evaluation may include these items, depending on the project scope and methodology that will be developed by the selected contractor during its planning and risk assessment. The selected vendor should reasonably expect to use the centralized information security policies and other relevant criteria that may be applicable to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. However, this would not necessarily mean reviewing the adequacy of the policies and other applicable criteria identified. The other specific information noted above, such as the number of IPs and applications, should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

24. Given that OSA's responses to the vendor questions may require changes to our responses to meet your requirements, would OSA consider extending the submission deadline by 3-4 weeks?

    No extension of this date can be granted.

25. According to the RFP page 10: “any testing or assessment of security practices and procedures concerning information technology…shall be conducted…in accordance with industry standards prescribed by the national institute of standards and technology or any successor agency”. Are there specific NIST Standards the department requires the vendor to align with? Are there other federal or state regulations or security standards that should be considered as part of the evaluation?

    The RFP language noted should be interpreted to mean that any testing or assessment procedures planned and conducted by the selected contractor need to be in accordance with applicable NIST standards (or any successors). For example, for this engagement, if the selected contractor plans to perform technical information security tests and examinations, such as vulnerability assessment and penetration testing procedures, it is required to align its procedures with applicable NIST standards, such as SP800-115, or any others that may apply. Also, as we understand, the Governor’s Office of Information Technology has adopted NIST 800.53 Rev.4 as a security framework for Executive Branch agencies/departments under its oversight. Thus, the selected contractor should confirm this once the engagement begins and determine whether there may be any other criteria that may need to be considered and applied during the engagement.

26. It is understood that the scope will be clearly identified as the initial part of the evaluation, however in the interest of estimating effort, what is the approximate scope of the evaluation in terms of number of systems and physical locations?

    The number of systems should be determined by the selected contractor, as necessary, once the engagement commences. CDOT’s physical headquarters is at 2829 W Howard Pl, Denver, CO 80204, and OIT’s physical headquarters is at 601 E 18th Ave Ste 130, Denver, CO 80203. State agencies typically utilize primary and backup data centers, but the selected contractor should determine this information when the engagement commences, as necessary.

27. Please let us know exactly what you are requesting in with the following question from page 14 of the RFP: "Provide a copy of the results of the organization’s most recent external peer review if the organization will conduct an audit under generally accepted government auditing standards.” If we are not an audit firm, does this pertain? If it does apply to firms that are not auditing firms, please let me know what you need to fulfill this requirement.

    For this evaluation engagement, there is no requirement to follow generally accepted government auditing standards (GAGAS). However, if bidders indicate in their proposals that they will conduct the engagement under GAGAS, a copy of the results of the organization’s most recent external peer review must be included in their proposals, which outlines that an independent assessment has been performed on the bidder’s structure of internal controls and quality control.

28. Are only the essential systems that have been defined by OIT in scope? Can OSA provide an estimate number of systems and applications that would be in scope?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed *scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.*

29. Can OSA provide an estimate number of physical locations the selected vendor would be to visit? Would visits to each of the five transportation Regions be required?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used, including any site visits that may be necessary to achieve the evaluation objective. CDOT's physical headquarters is at 2829 W Howard Pl, Denver, CO 80204, and OIT's physical headquarters is at 601 E 18th Ave Ste 130, Denver, CO 80203. Also, state agencies typically utilize primary and backup data centers, but the selected contractor should confirm this and any physical location information that may be needed when the engagement commences.

30. Is NIST 800-53 the required framework and set of controls for the assessment? If yes, are all controls in scope? Moderate and / or high?

    As we understand, the Governor's Office of Information Technology has adopted NIST 800.53 Rev.4 as a security controls framework for Executive Branch agencies/departments under its oversight. Thus, the selected contractor should confirm this, once the engagement begins, as necessary, and determine during its planning and risk assessment whether there may be other criteria that may need to be considered and applied during the engagement to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

31. Are all departments under CDOT in scope for the assessment?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, technologies and departments under CDOT that will be evaluated, as well as any detailed approach or methodology used that may be necessary to achieve the evaluation objective.

32. Are there any remaining actions or objectives from the cyber event that occurred in February of 2018 that need to be clearly identified in this engagement?

    The information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences during its planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The rules of engagement should include any of this related information, as necessary.

33. Is it possible for us to be provided the number of resources from OIT that support CDOT in any capacity including an idea of roles/responsibilities that are provided to CDOT, in addition to what is provided on the RFP, for purposes of scoping number of interviews and time needed for the planning requirements of the RFP?

    The information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences during its planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

34. Are there any additional policies, standards, specification or guidelines that will be considered in scope of the performance evaluation that are not listed on the websites of OIT or OIS? (anything in addition to the 18 policies CISPs listed at http://oit.state.co.us/ois/policies)

    The selected vendor should reasonably expect to use the centralized information security policies, standards, specifications and guidelines that are listed on the OIT/OIS website as criteria in conducting this evaluation. However, the selected contractor would also be expected to assess and apply any other applicable criteria needed to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP, including any not listed on the OIT/OIS website, such as related laws and regulations, leading best practices, informal management expectations, etc.

35. Can the list of Critical and Essential applications that is managed by OIT and referenced in the RFP be provided to assist with budgeting efforts for vulnerability scanning, penetration testing and control testing?

    The information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences during its planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

36. Can an inventory of CDOT systems including applications, servers, endpoints and network devices be provided to assist with the budgeting efforts for vulnerability scanning, penetration testing and control testing? (even summary quantities of users, servers, locations, network devices and applications is helpful)

    The information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences during its planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

37. Can a summary of any in house application development technologies/solutions be provided for the purposes of scoping application vulnerabilities/code testing?

    The information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences during its planning and risk assessment procedures to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP.

38. Please specify the total number of external public IP address as well as the number of live devices in scope for Vulnerability Assessment and Penetration Testing (VAPT). A live device indicates a device that is accessible on the internet and has a certain service running on it.

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

39. Please specify the number of internal IP addresses and subnets in scope for internal network VAPT.

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

40. Approximately how many physical locations are in scope for onsite visits to conduct VAPT?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective.

41. What type of Social engineering tests is the department expecting to be kept in scope:

    a. Phishing assessment – How many email IDs will be targeted?
    b. Physical Impersonation or piggy backing - How many number of locations will be in scope?
    c. Phone calls or pretext

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

42. Is wireless security in scope? If yes, please specify the number of locations to be covered.

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective.

43. How many web applications will be included as a part of VAPT?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective.

44. Will the department provided credentials for conducting authenticated web application penetration testing?

    Yes, OIT and/or CDOT would need to provide such credentials if authenticated web application penetration testing is deemed to be in scope by the engaged contractor during its planning and risk assessment procedures.

45. Please specify the number of static and dynamic pages for each application in scope for VAPT.

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

46. Page 7, top of page, 3rd line. "Exhibit G…" Will you expect a Management Response section to the report with time needed for management to develop a response to the finding/recommendation?

    Yes, the selected contractor is required to obtain management responses to the findings/recommendations, as noted on page 8 of the RFP.

47. Page 7, last table entry. Is it sufficient to have the Project Manager on-site for these meetings with the remaining team members on a web-ex?

This sounds reasonable and could be an option to fulfill this requirement, but it should be assessed further with the OSA during the engagement to determine the best option at that time.

48. The proposal requires a total number of hours (and price) for the evaluation; however, there is no information on the information technology infrastructure in existence on which to base that sizing. What is the size of the in-scope infrastructure?

    a. Number of servers?
    b. Number of firewalls?
    c. Number of policies?
    d. Number of departments?
    e. Number of databases?
    f. How many different operating systems are in-scope?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

49. Does the in-scope environment have any of the following within scope?

    a. Personal Health Information (PHI)
    b. Personally Identifiable Information (PII)
    c. Payment Card Information (PCI)
    d. Any other regulated data

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. This information should be requested and obtained by the selected contractor, if necessary, once the engagement commences.

50. Section D, #8, request a copy of the results of the organization's most recent external peer review if the organization will conduct an audit under generally accepted government auditing standards. Could OSA provide clarification in regards to what is desired by "external peer review," is the request for a third party audit?

    For this evaluation engagement, there is no requirement to follow generally accepted government auditing standards (GAGAS). However, if bidders indicate in their proposals that they will conduct the engagement under GAGAS, a copy of the results of the organization's most recent external peer review must be included in their proposals, which outlines that an independent assessment has been performed on the bidder's structure of internal controls and quality control.

51. For further clarification to Section D, #8, is the request to provide the “most recent peer review” only if we plan to state that the Security Evaluation we plan to perform would follow generally accepted government auditing standards?

    See answer to questions 50 above.

52. Section C and Section provides information about the General criteria for evaluation and total score. Will OSA provide additional details on how the scores will be distributed across the General Criteria listed? (e.g., how many points will be given for the Experience and Stability of the organization.)

    No, we do not share our scoring details with bidders or anyone external to our selection team. Further, as page 11 of the RFP states, “The State Auditor reserves the right to make an award without further discussion of proposals received.

53. Has a security control framework been adopted? If yes, which one?

    As we understand, the Governor’s Office of Information Technology has adopted NIST 800.53 Rev.4 as a security framework for Executive Branch agencies/departments under its oversight. Thus, the selected contractor should confirm this once the engagement begins and determine whether there may be any other criteria that may need to be considered and applied during the engagement.

54. Are there documented policies, procedures, standards, and guidelines in place? If so, how many?

    As noted in the RFP, Colorado statute [Section 24-37.5-403, C.R.S.] requires the CISO to develop and update information security policies, standards, and guidelines to be followed by Executive Branch agencies, including CDOT, as well as any vendors or the service providers they use. OIT has published these policies and standards on its website: http://www.oit.state.co.us/about/policies. Additional policies, procedures, standards, and guidelines in place should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

55. We respond to a large number of bid requests and appreciate our clients’ generosity in providing references for our firm. However, we do not want to overwhelm our customers with reference requests. Will COSA accept letters of recommendation in place of references with contact information? Alternatively, can we redact the contact information for our references in our proposal? If named a finalist for this RFP, we will provide full contact information upon COSA’s request.

    The proposal must provide three references for similar work performed.

56. How many information systems are in scope for the IT assessment?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will *be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective.*

57. The RFP states that penetration testing of departmental network sis in scope. Does that encompass external and internal network vulnerability assessments and penetration testing?

    a. If so, what is the approximate number of external and internal active IPs?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

58. Is a detailed firewall configuration analysis in scope?

    a. If so, what is the number of firewalls?
    b. Are the firewalls in HA mode?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

59. Is a router | switch configuration analysis in scope?

    a. If so, what is the approximate number of devices?
    b. What types of devices?

    The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

60. Is web application testing in scope?

    a. If so, what is the number of URLs to be tested?

b. How many applications?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

61. Is a network architecture review in scope?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective.

62. Is enterprise application testing in scope?

a. If so, how many applications?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

63. Is database testing in scope?

a. If so, what is the brand of the database servers?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

64. Is a server review in scope?

a. If so, what types and versions of servers are in scope?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

65. Is there a wireless network assessment in scope?

    a. If so, how any locations?
    b. How many controllers are in scope?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

66. For the social engineering in scope:

    a. What is the number of targets?
    b. What is the medium for testing? (e.g. phishing, phone pretexting, baiting, tailgating)

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.

67. Is a physical security assessment in scope?

    a. If so, how many locations?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation *objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences.*

68. Is a VPN configuration review in scope?

    a. If so, how many appliances?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences

69. Is a workstation configuration review in scope?

    a. If so, how many should be tested?

The engaged contractor will be responsible for developing a detailed, risk-based project scope and methodology during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objective, project deliverables, and timelines outlined in the RFP. The detailed scope will outline the specific information systems, applications, networks, and technologies that will be evaluated, as well as any detailed approach or methodology used to achieve the evaluation objective. As such, the information noted above should be requested and obtained by the selected contractor, as necessary, once the engagement commences. An appropriate sampling methodology will also need to be designed and applied by the selected contractor to achieve the evaluation objectives.