May 7, 2020

A Request for Proposal for an Evaluation of Web Application Security at the Colorado Statewide Internet Portal Authority

Responses to Potential Bidder Inquiries Submitted by Firm

Questions from Firm #1:

1) How many overall websites/web applications developed, operated, and maintained by SIPA are there?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. However, as noted in the RFP, the following link contains a list of all websites on the Colorado.gov platform:

- [https://www.colorado.gov/goingpacific/view-all-pacific-sites](https://www.colorado.gov/goingpacific/view-all-pacific-sites)

Additional information obtained from SIPA’s website ([https://www.colorado.gov/pacific/goingpacific/pacific-platform](https://www.colorado.gov/pacific/goingpacific/pacific-platform)) indicates, “The Pacific platform is a custom implementation of Drupal 7 made specifically with government entities in mind by Colorado Interactive. The platform launched in 2013 and hosts websites for over 125 agencies, departments, municipalities, and special districts.

2) Does documentation exist listing where each of these applications are hosted (i.e. network, segments, physical locations of servers), and the processes and controls that are currently in place to protect these websites/web applications?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

3) Of the total number of websites/web applications developed, operated, and maintained by SIPA, does OSA have an estimated number of websites/web applications that may be deemed mission critical?
**OSA Response:** The OSA does not have this information. It should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

4) Mission critical is defined as something that is essential to the operation of an organization. If a web application is deemed to not be essential to operation (e.g., a website that simply provides information to visitors), this web application, if compromised and in the right network location, could affect the security of a mission-critical web application, thus makes it imperative to fully evaluate ALL web applications. Is this OSA’s expectation also?

**OSA Response:** This could be a reasonable expectation, if it is determined to be appropriate through the Contractor’s planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

5) Are the web applications in-house developed, commercial off the shelf, or a combination of both? If a combination, what is the estimate (e.g., 50/50)?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

6) Is it expected that the successful bidder will perform full source code analysis/code review of applications deemed to be in scope as mission critical?

**OSA Response:** This is not expected, but it could be included if it is determined to be appropriate through the Contractor’s planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

7) The resources needed to perform a penetration test on a web application vary greatly. Factors include but are not limited to: if there is authentication, the number of authentication levels/permission matrixes, the number of dynamic pages, the number of static pages, the number of inputs, and complexity for the application’s intended flow.

   a. Will authentication be required to test some/all applications?

      **OSA Response:** Authenticated testing may be included, but 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 objectives, project deliverables, and timelines outlined in the RFP.

   b. If so, how many roles/authentication levels will be needed to test, on average, per application?
OSA Response: 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 objectives, project deliverables, and timelines outlined in the RFP.

c. How many dynamic pages are included, on average, per application?

OSA Response: This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

d. How many static pages are included, on average, per application?

OSA Response: This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

e. How many inputs are there to be tested per application?

OSA Response: This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

Questions from Firm #2:

8) We identified the following URLs linked within the Pacific Platform sites. Are the following URLs and their subpages also in-scope?

<table>
<thead>
<tr>
<th>Domain/URL</th>
<th>In Scope?</th>
</tr>
</thead>
<tbody>
<tr>
<td>coloradoaps.force.com</td>
<td></td>
</tr>
<tr>
<td>healthfirstcolorado.com</td>
<td></td>
</tr>
<tr>
<td>ops.colorado.gov</td>
<td></td>
</tr>
<tr>
<td>cpw.state.co.us</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.colorado.gov/revenueonline/">https://www.colorado.gov/revenueonline/</a></td>
<td></td>
</tr>
<tr>
<td>mydmv.colorado.gov</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.coloradolottery.com">www.coloradolottery.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.colorado.gov/tax">www.colorado.gov/tax</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.doc.state.co.us/oss/">http://www.doc.state.co.us/oss/</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://www.colorado.gov/dcj">https://www.colorado.gov/dcj</a></td>
<td></td>
</tr>
<tr>
<td>coloradostatefair.com</td>
<td></td>
</tr>
<tr>
<td>mycoloradojourney.com</td>
<td></td>
</tr>
</tbody>
</table>
**OSA Response:** The scope will only include current, operational Colorado state websites, web applications, and web services, whether internal or external facing, and will not include SIPA developed, operated and/or maintained websites and web applications/services that are not Colorado state government websites and/or web applications/services, such as city, county or special district websites and/or web applications/services. As such, to the extent that these URLs and subpages meet this criteria, these sites may be may included in the scope of this evaluation if deemed necessary to achieving the evaluation objectives, based on the results of the engaged Contractor’s planning and risk assessment procedures, in partnership with the OSA.

9) **Will this test take place in the Live environment (in Production) or a pre-production/staging environment?**

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP.

10) **We will deliver the final report as specified in the RFP. However, some results of the test may be available before the report delivery date. In this case, is it acceptable or desirable to deliver components of the report when they are complete in addition to the full, final report on schedule?**

**OSA Response:** Although this may be feasible, it is typically not acceptable or desirable, due to the OSA’s rigorous findings and report development and review process, which includes reviews, comments, and/or revisions by the OSA and SIPA, at multiple levels. Due to this, the process will adhere to the sequential schedule, with timed milestones and deliverables, as outlined in the RFP, unless exceptions are agreed to by the OSA.

11) **Clarification on “The engaged contractor will perform the engagement through a risk-based approach by selecting for review key, mission-critical state websites that enable agencies and citizens to conduct business electronically and to transmit and/or maintain sensitive information.” Is the expectation that some URLs will be completely untested, or is the expectation that some URLs will simply be less tested than other, critical websites?**

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP.

12) **Clarification on “Perform a review of key IT and/or information security processes and controls related to secure web application development, operations and maintenance, to determine whether such processes and controls have been designed, put in place, and operate effectively to minimize web application security risks.” Is it expected that this will be performed separately**
from vulnerability assessment of web applications and services? For example, we may interview developers, assess the software development and deployment process.

**OSA Response:** The related process and controls assessment can be considered a separate project task with associated procedures that will need to be developed and executed by the engaged Contractor. However, the procedures used to perform this assessment, such as the ones listed in the question, could potentially occur before, during, or after the related VA and pen testing procedures, based on the detailed, risk-based project scope and methodology the Contractor develops during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

Questions from **Firm #3**:

13) What is the approximate size of the State’s Internet-facing environment that will be in scope for this assessment (number of IPs)?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

14) Does the State maintain a test environment for web applications prior to deploying them into production? If so, is the test environment in scope?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, project deliverables, and timelines outlined in the RFP.

15) Does the State currently perform static and dynamic application testing for the web sites and applications? Will this be in scope for the assessment?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, project deliverables, and timelines outlined in the RFP.
16) Is there a known number of web applications that will be tested for this engagement? Understanding there are a number of websites and applications from the State of Colorado, are all web applications expected to be tested or a relative sample?

**OSA Response:** This information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, 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 objectives. An appropriate sampling methodology can be designed and applied by the selected Contractor to achieve the evaluation objectives. It is not expected that all state web applications will be tested, although this may be a possible approach, if the Contractor deems it necessary and feasible, in partnership with the OSA, through its planning and risk assessment procedures. It is likely that an appropriate, risk-based sample will be tested, in order to achieve the evaluation objectives, within the timelines outlined in the RFP.

17) BKD would look to perform a penetration test on the IT infrastructure that supports the web applications. Approximately how large is that environment (number of physical servers, virtual servers, routers/switches, and firewalls)?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

18) Most of this work, if not all, could be performed remotely. Is there any expectation of onsite time for meetings or other activities?

**OSA Response:** Although certain work procedures for this evaluation could likely be performed remotely, other work may need to be performed on-site. As such, the engaged Contractor should determine the most effective approach necessary to perform the procedures needed to achieve the evaluation objectives, project deliverables, and timelines outlined in the RFP.

Questions from Firm #4:

19) Are there any State Agency websites not listed in the link provided with the RFP that would be within the scope of this assessment?

**OSA Response:** Although most of the state agency websites within the scope of this evaluation should be listed at the link location provided within the RFP, there could potentially be some websites that are not listed there and that could be deemed to be in-scope, based on the risk. For
example, if there have been mission-critical websites developed since that listing was published, but the listing has not been an updated, these websites/web apps should also be considered. As such, this information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

20) Are any of the State Offices listed in the link provided with the RFP within the scope of this assessment?

**OSA Response:** As noted in the RFP, the scope of the evaluation will primarily review SIPA’s IT and information security related processes and controls that support the development, operations, and maintenance of the in-scope websites, web applications, and web services, but it may also include a review of any related agency-owned business processes and controls. Additionally, applicable SIPA contract management practices as well as procedures to evaluate IT or information security practices of SIPA’s third party vendors, contractors, and/or service providers, such as those related to Colorado Interactive (CI), may also be included in the scope of this evaluation if deemed necessary to the achievement of the objectives of evaluation, and based on the results of the engaged contractor’s planning and risk assessment procedures. 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 objectives, project deliverables, and timelines outlined in the RFP.

21) Are there any internally-facing websites (meaning within the State’s intranet) that OSA would expect to be included with the scope of this assessment?

**OSA Response:** Internally-facing websites could be included in the scope of this assessment if the Contractor deems it necessary and feasible, in partnership with the OSA, through its planning and risk assessment procedures to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. It is likely that an appropriate, risk-based sample of both internally-facing and externally-facing websites will be tested, in order to achieve the evaluation objectives, within the timelines outlined in the RFP.

22) Are there any state websites, web application, or web services other than those described in the RFP (i.e., Colorado.gov web portal and payment processing services) that OSA would expect to be included within the scope of this assessment?

**OSA Response:** There may be other state websites, web application, or web services other than those described in the RFP (i.e., Colorado.gov web portal and payment processing services) that could be considered and deemed to be in-scope as the Contractor performs its planning and risk assessment procedures to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.
23) The RFP mentions that Drupal is utilized to facilitate delivery of the Colorado.gov platform. Is the OSA aware of any additional application development platforms (e.g., ASP.net, PHP, Java, Ruby on Rails, etc.) utilized in the delivery of in-scope applications through SIPA?

**OSA Response:** The OSA is not aware of this information. It should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

24) Can the OSA speak to any specific testing time restrictions (e.g., anytime, non-business hours, business hours, etc.)?

**OSA Response:** The OSA cannot speak to any specifics related to this at this time. This type of information would likely be included in the rules of engagement that must be developed and put in place between the Contractor and SIPA prior to beginning fieldwork in order to agree in writing to any rules governing the manner in which the testing or assessment is to be conducted, including a mitigation plan for handling significant system outages or disruptions in the event they occur. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

25) Does the OSA have any expectations or requirements regarding the contractor performing authenticated and/or unauthenticated testing?

**OSA Response:** Although the OSA has no set requirement to perform authenticated and/or unauthenticated testing, it expects that each type of testing would likely be included in the scope of this evaluation to some extent, based on risk, to achieve the evaluation objectives and project deliverables, within the timelines outlined in the RFP. As such, the engaged Contractor will be responsible for developing a detailed, risk-based project scope and methodology, including any authenticated and/or unauthenticated testing, during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objectives and project deliverables, within timelines outlined in the RFP.

26) Is the OSA aware of any time constraints (e.g., planned software upgrades or migrations) on the part of SIPA or its partners that would need to be considered in the scheduling of testing activities?

**OSA Response:** The OSA cannot speak to any specifics related to this at this time. This information should be assessed and determined by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP, and included in the rules of engagement between the Contractor and SIPA, if necessary.
27) Does SIPA have any oversight or responsibility for the configuration of or content posted to the websites or applications it helps setup and support OR do these fall under the responsibility of the respective agencies?

**OSA Response:** Other than SIPA’s website itself, the content management is assumed to be the responsibility of the respective agencies. However, this information should be requested and assessed/verified by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

28) To the best of the OSA’s knowledge, does the Governor’s Office of Information Technology have any oversight authority or do they in any way support SIPA in its delivery of the in-scope web application services to the State?

**OSA Response:** According to Section 24-37.5-105(3)(i), C.R.S., states that the Governor’s Office of Information Technology (OIT) is to initiate or approve all procurements of information technology resources, enterprise facilities, and any goods or services related to such procurements for state agencies and enter into any agreement, contract, or enterprise agreement in connection with such procurements on behalf of a state agency or agencies. Further, Section 24.37.5-105(3)(n), C.R.S., states that OIT will develop a policy for the office’s use of external vendors, including SIPA, in delivering electronic information, products, and services. OIT’s chief information officer or the chief information officer's designee, sits on the SIPA board as one of 15 voting members (Section 24.37.7-102(2)(h), C.R.S).

29) Can the OSA provide any insight or direct us to any resources that can provide insight into the State’s oversight and management of SIPA and its third-party vendors, contractors and services providers?

**OSA Response:** There are some references noted in the RFP in Section IV, Supplemental Information, including a link to SIPA’s website: [https://sipa.colorado.gov/](https://sipa.colorado.gov/) Additionally, the Colorado statutes related to SIPA, C.R.S. § 24-37.7-101, may also help to provide insight or may be a good resource on this.

30) Does the OSA have any recommended or preferred criteria related to the forth bullet under OBJECTIVES, SCOPE, AND METHODOLOGY on page 6 of the RFP, which relates to performance of, “…a review of key IT and/or information security processes and controls related to secure web application development, operations and maintenance, to determine whether such processes and controls have been designed, put in place, and operate effectively to minimize web application security risks.

**OSA Response:** OSA staff have some experience with web app security reviews of this nature and can share prior audit programs or related information that may help to provide some ideas on what processes and control areas are most significant to web app security that could then be used by the Contractor to further assess any relevant criteria in use or intended for use by SIPA in its
operations. However, ultimately, the engaged Contractor will be responsible for developing a detailed, risk-based project scope and methodology, including a determination of applicable criteria related to the fourth bullet under the Objectives, Scope and Methodology on page 6 of the RFP, during its planning and risk assessment procedures, in partnership with the OSA, to satisfy the evaluation objectives and project deliverables, within timelines outlined in the RFP.

Questions from Firm #5:

31) How many current, operational Colorado state websites, web applications, and web services are developed, operated, and maintained by the SIPA today? (page 5)

**OSA Response:** See response to question #1 above and other related responses.

32) What percentage of this number does the OSA consider “key, mission-critical state websites that enable agencies and citizens to conduct business electronically and to transmit and/or maintain sensitive information.” (page 5)

**OSA Response:** See response to question #16 above and other related responses.

33) “In addition to any web application security frameworks and standards used by SIPA” What security frameworks and standards are in use by the SIPA today? (page 6)

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

34) How many additional agencies’ “related agency-owned business processes and controls” will need to be reviewed? (page 6)

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. Also, see response to question #20 above and other related responses.

35) How many “third party vendors, contractors, and/or service providers” are engaged by SIPA, and how many of these are in-scope? (Pages 6-7)

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, project deliverables, and timelines outlined in the RFP.
36) Under what, if any, circumstances would the use of a specialized subcontractor be considered a joint venture?

**OSA Response:** As noted in Section K of the RFP, “No joint venture proposals will be accepted. However, this requirement does not preclude the use of outside special consultants if deemed necessary by the Contractor.”

37) How many physical locations including business offices and data centers will be in scope for the assessment?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, project deliverables, and timelines outlined in the RFP.

38) Given the scope of the assessment is indeterminate – the first step of the project being to establish a scope – what provisions and facilities exist for modifying the agreement if the finally determined scope of work exceeds the bid amount?

**OSA Response:** As noted in Section G of the RFP, “The State Auditor...reserves the right to engage in further negotiation of the project scope, price, and contract terms after selection of the Contractor if, in the opinion of the State Auditor, it is in the best interest of the State to do so.” Additionally, as noted in the RFP, the OSA expects the successful bidder to execute and adhere to the terms and conditions in the OSA’s standard contract and its related exhibits, which are included in Section IV – Supplemental Information. The OSA’s standard contract contains provisions related to modifying the agreement, which may include a properly executed and approved written amendment to the Contract.

Questions from Firm #6:

39) How many unique domains and IP addresses are within the scope?

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

40) Will the Web Application Security Testing be performed authenticated or unauthenticated? If authenticated how many different user roles will be tested?
OSA Response: See responses to questions 7a, 7b, and 25 above.

41) Will the testing include API endpoints? How many API parameters? How many endpoints?

OSA Response: 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

42) In using a risk-based approach to selecting for review key, mission critical, state websites, how many websites at a minimum does OSA expect to be tested?

OSA Response: See response to question #32 above and other related responses.

43) Is all website development performed at a centralized location? If not, how many different sites will need to be visited in order to conduct staff interviews?

OSA Response: This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, project deliverables, and timelines outlined in the RFP.

44) Are any of the websites developed by external, third-parties? If yes, which websites?

OSA Response: Preliminary information gathered indicates that SIPA uses at least one external third party, Colorado Interactive (CI), in the development of websites. However, the nature, timing and extent of CI’s involvement with this, as well as whether other third parties are used, is unknown at this time. This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures, when developing a detailed, risk-based project scope and methodology, in partnership with the OSA, to satisfy the evaluation objectives and project deliverables, within the timelines outlined in the RFP.

45) How many staff interviews are expected to be conducted for reviewing secure SDLC processes?

OSA Response: 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as
necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

46) Is there an incumbent provider for this work currently?

**OSA Response:** There is not an incumbent provider for this work currently.

47) If this work was performed with a prior vendor, what was the contract amount?

**OSA Response:** N/A, see response to question #46.

Questions from Firm #7:

48) How many web applications, web sites, and web services and/or services will be in-scope?

**OSA Response:** See response to questions 42, 39, and other related responses.

49) How many are external-facing?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

50) What is the size of the applications? Number of web pages?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

51) How many employees and others do you estimate will need to be interviewed?

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

52) How many business processes and controls are in-scope?
**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

53) How many contract management practices and procedures to evaluate 3rd party vendors, contractors, and service providers are in-scope?

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

54) How many policies are available?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

55) Are all policies documented?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

56) For the penetration test, how many of the following are in-scope?
   a. Routers

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.
b. Servers

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

c. Workstations, laptops

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

d. Mobile devices

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

57) How many users of these services or applications?

**OSA Response:** 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 objectives, project deliverables, and timelines outlined in the RFP. As such, this information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

58) There are a number of on-site meetings stipulated in the RFP. In light of current circumstances, are these going to be required?
**OSA Response:** If any particular meeting is denoted in the RFP as being an on-site or in-person meeting, this would be the OSA’s expectation. However, given the current circumstances, related to the COVID-19 pandemic, which is what we assume is meant by “In light of current circumstances...,” if these conditions are present and/or persist during the time the work related to this evaluation is conducted, alternative meeting delivery/participation methods, such as video conferencing meetings, could potentially be used as possible alternatives. In such instances, and to help ensure the safety of everyone involved, the selected Contractor should work with the OSA’s contract monitor to determine and get approval for any potential meeting format on a case-by-case basis.

59) Is the template in Exhibit G what must be utilized for findings or may our existing template be used for detailed findings? Can this template suffice for the summary elements of the engagement (we typically provide more detail)?

**OSA Response:** As noted in the RFP, the findings must adhere to the OSA’s standards as described in “Exhibit G – Developing and Presenting Findings” of the OSA’s standard contract, which is included in Section IV – Supplemental Information. Additionally, the final report, including any associated confidential report, must adhere to the OSA’s standards as described in “Exhibit H – Reporting Requirements and Format for Separately Issued Reports” of the OSA’s standard contract, which is included in Section IV – Supplemental Information. In other words, yes, the template in Exhibit G must be utilized for those findings that will be included in the reports noted in the RFP (i.e., the public and confidential reports that will be developed for the purposes of reporting the results of this evaluation to the LAC and possibly other oversite bodies or legislative committees). That said, for similar evaluations that we have performed in the past, there have often been additional management level reports that we/our Contractors have developed in order to provide more detail, typically as they may relate to technical issues or problems found during select evaluation work. For example, such reports have often been used to accompany our public and confidential reports in order to communicate to management separately the various technical details associated with specific vulnerabilities or exploitations that may be found to exist or be exploited during the course of the evaluation. As such, this type of report would be highly desirable, if the nature and results of any of the evaluation work may dictate or necessitate. Thus, in such instances, after review and approval by the OSA, the selected Contractor could make use of its existing template(s) for this type of findings development and reporting.

60) What is the 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. Thus, the OSA will consider all proposals submitted with the required total cost information.

61) Page 14, Section II, 2nd Paragraph. Will you accept a separate redacted proposal for any CORA requests?
**OSA Response:** Any proprietary information included in the proposal must be clearly and specifically designated as such in the proposal. The OSA will redact proprietary information from the proposal pursuant to 24-72-204(3)(a)(IV), C.R.S., allowing for the denial of inspection of records including trade secrets, before providing the proposal in response to a CORA request. Alternatively, the OSA would accept a separate redacted proposal for any CORA requests.

62) Page 14, Item D.4. If a proposer does not have experience working with SIPA will they lose evaluation points?

**OSA Response:** No, there is no criteria, as noted in the RFP related to “experience working with SIPA” against which proposals will be evaluated. Please refer to page 17 of the RFP for the criteria the OSA will use to evaluate submitted proposals.

Questions from Firm #8:

63) During the COVID 19 pandemic, can we submit proposals electronically?

**OSA Response:** Yes, as noted in the RFP, electronic submission of proposals via email to the Contract Monitor is the required method of proposal submission.

64) How many website visitors do you have monthly?

**OSA Response:** The number of visitors to the OSA website is not subject to the requirements of this evaluation.

65) Is there any risk assessment methodology that is currently implemented?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

66) Will the penetration tests be performed in production or in a controlled environment?

**OSA Response:** 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 objectives, 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 objectives.

67) Are there any restrictions on the use of tools to perform vulnerability analysis or penetration testing?
**OSA Response:** The OSA would not necessarily foresee any restrictions on the use of tools to perform the vulnerability assessment and penetration test. However, this type of information would need to be determined, agreed upon, and included in the rules of engagement that must be developed and put in place between the Contractor and SIPA prior to the beginning of fieldwork in order to agree in writing to any rules governing the manner in which the testing or assessment is to be conducted. As such, this information should be assessed by the selected Contractor, and included in the rules of engagement between the Contractor and SIPA, if necessary, once the engagement commences and as determined through the Contractor’s planning and risk assessment procedures.

68) Taking into account that planning meetings will be held prior to the start of the security assessment. The analysis and exploitation of vulnerabilities are going to be carried out with a total knowledge of the analyzed systems or only with the necessary knowledge to perform these activities?

**OSA Response:** 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 objectives, 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 objectives.

69) Is there any established mechanism for encryption of protected or confidential information?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

70) Is the evaluation and security analysis going to be part of a process of continuous improvement and maintenance of security?

**OSA Response:** The OSA does not currently have any plans to contract for additional work beyond the scope of the evaluation that was outlined in the RFP.

71) Is there previous security analysis that can help to plan and develop the security evaluation?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.
72) How often are security analysis performed on the target systems?

**OSA Response:** This information should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

73) In case of detecting critical vulnerabilities, is there a special flow to report it?

**OSA Response:** See response to questions #59 and other related responses. Also, this type of information should be determined, agreed upon, and included in the rules of engagement that must be developed and put in place between the Contractor and SIPA prior to the beginning of fieldwork, in order to agree in writing to any rules governing the manner in which the testing or assessment is to be conducted, including any special flow to report critical vulnerabilities. As such, this information should be assessed by the selected Contractor, and included in the rules of engagement between the Contractor and SIPA, if necessary, once the engagement commences and as determined through the Contractor’s planning and risk assessment procedures.

74) Do you have an initial idea on the current state of the systems to be analyzed regarding information security?

**OSA Response:** The OSA does not have an initial idea on this. It should be requested and assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP.

Questions from Firm #9:

75) What is the approximate number of websites, web applications and web services expected to be included in the assessment?

**OSA Response:** See response to question #48 and other related responses.

76) Do you have an approximate number/percentage of the websites, web applications and web services expected to be included in the assessment that are externally/Remotely accessible versus internal facing?

**OSA Response:** See response to questions 21, 49, and other related responses.

77) Please confirm whether this evaluation is to be conducted as a consulting engagement or as an audit under audit standards.

**OSA Response:** According to page 5 of the Request for Proposal, the engagement will be conducted as a performance evaluation and is not considered an audit under government auditing
standards. That said, the OSA requires the engaged Contractor to draft any findings and related reports in accordance with OSA standards, as explained on page 8 of the Request for Proposal.

78) Will coordination with third party vendors be necessary to conduct any of the website, web application and web service evaluations?

**OSA Response:** This information should be assessed by the selected Contractor, as necessary, once the engagement commences during the Contractor’s planning and risk assessment procedures and when performing the work necessary to satisfy the evaluation objectives, project deliverables, and timelines outlined in the RFP. 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 objectives, 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 objectives.