The State Bar of California

Network Analysis & Security Assessment

Request for Proposal: Questions & Responses

November 15, 2016

1. The solicitation request EPO specialization as a requirement but do not see EPO configuration and firmware comparisons to industry listed as a service to be performed within Section A. #2. Can you confirm if CALBAR would like contractor to provide this EPO Configuration & Firmware services?

   This is listed as a preferred qualification since we make use of it although see EPO configuration and firmware comparisons to industry are not required as an evaluation point.

2. If answer to above question is "yes, call for an EPO specialist", what products are managed through EPO that are to be considered in scope for the configuration evaluation or is scope limited to the EPO server configuration itself or is no EPO server present.

   EPO is managing Virus Scan, Host Intrusion Protection, and Site Advisor via an on-prem server.

3. How many numbers do you want to be used during War Dialing?

   Minimum four: two in each office (e.g., 1 fax/copy machine, 1 system/server).

4. What are the operating systems of end-user computers and workstations?

   State Bar workstations run Windows 7.

5. Do computers and workstations run anti-virus and/or any malware protection?

   Yes, Stat Bar workstations run McAfee.

6. Could you please give specific examples of software/programs included in the "client-side test" (pg. 7, section 1)?

Web browsers (IE 11, Firefox), media players (Windows Media Player) and document editing programs (MS Word, Adobe Acrobat) are included in the client-side testing.

7. How many individuals are employed by your organization?

The Bar has roughly 575 employees.

8. General: Can we use the CALNET 2 agreement as the contractual vehicle?

We are on CalNet3.

9. Section III. A.3: How many locations are involved in the storage, processing, and transmittal of your sensitive information that is in scope (which locations should be included within the assessment for the physical security review?) Please include the type of facility and where the facility is located.

Our two offices; one in Los Angeles and other in San Francisco.

10. Is your organization subject to any specific (security and privacy-related) regulatory or industry standard requirements?

No.

11. How many staff in IT?

25 staffers.

12. How many staff in security?

Two: One IT Analyst II position is currently Open to Hire; One IT Analyst I.

13. Is your IT infrastructure/information assets centrally managed?

Yes.

14. Does the State Bar want its Security Awareness Program reviewed or do you need the program developed?

The Bar needs a program developed.

15. Do you need a web-based training solution? If so, how many seat/users need to be trained?

Open to vendor proposal as fit with industry best practice.

16. Do you need a hosted solution or do you have your own LMS?

There is no LMS in place today.

17. Do you want the solution white labeled?

Undecided at this time.

18. Do any playbooks for specific incident types exist and, if so, how many?

No

19. Is there an IR team in place?

Not formally.

20. Do you have technology to support the IR Plan / detect events and incidents?

Yes.

21. What are the tools in place today?

Specified within RFP.

22. Is wireless testing limited to two locations as listed under LAN Networks on page 3?

Yes.

23. Section III. A.1.e: Is this limited in scope to the 100 IP addresses as listed under "External Penetration Testing Assets of Server Locations" on page3?

Yes.

24. Are in-scope database platforms limited to Microsoft SQL or are other SQL server platforms in scope?

Yes, MS SQL.

25. Section III. A.1.h: Is this web application publically available?

Yes, https://www.calbar.ca.gov/Attorneys/MyStateBarProfile.aspx .

26. Can it be tested remotely across the Internet or must it be tested on site?

Yes, it can be tested remotely.

27. Section III. A.1.h: Is the requested assessment to be performed from an unauthenticated perspective or will the team be provided credentials to access all features/pages of the site for testing?

Credentials can be provided.

28. How many user role levels would be in scope for testing (i.e.: read only, change, super user, site admin, etc.)?

Open to vendor recommendation.

29. Please describe the features and functions of the web site (i.e.: login, search, user profile creation, real-time chat, messaging, etc.) to help us gauge the size and complexity of the applications.

No chat or messaging; https://www.calbar.ca.gov/Attorneys/MyStateBarProfile.aspx

30. What is the vision for knowledge transfer? For example, is this simply a proctored walkthrough of the report and approach or is this to be viewed as more of a training exercise for a half day or a day?

Training; duration as recommended by vendor.

31. How many client images will be in scope for client side testing? Can you list specific applications that would be tested in total?

"Client images", one. My State Bar Profile (MSBP);
https://www.calbar.ca.gov/Attorneys/MyStateBarProfile.aspx

32. Will you provide all of the possible Direct Inbound Dial numbers to the selected vendor?

Yes.

33. What are the major challenges, issues and pain points for the State Bar?

Definitive Security Posture.

34. Are there any network strategies being developed internally?

Yes.

35. Is there a movement to public cloud?

In some areas.

36. What cloud applications exists today (such as O365)

Out of scope.

37. Is circuit utilization provided via any of the management tools?

Yes.

38. Are their probes or taps providing application level visibility?

Yes.

39. Is Netflow enabled? Is there a NetFlow collector installed?

Yes, on the Internet, Firewall, and WAN router. Yes, through Scrutinizer.

40. What vendor platforms exist for the LAN and WAN (Cisco, Juniper, Arista etc.?

Cisco, CheckPoint, and F5.

41. What vendor platforms exist for the WLAN?

Cisco.

42. Does the State Bar have its own Public IP address allocation from ARIN?

Yes.

43. Is there documentation of the physical connectivity topology?

Yes.

44. Is there existing inventories of equipment?

Yes.

45. How many locations provide Internet connectivity or use Internet transport?

2.

46. Who is the primary/secondary internet carrier(s)?

AT&T and Level3.

47. Is broadband Internet leveraged for connectivity?

No.

48. Are there capacity planning tools in the environment?

No.

49. Is the QoS architecture utilizing a 4CoS or 6COS model?

Not sure.

50. How does the State Bar handle proactively changing QoS to support changes in application BW changes?

Done passively to the scoping of the application manufacturer.

51. Will asset value, risk tolerance, and security categorizations be provided? Identification of asset value is generally driven by the enterprise risk management and/or business management. Security team can leverage the asset values and risk tolerance to assist in prioritizing the security risk ratings for recommendations on mitigating security risk to acceptable levels; however, asset values and risk tolerance should be available to support.

No specific document exists that defines this; looking to work with vendor to identify.

52. With timing of RFP process and holidays, it’s only reasonable to expect that we could start the project. Completing the assessments and providing recommendations could be done by February 2017; however, we are unable to provide dates on “remediation” related items other than recommendations at this time.

Adjusted date expectations are:
November 11, 2016: Submission of questions deadline
November 18, 2016 (4p.m.): Submission of proposals deadline
December 2, 2016: Notice of intent to award
December 9, 2016: Final selection
February 28, 2017: Performance of assessment to be completed
March 31, 2017: Support consultative remediation to be completed

53. Does CA State Bar fall under the same CA Information Security Regulations as the majority of State Agencies such as SIMM Section 5300 and SAM sections 5300 – 5365.3?

No; the State Bar of CA is a "quasi-state" organization.

http://sam.dgs.ca.gov/TOC/5300.aspx
http://www.cio.ca.gov/Government/IT_Policy/SIMM.html

54. This would require alignment with CA Security Control requirements which largely map to National Institute of Standards Special Publication 800-53r4. Is a Compliance Readiness Assessment to this standard required as part of this RFP?

Not required but certainly expect vendor's guidance to industry best practices.

55. Making capability improvement recommendations based on industry good practices is simpler from an effort level than ensuring mapping to CA State (NIST) control requirements.

Understood, see last response.

56. Vendor must provide an onsite Project Manager for the duration of the effort. What is the expectation, number of hours days?

As vendor deems required, however should be addressed in RFP response.

57. Can project management work be done remotely?

Yes.