The State Bar of California

Network Analysis & Security Assessment

Request for Proposal: Questions & Responses

November 8, 2016

1. Will California Small Certified businesses be given preference in weighting of this RFP? We did not see a provision regarding SB cert.

   The State Bar does not give preference to small businesses; including any kind of certification won't hurt but all bidders are treated equally.

2. Was there a question submittal period or deadline in the RFP process? If not, are we able to conduct a site visit and ask more questions regarding the RFP content?

   There is a question submittal period per Section VI. General Information; subsection G. Questions Regarding the RFP. Questions are to be received five days before the RFP submittal deadline. "Days" means business days in the RFP; 5:00PM on Friday November 11 is the preferable deadline. There will be no on-site tours or visits at this time.

3. Are we able to use a third party sub-vendors for part of the work?

   Yes, however the sub-vendor and their proposed scope must be clearly listed and credentials provided per Section VI. General Information; subsection A. Submission Requirements (1). The sub-vendor will contract with the primary vendor, not the State Bar.

4. Our legal team is unable to review the terms of the RFP until after it is awarded and so we are unable to fully agree to them, is that a problem?

   Per Section VI. General Information; subsection A. Submission Requirements (9) specific terms may be reserved for future negotiation, but must be clearly identified and reasons given for the reservation.

   Understand that all documents submitted to the State Bar are subject to the California Public Records Act.

5. Is there an expectation of analysis for the 3,000 network devices authorized on the network?

   No, there is no expectation of a full analysis of every device.

6. Does manual verification entail an onsite inventory of the (100) IP addresses and the equipment?

   No, there is no inventory process intended.

7. On page 10, under State Bar Responsibilities, what will determine the transition from draft deliverables to final deliverables with respect to the State Bar review period and changes to be made, if needed?

   The review period is to address any "obvious" omissions, complexities, or out-of-scope tasks submitted with proposals; review will be done expeditiously and the draft deliverables will be considered as final deliverables once there is agreement between the State Bar IT Project Team and the vendor with all issues satisfactorily resolved.

8. Will the vendor have access to the current monitoring tools (SolarWinds, Scrutinizer and SCOM) for network discovery and packet capture tasks?

   Yes, the vendor will have accessed to current monitoring tools while partnered with State Bar staff.

9. Will the vendor be able to install a temporary VM for a network discovery tool/application in the current data center for extended network capture tasks?

Yes, under the supervision of the IT Project Team the vendor may install a temporary virtual machine for discovery within the authorized scope; to be removed upon delivery of final products unless otherwise negotiated.

10. Will VPN access be made available to network engineers to the San Francisco and Los Angeles networks to facilitate performing the Scope of Work?

Yes, State Bar VPN access will be granted on an as-needed basis to Vendor personnel.

11. The Network analysis requires review of the wireless architecture. Please provide a description of the scope and scale of the wireless network to be evaluated.

Wireless Controllers (2)

- *Los Angeles: ~36 Access Points*
- *San Francisco: ~11 Access Points*

Broadcast SSIDs (2)

- *Guest: Internet only*
- *Staff: Internal Active Directory authentication required*
- *2 VLANs*

12. Under "Minimum qualifications and experience", the last statement says "Public Agency is preferred". Does this mean that the proposer must have experience providing security vulnerability and risk assessment services to public agencies, or does this sentence have another meaning?

This is actually a Preferred Qualification; the State Bar prefers vendors who have experience providing security vulnerability and risk assessment services to public agencies and the additional requirements inherent in them.

13. If data or information is stored in the in-scope architecture, have you performed data and/or asset classification?

There is data stored this architecture; classification has not been performed.

14. How would you describe your documentation set for the in-scope architecture?

There is minimal documentation of the architecture as a whole.

15. Is there an existing logical network diagram that can be shared showing the products to be assessed and the interconnections between them?

Yes, there is an existing diagram which is available upon award or in advance by request.

16. How many sets of information security policies do you maintain?

The State Bar IT Department maintains a single set of security policies, however they are in need of review and update. The products of the assessment will be used to update the current policies; recommendations on best practices are welcome and encouraged.

17. What is the size of your information security policies (# of pages) and are they mapped to any particular control standard?

The current security policy is 26 pages in length and is not mapped to any particular control standard.

18. Is the information security function centralized?

Yes, information security is a centralized function within the State Bar IT Department.

19. How many systems handle PII data?

There is a single system that handles PII data (applicants, membership, and perhaps public data); it resides on the i5.

20. In conjunction with a Penetration test, we can pair a phishing campaign to further our exploit effort into the environment. If you are interested in this pairing please share how many email addresses should be used for this campaign?

Unless the proposed phishing campaign is included as part of your assessment standards we consider it to be an out of scope add-on and are not interested at this time. Add-on's may be quoted within the proposal as optional items.

21. For the penetration test, will this also cover PCI?

Unless the proposed Payment Card Industry security test is included as part of your assessment standards we consider it to be an out of scope add-on and are not interested at this time. Add-on's may be quoted within the proposal as optional items.

22. For the penetration testing, is a retest required?

No, no retest is required.

23. Can you define the Security Infrastructure needing review? Firewalls (Make, Model, Version, Configuration HA or Stand-Alone, and how many rules are on each one). Please also define the same for IDS/IPS.

The State Bar employs Cisco and Checkpoint firewalls; F5 IDS/IPS.

24. Provide a list of operating systems for the servers and list the application server's in scope for Server hardening?

<u>Physical (3)</u>
Windows 2003 (Web)
Windows 2008 (Web)
Windows 2008r2 (SQL)

<u>Virtual (1)</u>
Windows 2012 (SQL)

25. For the Vulnerability Scanning, are you looking for a one-time assessment or would you be receptive to a subscription based service?

The State Bar is looking for a one-time assessment. A subscription based service may be included as part of your recommendation for future mitigation.

26. Would you be interested for the Web Application testing to also use a subscription based service or are you seeking a one-time assessment?

The State Bar is looking for a one-time assessment. A subscription based service may be included as part of your recommendation for future mitigation.

27. For the web applications in scope, what type of web application is under consideration for assessment?

The My State Bar Profile web portal is within the intended scope of this RFP; located at: https://members.calbar.ca.gov/login.aspx?ReturnUrl=%2f

28. Is there a budget amount allocated for this project that you can provide to us?

The State Bar does not disclose budgetary information.

29. Is concerted rolled up reporting the only way you will accept?

Concerted rolled up reporting is strongly preferred; if another type is suggested please make the case for it in your proposal.

30. Or would accept standalone reporting for each functional area?

Standalone reporting per functional area is acceptable based on quality.

31. Is having a Project Manager on site a necessity?

An on-site Project Manager is preferred but not required.

32. How many different types of operating systems (e.g. Windows, UNIX, mainframe, etc.) are present in scope?

Windows (135)

System i (1)

33. Provide a number for each type of server:

Estimated In-Scope
Web Servers (6)
Application Servers (20)
Database Servers (16)
Log Servers (1)
Administrative / Other (2)

34. Section II, Statement of Work – Background (p.2) - This section indicates that the vendor should evaluate the State Bar's security controls against the CIS 20 Critical Security Controls (SANS Top 20); however, these standards are not mentioned in the detailed scope of work that starts on page 4. Does the State Bar want the vendor to conduct a gap analysis against the CIS 20 CSCs and map findings and recommendations to these standards?

Yes, a gap analysis is desired. SANS Top 20 is inferred within Section III Requirements and Scope of Work; subsection B. Security Assessment (8) & subsection D. Penetration testing (16).

35. Section III, Requirements and Scope of Work – General Work Requirements (p. 4) - Under Line Item 2, Configuration and Firmware Comparisons to Industry Best Practices, what is included in the "Security Infrastructure"?

Security Infrastructure includes: Cisco Firewalls/VPN & Checkpoint IPS/Firewalls; F5 Web Application Firewall; and WebSense.

36. Section III, Requirements and Scope of Work – General Work Requirements (p. 4) - How many MS SQL databases is the vendor expected to test?

The vendor is expected to test 3 SQL databases.

37. Section III, Requirements and Scope of Work – General Work Requirements (p. 4) - How many routers and switches are in scope for the configuration audits?

Routers (4)
Switches (60)

38. Section III, Requirements and Scope of Work – General Work Requirements (p. 4) - How many VPN appliances are in-scope for the configuration audits?

The State Bar's VPN solution is embedded in the 2 Cisco Firewalls; in-scope.

39. Section III, Requirements and Scope of Work – General Work Requirements (p. 4) - Line Items 3, 4 and 5 indicate that the vendor will either review or develop information security policies and procedures, a user security awareness training program and an incident response plan. Which, if any, of these artifacts exist already? In other words, is the vendor expected to review and modify these artifacts, or to develop them from scratch?

The State Bar IT Department maintains a single set of security policies, however they are in need of review and update. The products of the assessment will be used to update the current policies; recommendations on best practices are welcome and encouraged.

40. Section III, Requirements and Scope of Work – Security Assessment (p. 5) - Does the Security Plan include policies, procedures, guidelines and standards for user security awareness training and incident response?

Yes, the Security Plan includes all items listed above.

41. Section III, Requirements and Scope of Work – Penetration Testing (p. 7) - Should social engineering tests be phone-based only, or is email phishing desired, as well? How many users should the vendor target in the social engineering campaign?

Email phishing is not a desired method; the number of users targeted is at the discretion of the vendor.

42. 24) Is English the primary language used in your organization and to be used during the assessment?

Yes, English is the primary language used at the State Bar.

43. What is the size of the target address range(s) to be assessed (e.g. one class B network, three class C networks, etc.)?

San Francisco
Class C (1)

Los Angeles
Class C (1)

44. How many Internet accessible systems are in scope for testing?

2 internet accessible systems are in-scope.

45. Are there any timing limitations (e.g. night time or weekend only) limitations on the external testing? If so, please specify.

There are no timing limitations at this time.

46. What is the size of the target address range(s) to be assessed (e.g. one class B network, three class C networks, etc.)?

San Francisco
Class B (16)
Class C (11)

Los Angeles
Class B (13)
Class C (9)

47. Approximately how many servers are in scope for testing?

Approximately 45 servers are in-scope.

48. Approximately how many workstations are in scope?

Approximately 700 workstations are in-scope.

49. Approximately how many network devices (routers, firewalls, etc) are in scope?

Firewalls (2)
HA Firewalls (2)
IPS (2)
HA IPS (2)
VPN (2)
Edge Routers (2)
Internal Routers (2)
Core (2)

50. Are there any timing limitations (e.g. night time or weekend only) limitations on the internal testing? If so, please specify.

There are no timing limitations, but all non-interrupting activities are preferred to take place during standard business hours (8:45am – 5:00pm, M – F).

51. What locations are in scope for wireless testing?

Both San Francisco and Los Angeles locations are in-scope.

52. How many locations are in scope for this wireless testing?

Both San Francisco and Los Angeles locations are in-scope.

53. At each location, how many buildings and floors are included in the scope of wireless testing? What is the approximately square footage per location (if known)?

San Francisco (1)
7.3 floors (13 total) – 120,000 usable sq. ft.

Los Angeles (1)
5 floors (5 total) – 110,000 usable sq. ft.

54. How many separate wireless networks are in scope and what are they used for (guest network, employee, point-of-sales systems, etc.)?

Wireless Controllers (2)

- *Los Angeles: ~36 Access Points*
- *San Francisco: ~11 Access Points*

Broadcast SSIDs (2)

- *Guest: Internet only*
- *Staff: Internal Active Directory authentication required*

55. Are there any thick access points in use or does the wireless environment consist of thin access points under a wireless controller?

The State Bar employs only Thin Access Points under a wireless controller.

56. If multiple locations are in scope, does each location have its own configuration, or are all configurations centrally managed?

Each location has its own configuration.

57. What brand(s) of access points and controllers are in use?

Only Cisco brand access points and controllers are in use.

58. What encryption type(s) are you using (WEP, WPA-PSK, WPA Enterprise, etc.)?

WPA+WPA2
Web Authentication (Guest Network only)

59. Are you using a captive portal?

Yes, the wireless Guest Network uses a captive portal.

60. Is rogue access point detection within scope?

Yes.

61. Is there a standard client configuration that you would like us to review?

Yes, it will be available upon award.

62. How many locations are in scope for a physical security assessment?

Both San Francisco and Los Angeles locations are in-scope.

63. Are you interested in a physical penetration test, a physical security review, or both?

The State Bar is interested in a physical penetration test.

64. Extent of physical security testing (tailgating, attempting to access certain areas such data center floors, etc.

Scope and extent of physical testing will be determined after award and based on vendor proposal.

65. Do you have established policies and directives associates with Physical Security? If yes. How many documents?

Policies, processes and documentation will be available to vendor upon award if physical testing is agreed to.

66. Social engineering through telephone – phone calls to obtain sensitive information from employees or helpdesk; how many employees should be called?

The number of State Bar employees to call is at the vendor's discretion.

67. What information would you like us to attempt to gain (e.g. passwords, customer data, etc)?

Attempt for users to reveal their passwords to any system.

68. Social engineering through phishing – emails to employees to direct them to a "malicious" web site; how many employees are in scope?

The number of State Bar employees to call is at the vendor's discretion; phishing is not preferred as a separate method unless it meets the vendor's own standards. No specific information is desired through this method.

69. How many locations are in scope?

Both San Francisco and Los Angeles locations are in-scope.

70. Which of the following policies and related procedures exist and approximately how many pages long is each document?

DOCUMENTATION	EXISTS?	APPROXIMATE NUMBER OF PAGES
Network Diagram(s)	*Y*	*1*
Firewall Policy Documentation	*N*	
System Hardening and Configuration Standards	*Y*	*1*
System Patch Policy & Procedures	*Y*	*1*
Change Control Procedures	*Y*	*2*
Data Retention and Disposal Policies	*N (Separate Ongoing Initiative)*	
Encryption Policy	*Y**	*26*
Anti-Virus Policy	*Y*	*2*
User ID Authorization Forms	*Y*	*1*
Data Restriction and Privilege Control Policy	*N*	
Password Policy	*Y*	*1*
Security Log Policy	*N*	
Security Assessment Reports	*N*	
Application Code Review Policy	*N***	
Incident Response and Monitoring Policy	*Y**	*26*
Disaster Recovery Plan and Policy	*Y (Draft)*	*4*
System Backup Policy	*Y*	*2*
Third Party Contracts (handle cardholder data)	*N*	

Information security policy	*Y**	*26*
Information security plan	*N*	
Storage/maintenance of Hard Copy and Electronic Media Policy	*Y**	*26*
Media Inventory Documentation	*Y*	*2*
Media Destruction Policy	*N (Separate Ongoing Initiative)*	

** Refers to same single security document.*
*** Strictly adhered to practice, but no formal document.*