RFP 2018-04 – Information Security Third Party Assessment
Questions and Answers

QUESTION	ANSWER
1. Page 5, Section 1.4 – are we reading this correctly that, across a maximum total cost of $802,000, no more than $465,000 can be invoiced in either of the two years of the project?	$465,000.00 first year and second year $337,000.00
2. Page 20, Section 3.8 – will travel expense not be reimbursed at all, or must our proposal include an assumption of travel costs as part of the single fixed fee cost proposal?	No travel reimbursements.
3. Exhibit A (Standard Agreement), page 7 – Requirement 5 – This requirement seems to be an open-ended requirement to provide cyber incident forensic investigation services. Those are almost always performed on an hourly basis, and are impossible to estimate, as they will always depend on the nature and extend of the incident and the forensic requirements. Is a rate schedule for those services sufficient?	This is for making forensic copies of hard drives as required.
4. Once awarded, when is the project expected to start?	As soon as the contract is awarded.
5. In addition to the MARS-E security and privacy controls, does Covered California wish for us to include an assessment of the HIPAA Security, Breach Notification and Privacy Rules?	No
6. What was the date of the last risk assessment? a. What was performed? b. If we are awarded this contract, can we see the previous risk assessment report?	June 2018 a. Evaluating risks in the system and control implementation. b. TBD
7. Does Covered California have an Incident Response Plan?	Yes
8. If yes to above, when was the last time the Incident Response Plan was tested? And how was it tested?	Annually Based on the process documentation.

9. What is the size of your network? a. External – Number of internet facing IPs? How many are live? b. Internal – Number of IP addresses? i. Number of subnets ii. If possible, breakdown of servers, workstations, and network devices iii. Number of virtual machines	Will be shared if contract is awarded.
10. How many physical locations are in scope?	2 – 5.
11. Can all internal IP addresses be access from one location? This is to determine if the internal penetration test can be performed from one location, or if multiple site visits are required.	One to two locations.
12. How many Wi-Fi networks are there, and at what locations?	Multiple, two locations.
13. How many web applications are there? Do these include web databases and forms for submission?	One. Yes.
14. Are web applications custom developed? If so, what SDLC methodology is used?	No
15. Does Covered California maintain payment card (PCI) data on premises?	No
16. How does Covered California manage payment card transactions? What are the payment channels (ex. Card present, web-based, token, etc.)	N/A
17. Does Covered California submit a ROC or SAQ for PCI compliance? If awarded the contract, can we see the latest ROC/SAQ for reference?	N/A
18. What are the primary applications that host PHI/ePHI? Where are they located?	One. Data Center
19. Does Covered California allow for remote access into the environment?	Yes
20. Is social engineering in scope? For example remote (phishing, pretexting) or physical (tailgating, posing as the delivery person) means?	No

21. Can bidders include additional information other than what is specified on 4.2.2? For example, a cover letter and executive summary?	Yes
22. Is the scope of the assessment for all controls within the MARS-E framework? Or is the scope of the assessment a subset of the controls from Year 1, Year 2, or Year 3?	All controls.
23. Could you please provide the number of IP addresses, applications, and servers that are in scope of the vulnerability assessment?	Will be provided when contract is awarded.
24. Please provide the number of policies and procedures in place that would need be to reviewed.	Approximately 75 plus or minus
25. Is the IT organization centralized or decentralized?	Decentralized
26. Has a security control framework been adopted? If yes, which one?	MARS-E (NIST)
27. When was the last information security assessment of this nature performed?	Ongoing – full in 2016.
28. Are there documented policies, procedures, standards, and guidelines in place? If so, how many?	Same as 24.
29. Is there an incumbent and are they eligible to bid on this project? If so, who was the incumbent and what was the value of the contract?	N/A
30. How many data centers does Covered California maintain?	Two
31. For Requirement 2, external network vulnerability assessment and penetration testing, what is the approximate number of active IPs?	Will be provided when contract is awarded.
32. For Requirement 2, internal network vulnerability assessment and penetration testing, what is the approximate number of active IPs?	Will be provided when contract is awarded.
33. For Requirement 2, is web application penetration testing in scope? If so, how many applications and/or URLs?	Three
34. For Requirement 2, how many staff will participate in knowledge transfer?	Four to Six

35. For Requirement 2, is a wireless network assessment in scope? If so, how many controllers and locations are in scope?	Possibly. 2-6
36. For Requirement 2, are detailed configuration reviews of network devices, servers, or databases in scope (e.g., routers/switches, firewalls, IDS, workstations)? If so, please provide quantities for each component in scope, including the number of operating systems. Please indicate if firewalls are in HA pairs.	Yes. Will be provided when contract is awarded. Yes
37. For Requirement 4, is Covered California seeking to conduct a risk assessment (a review of critical enterprise technologies and processes) with the deliverable of a prioritized risk matrix?	Possibly
38. For Requirement 4, how many staff will participate in knowledge transfer?	Four to six
39. Would Covered California accept a USB in lieu of a CD-ROM for the electronic proposal response?	No.
40. Our firm's methodologies and client information are typically marked "confidential" on our proposals to safeguard our business and clients. The RFP states these pages may be rejected. Should we provide a redacted copy of our proposal instead?	Yes, you can provide a redacted copy.
41. We noticed that the attachments listed on Attachment 10: Proposal Checklist do not match the RFP files. For example, Attachment 2 on the Proposal Checklist is Federal Debarment, Suspension, Ineligibility and Voluntary Exclusion – Certification, but the file labeled Attachment 2, when opened, states that it is Attachment 2: Form 700 Statement of Economic Interest. Are these forms fine to submit as-is, or will Covered California provide a revised checklist or forms?	The RFP files list is correct. We are no longer including the Federal Debarment, Suspension, Ineligibility and Voluntary Exclusion – Certification. See the updated List of Attachments for the updated Attachment 9: Proposal Checklist.