RFP 2021-05 Information Security 3rd Party Assessment
Questions and Answers

Bidder Questions:	Covered CA - Response:
1. In the scope section (Exhibit A), page 3 of 16, Requirement 2, the words "audits" and "assessments" are plural. Page 6 of 16, Requirement 4 calls for "additional assessments as requested". Given the evaluation criteria includes selection of winning bid based (in part) on low price, and the actual work effort is not fixed, what are the state's expectations concerning bidders calculation of hours of work effort?	Level of work varies and will be further defined and agreed upon by contractor and Covered Ca on a monthly basis.
2. Given the CMS audit cycle is a full assessment by an independent assessors every 4 years, with self-attestations in years 2-3, what are the state's expectations for utilization of the independent assessor in years 2 and 3 (we do have clients who utilize the our independent assessor services for years 2 and 3 self-attestations, but as it is not a requirement, please clarify the states intent for years 2-3 of the contract).	Expectation is to use independent assessor for full assessment, unless required by authoritative agency (e.g. CMS).
3. Exhibit A, Requirement 3 (page 5) – Does the phrase "Triennial Certification and Accreditation assessment tasks that includes testing of all MARS-E security and privacy controls for the third-party assessment. The third-party assessment shall include attestation requirement as mandated by CMS based on MARS-E Security Assessment Control CA-2 to include security and privacy controls and control enhancements" include any requirements that are in addition to the one 'Full' Independent Assessment for ATC renewal required by CMS every four years? Is the state requesting anything in addition to or other than those independent	This requirement includes all tasks required as part of the full independent assessment required by CMS.

assessor services as required by CMS?	
4. Exhibit A, Requirement 3B (page 5) – for clarity, is the state simply requesting/ensuring that the 'recommendations' field of the SAR be of sufficient clarity and detail as to allow the state's integrator to understand the weakness and the devise a plan of action, or is there something in addition to the CMS requirement that is being requested?	The contractor is responsible for clearly documenting any weaknesses during evaluating or assessing controls and communicate to SI who is responsible for executing the remediation or mitigation steps.
5. Exhibit A, Requirement 3F (page 6) – the phrase 'for management' is interpreted to mean a deliverable that is over and above what is required by CMS, is that an accurate assumption?	The intended audience for this report includes Exchange IT and Business management.
6. Exhibit A, Requirement 3H.C (page 6) – we believe the intent is to emphasize the requirement to provide a SAP that is in alignment with CMS requirements, is there something in addition to the CMS requirements the state is requesting?	Requirement is inclusive of all necessary reports and plans required by CMS.
7. Exhibit A, Requirement 3H.C (page 6) - the requirement refers to systems (plural). Are there other systems in scope in addition to the MMIS system, and if so can the state provide any information to indicate scope/scale (i.e. # of hosts, IPs, URLs, etc.)?	System landscape includes multiple hosts and services; on-premise and cloud-based.
8. Exhibit A, Requirement 4 (page 6) – can the state provide an indication of how many additional assessments would the requested per year? Can the state confirm the term assessment refers to technical testing (i.e., vulnerability scans, pen tests, or is the scope inclusive of reviews of updated operational controls?	Additional assessments (no more than three) have been required during full independent attestation, as required by authoritative agency (e.g. CMS).
9. Exhibit A, Requirement 4.L.5 (page 6) – can the state provide any indication of scope/scale of the amount of static code to be reviewed (types of code (i.e. web app, etc., lines of code, scripting vs compiled, COTs, etc.?	A combination of web applications, compiled code, and scripts are in-scope. Approximately: 1200 IPs, up to 10 URLs, and 75 code components, 2 million lines of code.
10. Exhibit A, Requirement 4.m (page 8) – how is the requirement for on-site assessments affected by the pandemic? Is the CISO currently	Customer supports hybrid work environment. Remote work is permitted.

granting any exceptions or approvals for remote work?	
11. Exhibit A, Requirement 5 (page 8) – can the state provide any context for scope/scale for this requirement, such as the # of incidents requiring this service in the past1/3/5/10 years? As with question 1, can the state clarify its intent concerning providing pricing with estimated hours when the number of times the service will be delivered is not known?	Varies. Level of work varies and will be further defined and agreed upon by contractor and Covered Ca on a monthly basis.
12. Regarding Section 4.2.1 of the RFP: Attachment 10: Non-Collusion Declaration, isn't listed in either the Attachment 6 Proposal Checklist or in Section 4.2.1 of the RFP. Are we correct in assuming that this form should be included in the "Required Attachments" section of our proposal as described in Section 4.2.1 of the RFP following the completed Attachment 6 form?	NA - Not a Public Works project
13. Is this engagement considered to be more of a staff augmentation? Or is the intent to be more of a program with expected deliverables?	Majority of engagement is program with deliverables.
14. Can this be a fixed fee price or as-a-service model? Or is this strictly T&M?	T&M
15. Is onsite work a requirement? If so, can you identify what portions of the engagement will adhere to that requirement? ie. certain tasks, estimated hours, etc.	On-site visits may be required as part of a specific deliverable (e.g. site assessment, etc). To be further defined and agreed upon by contractor and Covered CA.
16. How many Pen Tests will be required per year?	Minimum of one (1) per year.
17. How extensively do you utilize SaaS/Cloud services? Do you anticipate we will need to review and/or meet with some of these key partners? If so, approximately how many and which ones?	Cloud-based services are used extensively, with minimum amount using on-premise services. Limited need to meet with providers.
18. How will we access the in-scope systems (via Internet, VPN, Firewall IP restrictions, etc.)?	In-scope systems will be accessed based on needs, not limited to client-based VPN

19. What types and how many devices are in-scope for the engagement? Can any sampling be done on any of the device configurations?	Approximately: 1200 IPs, up to 10 URLs, and 75 code components, 2 million lines of code. To be discussed and agreed upon between contractor and Covered Ca.
20. How many (approximate) rules are on each device (Firewalls, IDS, etc.) or how many (approximate) total rules are there on all in-scope devices.	Variable, non-static environment.
21. Do you have an updated network diagram that can be provided at the start of the engagement?	Yes.
22. Number of live hosts/nodes exposed to the internet? A rough estimate or range is fine.	Up to 10.
23. At what hours of the day would internal/external pen testing be performed? Business hours or after hours or weekends?	After hours, during non-critical operating periods as defined by customer.
24. Are any in-scope nodes hosted with a third-party cloud provider?	Yes.
25. What level of information sharing would you like to use during this project? Semi-Blind (provide IP ranges and hostnames only), or Hybrid (have contractor identify target ranges and fill in any gaps prior to the assessment)	Full Disclosure.
26. What level of evasiveness would you like us to employ for this engagement? Non-Evasive, or Hybrid-Evasive	Non-evasive
27. Do you leverage a GRC, IRM, and/or risk analysis (e.g., RiskLens) solution for your risk assessments? If, so please identify what you use if it is required for us to utilize for this assessment.	Not required as part of the assessment.
28. Would Covered CA accept 4-years E-MARS experience, plus additional experience with the more stringent CMS ARS to show the proposing vendor meets and exceeds the 5-year E-MARS experience minimum requirements?	One (1) year of CMS ARS experience can be used to meet the minimum years of overall experience requirement.