RFP 2026-01 Information Security Services
Questions and Answers

Contents

Questions about Current Contract/Contractor

#	Proposer Questions:	Covered California's Responses:
1	**Security Platforms in Scope** Sections 2.1.6 and 2.2.3 and Exhibit A require support for Covered California's governance, risk, and compliance system, log aggregation, threat detection, endpoint security, and data-loss-prevention capabilities. Will Covered California identify the current platforms and technologies used for: • Governance, risk, and compliance • Security information and event management • Endpoint security and detection • Data-loss prevention	Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
2	**Third-Party Security Vendors** Please identify the third-party security vendors currently engaged by Covered California and clarify which responsibilities will remain with those vendors versus those expected of the selected provider.	SecurityScorecard, used for conducting third-party security risk assessments, will remain. The overall third-party data risk and process oversight remains with Covered California.
3	**Backup & Disaster Recovery Platform** Is Covered California expecting the selected provider to retain and manage the existing backup and disaster recovery platforms, or should proposers anticipate migrating to their preferred solution? If the current solution is to remain in place, please identify the products and technologies currently in use.	This question is not relevant to this RFP.
4	**User & Device Counts** Please provide current volumes for: • Employees and contractors • Managed workstations • Mobile devices • Physical servers • Virtual servers • Cloud servers • Supported locations • Remote workforce population	The number of users and endpoints is approximately 2,000. Covered California is a hybrid workforce, with most work performed remotely.

#	Proposer Questions:	Covered California's Responses:
5	**Current Staffing Model** How many individuals currently support the Covered California environment today, including internal staff, consultants, contractors, and third-party vendors? Please provide a high-level breakdown of responsibilities.	The information security team includes 9 state employees. At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors.
6	**SCOPE & ENVIRONMENT** Will Covered California share information about the current security tool environment (e.g., SIEM/log aggregation, EDR, and the governance, risk, and compliance platform referenced in Section 2.1(6)) to inform the Understanding and Approach narrative and Work Plan?	Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
7	**SCOPE & ENVIRONMENT** Is there a current incumbent providing these services, and is a transition or knowledge-transfer period anticipated at contract start on December 1, 2026?	There is a current incumbent providing these services. Transition will be provided by state staff.
8	Can Covered California share a high-level overview of the current environment (applications, cloud platforms, key security technologies, and systems in scope)?	Covered California is primarily cloud-based and uses a hybrid, multi-cloud environment: Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
9	**Environment & Technology** Can Covered California provide a high-level overview of the IT environment, including: • Number of users • Number of endpoints • Number of servers • Cloud environments (AWS, Azure, GCP) • Data centers Network locations	The number of users and endpoints is approximately 2,000. Covered California is a hybrid workforce, with most work performed remotely. CalHEERS and Covered California is cloud-based using all major cloud platforms.

#	Proposer Questions:	Covered California's Responses:
10	Can Covered California provide a high-level description of its current security technology environment and scale, including its primary GRC, SIEM, endpoint, vulnerability management, IAM, DLP, and cloud security platforms?	Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
11	**General Scope** Can Covered California provide an overview of the current Information Security organization, including the number of internal security personnel and functional responsibilities?	The current information security organization consists of information security leadership, a security engineering team and a compliance team. The information security team includes 9 state employees. At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors.
12	**Environment & Technology** What security technologies are currently deployed (SIEM, EDR, IAM, DLP, vulnerability management, GRC, SOAR, etc.)?	Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
13	**Environment & Technology** Which GRC platform is currently in use?	Optro https://optro.ai/
14	**Security Incident Response** What is the current incident severity classification model?	Incident classification is based on the number of users impacted and the type of data involved.
15	**Threat Detection & Security Operations** Which SIEM platform is currently deployed?	Splunk
16	**Threat Detection & Security Operations** Who currently operates the SIEM platform. Is it internally managed or is it managed by an MSSP?	The Splunk SIEM is primarily managed by NuHarbor, the contracted MSSP.
17	Who are previous incumbents on this project?	e360
18	Is there an incumbent contractor?	Yes
19	Is there an incumbent team? Are they precluded from responding?	There is an incumbent contractor, and they are not precluded from responding.
20	**2.1 Project Team Minimum Qualifications** Is the incumbent vendor and/or their subcontractors eligible to bid on this RFP?	Yes.

#	Proposer Questions:	Covered California's Responses:
21	**Threat Detection & Security Operations** Approximately how many log sources are currently monitored?	Not relevant to this RFP
22	**Threat Detection & Security Operations** What specific security software suites, Endpoint Detection and Response tools, Identity and Access Management platforms, and Governance, Risk, and Compliance systems are currently deployed across Covered California and CalHEERS?	Security technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
23	Which systems, applications and infrastructure make up the "Covered California environments" referenced alongside CalHEERS?	Covered California is primarily a Microsoft environment. Security technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
24	**Data Protection** Which data protection technologies are currently implemented (DLP, DSPM, encryption, classification)?	Microsoft Purview
25	**Data Protection** Is there an existing Insider Threat Program?	Yes, with the expectation that improvements will be made in compliance with ARC-AMPE.
26	**Data Protection** Approximately how many repositories contain regulated or sensitive data?	There are several repositories for regulated data.
27	**Data Protection** Is Microsoft Purview or another data governance platform currently deployed?	The current solution is Microsoft Purview
28	**Penetration Testing** Do you expect vendor to include penetration testing & application security platforms or currently do you have these platforms? If yes please provide details	Penetration testing only
29	**Digital Forensics** What forensic tools are currently used?	No forensic tools are owned by Covered California; we rely on the contractor to provide forensic services and tools.

#	Proposer Questions:	Covered California's Responses:
30	**Scope of Work and Environment** Does Covered California currently maintain a governance, risk, and compliance (GRC) platform that the selected contractor would be expected to administer, or is the contractor expected to recommend and implement a platform?	Optro https://optro.ai/
31	**Exhibit A – Scope of Work, Section E. Technical Security** Can Covered California provide a high-level list of major security technologies currently deployed (e.g., SIEM, SOAR, DLP, IAM, Vulnerability Management, etc.) that the contractor will be expected to support?	Security technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
32	**Third-Party Risk Management** Approximately how many vendor security assessments, reassessments, and exception reviews are performed annually, and what assessment methodology is currently used?	SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
33	How many in-scope systems, applications and control families are covered by the annual assessment?	Annual independent assessment includes one-third of the 472 ARC-AMPE controls. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
34	Which platforms are currently deployed for GRC, security information and event management (SIEM), firewalls, endpoint detection and response (EDR), identity and multi-factor authentication, and email gateway?	Current technologies include: • Optro for GRC • Splunk for SIEM • CrowdStrike for endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management
35	What are the monthly SIEM alert volumetrics by severity?	Covered California maintains a contract with an MSSP to monitor Splunk alerts.
36	What is the current false positive rate of alerts in the existing SIEM?	Covered California maintains a contract with an MSSP to monitor Splunk alerts.
37	How many third-party assessments are performed annually, by vendor criticality or tier?	SecurityScorecard, used for conducting third-party security risk assessments, will remain.

#	Proposer Questions:	Covered California's Responses:
		The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
38	What assessment methodology is currently used for third-party reviews, and how many controls are assessed per assessment?	SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
39	Which third-party risk management platform is currently used?	Optro https://optro.ai/
40	Can Covered California provide a high-level overview of the current security technology environment (e.g., SIEM, EDR, IAM, vulnerability management, GRC platform, cloud providers, ticketing platform) that the Contractor will be expected to support?	Current technologies include: • Optro - GRC • Splunk - SIEM • CrowdStrike - endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor - MSSP
41	Can Covered California provide a high-level description of its cloud environment (AWS, Azure, GCP, SaaS, hybrid) and the approximate proportion of workloads operating in each environment?	Covered California operates a cloud-first, hybrid, multi-cloud environment using multiple commercial cloud providers, hosted SaaS applications, and limited residual on-premises infrastructure. To reduce security risk, Covered California does not disclose provider names, workload percentages, or detailed account, network, location, or configuration information. For planning purposes, prospective vendors should assume a predominantly cloud-hosted environment, distributed across multiple cloud and SaaS environments, with a minimal on-premises footprint.
42	**Security Incident Response** Approximately how many security incidents are handled annually?	Approximately 5.
43	**Third-Party Risk Management** Approximately how many vendor security assessments are performed each year?	SecurityScorecard, used for conducting third-party security risk assessments, will remain.

#	Proposer Questions:	Covered California's Responses:
		The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
44	**Third-Party Risk Management** Is there an existing third-party risk management platform?	Optro https://optro.ai/
45	**Threat Detection & Security Operations** What is the average daily log ingest volume in GB or TB per day across the environment, and is the contractor expected to manage or ingest logs directly into a state-owned SIEM or provide vendor-hosted log storage?	This is not relevant to the RFP. Covered California maintains a contract with an MSSP to monitor Splunk alerts.
46	What is the hosting model, and approximately what proportion of in-scope systems is on-premises versus cloud-hosted?	Covered California operates a cloud-first, multi-cloud environment using multiple commercial cloud providers, hosted SaaS applications, and limited residual on-premises infrastructure.
47	Can Covered California provide estimated annual volumes or historical utilization for project-based services, including independent assessments, penetration testing, digital forensics, and surge staffing? If historical data is unavailable, please provide reasonable planning assumptions so that all proposers can develop pricing on a consistent basis.	Below is an estimate of annual hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700
48	**Exhibit A – Scope of Work, Section C. Security Incident Response** Can Covered California provide historical averages regarding the number of security incidents, major incidents, and after-hours response events supported annually?	Approximately 5 security incidents. After-hours support may be needed in the case of a major security incident.
49	Approximately how many users does Covered California support?	The number of users and endpoints is approximately 2,000.
50	How many endpoints are on the network, by type (workstations and laptops, servers, other)?	The number of users and endpoints is approximately 2,000.
51	What is the total third-party vendor population in scope, and the criticality or tier distribution?	SecurityScorecard, used for conducting third-party security risk assessments, will remain.

#	Proposer Questions:	Covered California's Responses:
		The RFP scope includes oversight and coaching of others performing third-party security risk assessments
52	**Environment & Technology** To understand the complexity of the environment can you confirm if CalHEERS hosted entirely in the cloud, on-premises, or in a hybrid environment?	CalHEERS is hosted entirely in the cloud

Questions about the RFP

#	Proposer Questions:	Covered California's Responses:
53	**Qualifications and Responsiveness** Section 2.1.1 excludes contractors that have provided information technology services for CalHEERS or Covered California from July 1, 2024 to the present. Does this exclusion apply to the prime contractor only, or does it also extend to named subcontractors?	This exclusion extends to named subcontractors.
54	**Qualifications and Responsiveness** Section 4.3.4 requests narratives for up to five projects completed in the past two years. For multi-year engagements that are currently active and began within the past two years, may these be included as past projects, or must the project be completed?	Narratives from currently active engagements will be accepted
55	**Qualifications and Responsiveness** Section 4.3.3 limits the Project Team Qualifications narrative to five pages. Are resumes included in or excluded from the five-page limit?	Exhibit C, Attachment 1 - Resumes are excluded from the five-page limit.
56	**Preference Programs** Section 6.3 references the Disabled Veteran Business Enterprise (DVBE) incentive available to proposers with DVBE subcontractor participation. Must the DVBE subcontractor hold California DGS OSDS DVBE certification specifically, or is federal	Vendors must hold the California DGS OSDS DVBE certification specifically.

#	Proposer Questions:	Covered California's Responses:
	Service-Disabled Veteran-Owned Small Business (SDVOSB) certification accepted?	
57	Is there a preference for local vendors?	Remote vendors are considered, but monthly travel to Sacramento will be required for full-time staff.
58	**RFP Section 2.1 Project Team Minimum Qualifications** Would this work preclude us from future CalHEERS IT services contracts after the Information Security Services contract ends?	We cannot speak to future RFPs and decisions made by other Programs.
59	**RFP Section 2.1 Project Team Minimum Qualifications** Please clarify the minimum organizational-independence requirements between the operational security support team and the independent assessor team. Specifically, will separate engagement leadership, personnel, workpapers, quality review, and reporting/escalation paths within the same contractor organization satisfy the requirement, or must the assessor team reside in a separate legal entity, business unit, service line, or subcontractor organization? Please also confirm whether personnel who design, implement, administer, or operate an in-scope control are prohibited from assessing that control and whether any look-back or cooling-off period applies.	Covered California does not require the independent assessor team to reside in a separate legal entity. Separate organizational reporting structures within the same contractor organization may satisfy the requirement, provided the assessor team is organizationally and operationally independent from the operational support team. The assessor team may not assess controls for which its personnel had direct design, implementation, administration, or operational responsibility. No separate look-back or cooling-off period applies unless otherwise required by applicable standards or a future contract amendment.
60	**2.2 Technical Minimum Qualifications** Under Covered California, how many applications are in-scope for the review? Can Covered California provide additional details for each application such as size (number of pages), custom/vs. COTS, number of user/roles, and on premises/SaaS?	Annual independent assessment includes one-third of the 472 ARC-AMPE controls. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
61	**RFP 2026-01 Purpose Statement** For us to accurately estimate the scope of work for the in-scope services (Risk Management, Compliance, Security Architecture, Incident Response, TPRM, Threat Monitoring, Data Protection, and Independent Assessment Services) can	At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors. Current technologies include: • Optro - GRC • Splunk - SIEM

#	Proposer Questions:	Covered California's Responses:
	Covered California provide historical data such as number of FTEs required, or special consideration in these categories that would help us estimate the scope of work?	• CrowdStrike - endpoint security • DLP – Microsoft Purview • Tenable – Vulnerability management • NuHarbor – MSSP There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
62	Would Covered California consider extending the proposal submission deadline by two (2) weeks? Given the breadth of the required services—including operational security support, independent assessments, penetration testing, digital forensics, specialized staffing, and the proposal documentation requirements—additional time would allow proposers to finalize key personnel commitments, incorporate Covered California's responses to proposer questions, and submit more comprehensive and competitive proposals. We believe this would maximize competition and enable Covered California to evaluate the strongest possible responses.	No, the timeline cannot be extended by 2 weeks.
63	**SUBMISSION MECHANICS** Section 4.3.4 requests up to five projects "completed in the past two years." Do ongoing or multi-year engagements that are active within that window qualify, or must the engagement have concluded within the past two years?	Narratives from currently active engagements would be accepted
64	**SUBMISSION MECHANICS** Do the required "table showing hours per week by person" (Section 4.3.1) and the team resumes (Exhibit C, Attachment 1) count against the applicable five-page narrative limits, or are they excluded?	No, the table and resumes are not counted in the five pages.
65	**SUBMISSION MECHANICS** Section 2.1(4) requires background clearance before accessing confidential information. Must clearances be completed before contract execution and performance start, or can they be initiated after award?	Background checks will be initiated after award.

#	Proposer Questions:	Covered California's Responses:
66	**Contract & Commercial** The RFP indicates proposals must be submitted via email to HBEXSolicitation@covered.ca.gov. What is the maximum email attachment file size limit permitted by Covered California's mail server, and are multi-part email submissions allowed if total attachment size exceeds file boundaries?	Per the RFP Section 1.9 Format of Proposal Proposers must submit a proposal package that contains all required attachments, documents, narrative responses, and Model Contract exhibits. Proposals must be submitted electronically via email to HBEXSolicitation@covered.ca.gov with "RFP 2026-01" in the subject line. You may submit proposals through multiple emails if necessary.
67	**Contract & Commercial** Paragraph 1.9 or Section 1.10 specifies page limits for narrative sub-sections. Do these page limits apply strictly to core narrative text, or do they include cover pages, table of contents, divider pages, resumes, and official attachments?	Applies to core text.
68	**Contract & Commercial** Will Covered California issue formal written addendums for all responses to vendor questions submitted by August 05, 2026, at 12:00 PM PST, and is there a specific addendum acknowledgement sheet required in the proposal package?	Yes. Covered California will issue formal written addenda, as necessary, in response to vendor questions submitted by the deadline. All prospective bidders are responsible for monitoring the solicitation website for any addenda issued. https://hbex.coveredca.com/solicitations/#RFP-2026-01
69	**Contract & Commercial** Will Covered California allow the selected vendor to provide standard certificates of liability insurance upon bid submission and finalize custom state-specific additional insured endorsements during final contract execution prior to December 1, 2026?	Per the RFP section 4.2.2 Required Documents - Proposals must include all required insurance documents. If the Proposer cannot include required insurance with its proposal, a written explanation detailing why it cannot comply with the requirements. https://hbex.coveredca.com/solicitations/#RFP-2026-01
70	**Contract & Commercial** What is the anticipated timeline for state approval of criminal background checks under California Government Code Section 1043 and 10 CCR 6456, and may personnel	Please see responses to Question #82.

#	Proposer Questions:	Covered California's Responses:
	begin onboarding conditionally while background clearance is pending?	
71	We kindly request a 1-2 week extension of the proposal submission deadline to ensure a thorough and high-quality response.	Per the RFP Section 1.2 Key Action date proposal is due by August 31st, 2026 by noon. Should the date be extended, an addendum will be issued and announcement will be made. https://hbex.coveredca.com/solicitations/#RFP-2026-01
72	**Scope of Work and Environment** Section 3.3 refers to Model Contract Exhibit A – Scope of Work for the detailed description of services. Can Covered California confirm that all Model Contract exhibits, attachments, and forms referenced in the RFP are available for download from the solicitation website at hbex.coveredca.com/solicitations? If any are not yet posted, when will they be made available?	All Model Contract Exhibits, Attachments, and Forms are available for download on the solicitation website at https://hbex.coveredca.com/solicitations/#RFP-2026-01
73	**Contract & Commercial** Are external auxiliary attachments—such as sample executive dashboards, weekly reporting templates, audit methodology matrices, threat modeling frameworks, cloud architecture diagrams, and standalone technical vendor capability sheets—permitted as separate supplemental appendices without counting toward narrative page limits?	Yes, permitted as a separate supplemental document and excluded in counting towards narrative page limits.
74	May a Proposer satisfy the minimum corporate and personnel qualifications through the combined experience of the Proposer and its identified subcontractors?	Yes
75	For the past-project requirement, may completed task orders, assessments, audits, or formally accepted project phases performed under an ongoing contract qualify as projects completed within the past two years?	Yes
76	If the Proposer does not intend to use or provide generative artificial intelligence in performing the contract, which portions of Attachment 7, HBEX 707, must be completed?	Attachment 7 - HBEX 707 Generative Artificial Intelligence Risk Assessment must be submitted even if the proposer does not intend to use or provide generative artificial intelligence in performing the contract.

#	Proposer Questions:	Covered California's Responses:
		Per the RFP section 4.2.4 Failure to submit the Generative Artificial Intelligence Risk Assessment (HBEX 707) will result in disqualification of the Proposer. https://hbex.coveredca.com/solicitations/#RFP-2026-01
77	Please confirm the preferred electronic file-naming convention, maximum email attachment size, and procedure for submitting the proposal through multiple emails if necessary.	Per the RFP Section 1.9 Format of Proposal Proposers must submit a proposal package that contains all required attachments, documents, narrative responses, and Model Contract exhibits. Proposals must be submitted electronically via email to HBEXSolicitation@covered.ca.gov with "RFP 2026-01" in the subject line. You may submit proposals through multiple emails if necessary.
78	Section 2.1, item 1 (p. 15) We completed strategy work for Covered California that concluded in late 2024. Does this strategy work preclude us from responding to this RFP?	Yes, it does if security was included in the strategy.
79	Section 2.1, item 1 (p. 15) Would Covered California consider shortening the IT work preclusion to 1 year, from July 1, 2025?	No
80	**ELIGIBILITY & INDEPENDENCE** Section 2.1(1) excludes contractors that provided "information technology services" for CalHEERS or Covered California from July 1, 2024 to present. Does this exclusion extend to a Proposer's parent company, affiliates, or proposed subcontractors? Does it include security advisory or assessment services, or only implementation/operational IT services?	This exclusion extends to a Proposer's parent company, affiliates, or proposed subcontractors
81	**ELIGIBILITY & INDEPENDENCE** Sections 2.1(12) and 3.2 require the independent assessor team to operate under a reporting structure separate from operations staff. Can a single Proposer provide both the operational security	A company organization chart must be provided as evidence of separation.

#	Proposer Questions:	Covered California's Responses:
	support and the independent assessor functions under one award? If so, what documentation will Covered California require to demonstrate that the separation satisfies ARC-AMPE and Government Code Section 11549.3 independence requirements?	

Questions about Staffing and Background Checks

#	Proposer Questions:	Covered California's Responses:
82	**Background-Clearance Timing** Exhibit A requires all personnel to comply with the criminal-background-check requirements of Government Code Section 1043 before accessing confidential information, at the Contractor's expense. Given the anticipated December 1, 2026 contract start date, when may clearance processing begin relative to contract execution, and what processing timeframe should Proposers assume?	Pursuant to Exhibit A, background check clearance must be completed prior to the commencement of work under this contract. The estimated processing time for background check clearance is approximately two weeks, but may take longer depending on DOJ/FBI processing and circumstances of the check.
83	May personnel performing annual assessments, penetration testing, digital forensics, and other specialized services be provided on a project or surge basis outside the three-to-four-person full-time staffing complement?	Yes
84	**STAFFING & LEVEL OF EFFORT** Section 2.1(2) requires "three full-time security professionals, including one designated manager." Is the manager counted within the three, or in addition to them? Do these three cover operational support only, with the independent assessor team (Section 2.1.12) staffed separately and additionally?	One of the full-time employees will act as the manager for the other full-time operational staff.
85	**STAFFING & LEVEL OF EFFORT** For cost-estimating purposes, can Covered California provide an expected annual level of effort (e.g., estimated hours) for (a) the core full-time operational team, (b) surge or project-based work, and (c) the independent assessment and penetration testing scope?	Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700
86	Can Covered California provide staffing/workload assumptions to support resource planning?	At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors.
87	What is the expected effort split across security operations, GRC, assessments, penetration testing, and incident response activities?	Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200

#	Proposer Questions:	Covered California's Responses:
		Full-Time staff 6,000 **Total** 8,700
88	Does the requirement for three full-time security professionals refer to the core embedded team, with services such as independent assessments, penetration testing, digital forensics, remediation support, and other surge activities staffed separately?	Three full-time refers to the operational staff. Independent assessors, penetration testing, digital forensics, and project-based staff are separate.
89	Please confirm whether the three full-time security professionals required by Section 2.1.2 represent a minimum staffing and coverage requirement, and whether Proposers may propose alternative staffing and delivery configurations, provided all service coverage, personnel qualification, independence, responsiveness, and service-quality requirements are satisfied.	Three full-time represents minimum staffing.
90	To support comparable staffing and cost proposals, please provide the anticipated annual workload ranges or planning assumptions for the major service areas in Exhibit A, including recurring operational activities, planned projects, independent assessments, penetration tests, forensic matters, incident-response activations, and surge requests.	Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700
91	**Staffing** The Scope of Work specifies three to four full-time security professionals. Does this include the Project Manager, or is the manager in addition to these resources?	A Project Manager is not in scope for this RFP. One of the full-time resources must act as a manager for the additional full-time resources.
92	**Staffing** What are the expectations for after-hours and on-call support?	After-hours support is needed when working on a tight compliance deadline or if needed to support a major security incident.
93	**Staffing** Which specific roles within the proposed 3 to 4 full-time security staff will be designated as filing positions under Covered California's Conflict of Interest Code requiring electronic Form 700 completion?	These contractor positions are not required to file a form 700.
94	**Staffing** Are there any citizenship requirements & security clearance certifications required for full-time security staff?	Covered California's criminal background check

#	Proposer Questions:	Covered California's Responses:
95	**Contract & Commercial** Are labor categories fixed or may vendors propose alternative staffing models? Based on the scope, we anticipate more than 4 resources are required to cover all the functions. Can we have more than 4 resources which will be within the budget limit?	More than 4 resources, all within budget limits, are permitted.
96	**Contract & Commercial** Are option years expected to have the same staffing levels as the base contract?	Yes
97	**Scope of Work and Environment** Section 2.1.2 requires a team of three full-time security professionals, including one designated manager. For purposes of staffing the proposal, does 'full-time' mean 40 hours per week dedicated exclusively to this contract, or does Covered California define the term differently?	'Full-time' means 40 hours per week dedicated exclusively to this contract
98	**Scope of Work and Environment** Section 3.2 references the need for independent security and privacy assessments using ARC-AMPE and NIST SP 800-53 Revision 5, and that the independent assessor must maintain separate organizational reporting structures from operational staff. May the Proposer satisfy this requirement by using a qualified subcontractor for the independent assessment function while performing operational security services with its own staff?	Yes
99	The RFP states that the Contractor must provide a team of three full-time security professionals and Exhibit A references with three to four full-time security professionals. Can Covered California confirm the minimum staffing model and whether four full-time resources would be evaluated more favorably than three?	Three full-time security professionals represent a minimum staffing and coverage requirement. At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors.
100	**RFP 2026-01 Section 2.1 Project Team Minimum Qualifications** Is the project manager's role expected to be a full-time resource? Is the project manager's role one of the three required security professionals?	Section 2.1 refers to a staff manager, not a project manager. Yes, one of the full-time roles will act as the manager for the additional operational contractors assigned to Covered California.

#	Proposer Questions:	Covered California's Responses:
101	Section 2.1(2) requires a team of three full-time security professionals, while Exhibit A Section D.2 requires three to four. Please confirm the number of full-time staff to be proposed.	The proposal should include at least three full-time.
102	Should the independent assessor personnel be included within the three to four full-time staff, or proposed as additional resources beyond that team?	The independent assessor personnel should not be included in the full-time operational personnel.
103	**Exhibit A – Scope of Work, section D. General Scope or Tasks** Can Covered California provide estimated annual volumes for each of the services that Covered California is requesting? This information would support more accurate staffing and pricing assumptions.	Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700
104	**Security Incident Response** Are forensic investigations included within the base scope which will be performed by one of the 4 full-time security staff? Or can it be added as a need basis which could be charged on hourly basis within the budget limit?	The individuals used for forensic investigations will be engaged on an as-needed hourly basis.
105	RFP Section 2.1.2 requires a team of three full-time security professionals, while Exhibit A, Section D.2 requires three to four full-time security professionals. Please confirm the mandatory minimum number of full-time personnel that must be proposed, staffed, and priced during each contract year. Is the fourth full-time professional mandatory, optional, or activated only when requested?	Propose at least three full-time contracted staff.
106	**Contract & Commercial** If Covered California exercises its right to adjust contract scope under the Qualified Health Plan Assessment Contingency Clause, what notice period will be provided to the contractor to adjust staffing allocations without penalty?	Not applicable to this RFP.
107	Exhibit A requires three to four full-time security professionals, while Exhibit B, Attachment 1 states that estimated annual hours will not exceed 2,000 for all personnel. Is the 2,000-hour limitation intended to apply	The 2,000 hours is an estimate for each full-time contracted staff.

#	Proposer Questions:	Covered California's Responses:
	per full-time position, per labor category, or collectively to all personnel?	
108	**Number of Full-Time Positions to Price** Section 2.1.2 requires a team of three full-time security professionals, including one designated manager, while Exhibit A requires three to four full-time security professionals. Please confirm the number of full-time positions Proposers should include in the Cost Worksheet.	The proposal shall include at least three full-time security professionals, with one serving as management oversight for the other contracted staff.
109	Please clarify the minimum organizational-separation requirements between personnel providing operational security support and personnel performing independent security and privacy assessments, penetration testing, or related independent-assessor services. Are separate reporting lines within the same prime contractor sufficient, and may the teams share corporate quality, administrative, technology, or subcontractor resources?	Yes, separate reporting lines within the same prime contractor are sufficient and the teams may share corporate quality, administrative, technology, or subcontractor resources. The operational staff leadership may not have influence over the independent assessment area of the organization, and vice versa.
110	What level of organizational separation is required for the independent assessor team? May a subcontractor perform this function under a separate reporting structure with direct access to Covered California?	Yes, a subcontractor is allowed with the understanding that the proposer is responsible for the work performed by the subcontractor.
111	**Exhibit A – Scope of Work** In addition to the requirements of having 3-4 dedicated FTE's, how many additional FTE's were required to perform the scope of work in the previous year?	At peak, information security contractors have included 4 full-time, 4 project-based, and 3 independent assessors. Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700

Questions about Exhibit A, Scope of Work, and Expectations for the Contractor

#	Proposer Questions:	Covered California's Responses:
112	Exhibit A – Scope of Work What is the frequency of the penetration testing?	Once a year.
113	Exhibit A – Scope of Work Can more information be shared about the scope of the penetration testing, e.g., how many end points, websites, etc.	Annual independent assessment includes one-third of the 472 ARC-AMPE controls. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
114	Please provide the anticipated annual volume of security assessments, penetration tests, and compliance reviews.	The independent assessment and penetration test are an annual event. SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
115	**Penetration Testing** How many internal and external penetration tests are expected annually?	Once a year.
116	**Penetration Testing** Which environments are included (production, test, development)?	Primarily production.
117	**Penetration Testing** For the annual independent assessment and penetration testing deliverables, what is the precise scope of targets, including IP address ranges, web applications, APIs, and mobile endpoints requiring internal and external penetration testing? • Total No of External IPs in scope for testing: • Total No of Internal Assets in scope for testing: • Total No of Web Applications in scope for testing: • Total No of Apis in scope for testing:	There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.

#	Proposer Questions:	Covered California's Responses:
	Total No of Mobile Apps in scope for testing:	
118	**Penetration Testing** Are web applications, APIs, cloud infrastructure, wireless networks, and mobile applications included?	Wireless networks and mobile applications are not included
119	**Penetration Testing** Are social engineering or phishing assessments required?	No
120	**Penetration Testing** Are authenticated vulnerability assessments expected as part of penetration testing?	No
121	**Penetration Testing** Is remediation validation and retesting included within the engagement?	Yes
122	**Penetration Testing** What are the authorized time windows for active vulnerability scanning and penetration testing, and what are Covered California's operational escalation procedures for critical vulnerabilities identified during active testing?	Vulnerability scans are not in-scope. Penetration testing can be performed at any time low and slow.
123	**Penetration Testing** To ensure compliance with CMS ARC-AMPE requirements, can Covered California confirm that the independent assessment team performing penetration testing and compliance audits may share corporate overhead resources while maintaining distinct project management and reporting structures from the operational security staffing team?	Confirmed, the reporting structure must be separate.
124	**Exhibit A – Scope of Work, Section Penetration Testing, section 2.1 Project Team Minimum Qualifications** How many penetration testing engagements are anticipated annually, and what is the approximate scope of each engagement (external, internal, application, cloud, API, red team, etc.)?	Once a year. Includes external, internal, and cloud. Web application testing may be requested under the project-based billing. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
125	**Penetration Testing Services** What is the anticipated annual scope for penetration testing activities (applications,	There are approximately 80 IP addresses and 20 applications included in the annual

#	Proposer Questions:	Covered California's Responses:
	infrastructure, cloud environments, APIs, CalHEERS components, etc.)? Please provide an estimated number of assets by category (e.g., # of EC2 instances, # of servers, # of databases etc.)	independent assessment and penetration test.
126	Does the assessment and penetration testing scope extend to components operated by the Department of Health Care Services or a system integrator, or stop at the Covered California perimeter?	Department of Health Care Services is not in-scope, but the CalHEERS environment managed by the system integrator is. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
127	What is the penetration test scope type (external, internal, web application, API, social engineering, wireless) and approximate target count per annual cycle?	Once a year. Includes external, internal, and cloud. Web application testing may be requested under the project-based billing. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
128	What level of effort was expended on the most recent annual independent assessment and penetration test?	Below is an annual estimate of hours based on historical data: Assessment/Pentest 1,500 Project based work 1,200 Full-Time staff 6,000 **Total** 8,700
129	To ensure compliance with CMS requirements may we get more information on Penetration Test cadence, scope size, or environment counts?	Once a year. Includes external, internal, and cloud. Web application testing may be requested under the project-based billing. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
130	Exhibit A – Scope of Work What is the frequency of conducting the risk assessment?	Independent assessments are required annually.
131	Is the contractor expected to provide advisory services only, or also hands-on implementation and operational support?	Advisory services, hands-on administration of security technologies, and operational support.

#	Proposer Questions:	Covered California's Responses:
132	What level of after-hours monitoring and incident response coverage is expected beyond Covered California's core business hours? Are there defined notification, response, and escalation service levels?	The contracted staff will not participate in after-hours monitoring. After-hours support is needed when working on a tight compliance deadline or if needed to support a major security incident.
133	Please clarify incident response expectations, including after-hours support, response SLAs, and any 24x7 coverage requirements.	The full-time staff may be called outside of normal business hours to assist the security team with a major security incident.
134	**Security Incident Response** Will the contractor be expected to provide incident response outside normal business hours?	The full-time staff may be called outside of normal business hours to assist the security team with a major security incident.
135	**Linux & Application Support** To what extent is the selected provider expected to provide hands-on administration, patching, troubleshooting, and support for Ubuntu Linux servers, PostgreSQL/MySQL databases, Ruby on Rails applications, and the Grants Management System environment? Are any of these systems supported by separate application owners, developers, or third-party vendors?	There is no expectation to provide hands-on administration of the listed technologies.
136	**Public Website & Grants Management System Support** Does support for the public website and Grants Management System include application-level troubleshooting, code-level support, database administration, deployments, and performance optimization, or is support limited to the underlying infrastructure and hosting environments?	This question is not applicable to this RFP
137	**Policy Development & Governance** To what extent is the selected provider expected to develop, maintain, and enforce information security, data classification, retention, and access governance policies, versus providing advisory support to Covered California stakeholders?	The operational contractor staff will be involved in all services listed.
138	**Compliance Program Ownership** Will Covered California maintain internal resources responsible for governance, risk, and compliance activities, or is the selected provider expected to serve as the primary	The Covered California CISO will remain accountable for security work performed and will serve as the primary owner and operational resource.

#	Proposer Questions:	Covered California's Responses:
	operational resource supporting ongoing compliance, audit readiness, and regulatory requirements?	
139	**Scope Boundaries** Please clarify whether the selected provider is expected to serve as the primary owner and operator of end-user support, server infrastructure, application support, security operations, compliance activities, disaster recovery planning, vendor management, and onsite support functions, or if any of these responsibilities will remain with internal staff or existing service providers.	The Covered California CISO will remain accountable for security work performed and will serve as the primary owner.
140	Does Covered California expect all service areas identified in Exhibit A to be continuously supported throughout the contract term, or will activities be authorized and prioritized through annual work plans, task authorizations, or another governance process? Please describe the anticipated process for assigning, sequencing, approving, and modifying work	Project-based work will be based on annual work plans and risk mitigation work.
141	**Threat Detection & Security Operations** Is the contractor expected to perform continuous monitoring or provide advisory support only?	Advisory support.
142	**Digital Forensics** Are forensic services expected to include legal testimony or expert witness support?	There is a potential need to provide testimony.
143	**Contract & Commercial** How will surge support or additional project work be authorized?	Authorized by the CISO.
144	Does the scope include onboarding and inherent risk assessment of new vendors, or only ongoing reviews?	The scope includes oversight and coaching of others performing third-party security risk assessments.
145	Is remediation management (tracking, validation, reporting and closure of findings) included, or is the role limited to assessment and risk reporting?	The full-time operational staff will be involved in remediation management.
146	Is continuous monitoring or breach notification included? If so, what capabilities and data sources are in use?	No
147	What service level expectations apply to assessment completion, remediation follow-up, and risk escalation?	Independent assessments must follow a strict CMS timeline. Operational staff will work closely with the CISO on remediation

#	Proposer Questions:	Covered California's Responses:
148	Cyber resiliency was not specifically called out in the RFP. Is this something they would like to include as part of the scope?	A separate call-out for cyber resiliency is not needed.
149	**General Scope** Is the intent to augment the existing security team or to outsource specific security functions?	Augment existing security resources
150	**General Scope** Are there any anticipated organizational or technology changes that may affect the scope during the contract term?	Not that we are aware of. There is always potential for technologies to shift within the Covered California and CalHEERS environments.
151	**Environment & Technology** What cloud platforms and SaaS applications are in scope?	Covered California operates a cloud-first, hybrid, multi-cloud environment using multiple commercial cloud providers, hosted SaaS applications, and limited residual on-premises infrastructure. To reduce security risk, Covered California does not disclose provider names, workload percentages, or detailed account, network, location, or configuration information. For planning purposes, prospective vendors should assume a predominantly cloud-hosted environment, distributed across multiple cloud and SaaS environments, with a minimal on-premises footprint.
152	**ARC-AMPE Equivalent Experience** ARC-AMPE was published in March 2025 and became mandatory for Administering Entities on March 4, 2026. Section 2.1.12 requires demonstrated experience conducting independent assessments using ARC-AMPE or NIST SP 800-53 Revision 5. Will Covered California accept demonstrated assessment experience under MARS-E Version 2.2, or assessments performed against the NIST SP 800-53 Revision 5 baseline from which ARC-AMPE Volume II is derived, as satisfying this requirement?	Proposers should have experience with ARC-AMPE or NIST SP 800-53 revision 5.
153	**Security Platform Responsibilities** Is the selected provider expected to assume administration and operational responsibility for the existing security platforms (e.g., Darktrace, SentinelOne, SilverSky, Microsoft	The operations staff will provide advisory support and some hands-on support for security technologies.

#	Proposer Questions:	Covered California's Responses:
	Defender, Carbon Black, KnowBe4, OneLogin, Keeper), or may proposers recommend alternative technologies as part of their solution?	
154	**Master Services Agreement** Is the awarded provider required to contract exclusively under Covered California's agreement and standard terms, or is Covered California willing to negotiate from a provider's standard managed services agreement and scope of work?	The contractor can propose edits to the Covered California agreement that may be taken into consideration.
155	Which compliance areas are they most concerned about or feel may warrant special attention?	All ARC-AMPE/NIST SP 800-53 rev 5 control families.
156	Have they performed an assessment leveraging ISO 27701 or the NIST Privacy Framework? Is this something they would like to include as part of the scope?	No, they are not part of the scope.
157	Have they performed an assessment of the AI security risks leveraging a standard such as the NIST AI Risk Management Framework? Is this something they would like to include as part of the scope?	Covered California and CalHEERS have an AI security risk management process.
158	**Governance, Risk & Compliance** What compliance assessments (ISO, SOC2 etc.) are planned during the contract period?	ARC-AMPE
159	**Governance, Risk & Compliance** How many security policies and standards are expected to be created or updated annually?	At least 20
160	**Governance, Risk & Compliance** Are there established governance committees that the contractor will participate in?	Yes, for both the CalHEERS and Covered California environments.
161	**Security Engineering** Approximately how many security architecture reviews are expected annually?	At least 40.
162	**Security Engineering** Will the contractor participate in application design reviews and cloud architecture reviews?	Yes
163	**Security Engineering** Are there any planned cloud migrations or modernization initiatives?	Migrations are completed, but there are ongoing modernization initiatives that will require a security review.

#	Proposer Questions:	Covered California's Responses:
164	**Third-Party Risk Management** Will the contractor participate in contract security reviews?	No, contracts are handled by state staff.
165	**Third-Party Risk Management** How many assessments are required each year?	SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
166	**Third-Party Risk Management** What is the compliance framework that they want contractor to align with?	Assessments are based on a tailored process developed by a contracted vendor. SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
167	**Threat Detection & Security Operations** Will the contractor develop new log collectors, create new threat detection rules and use cases?	Covered California is contracted with an MSSP that is responsible for log collections. The contractor's role will be to ensure appropriate system logs are captured and compliant.
168	**Independent Security Assessment** How many systems are included in the annual independent assessment?	Annual independent assessment includes one-third of the 472 ARC-AMPE controls. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test.
169	**Independent Security Assessment** Is the assessment limited to CalHEERS or does it include additional Covered California systems?	Additional Covered California systems are included in the independent assessment.
170	**Independent Security Assessment** Are privacy assessments required in addition to security assessments?	The scope of the ARC-AMPE independent assessment includes privacy controls.
171	**Digital Forensics** Approximately how many forensic investigations are performed/expected annually?	We don't expect more than 5 investigations annually.

#	Proposer Questions:	Covered California's Responses:
172	**Exhibit A – Scope of Work, Section Digital Forensics.** Can Covered California provide estimated annual volumes for workstation forensic investigations and whether any SLAs exist for evidence collection and case response?	We don't expect more than 5 investigations annually.
173	**Exhibit A – Scope of Work, Section D. Third-Party Risk Management (TPRM)** Can Covered California provide the estimated annual volume of third parties that will require security assessments, due diligence reviews, contract/control reviews, and ongoing monitoring under the Third-Party Risk Management (TPRM) program? Additionally, can Covered California provide the approximate breakdown of vendors by risk tier (e.g., high, medium, low) and identify whether assessments are expected for new vendors only or both new and existing vendors on a recurring basis?	SecurityScorecard, used for conducting third-party security risk assessments, will remain. The RFP scope includes oversight and coaching of others performing third-party security risk assessments.
174	**Exhibit A – Scope of Work – Independent Assessor Services** For ARC-AMPE compliance assessments, does year 1 include full ARC-AMPE controls or only 1/3rd control assessment?	Annual independent assessment includes one-third of the 472 ARC-AMPE controls. There are approximately 80 IP addresses and 20 applications included in the annual independent assessment and penetration test. .
175	**Security Incident Response** What are the expected responsibilities of the contractor during security incidents, including investigation, containment, forensic analysis, communications, and after-action reporting?	Contractor's responsibilities are limited to oversight and advisory roles.
176	Exhibit A Section D.2 assigns security policy development, architecture, control implementation and GRC administration to the Contractor. Section D.3 requires the Contractor to perform the independent annual assessment of the same environments. Does the assessment scope include controls that the Contractor's own operational team designed or implemented?	Yes, that is why the independent assessor staff must have separate reporting lines within the contractor's organization to qualify as independent assessors.
177	For controls the Contractor implemented, may the assessor rely on the operational team's testing, or must it test independently?	The operational team will participate in internal assessments, however independent assessments will require independent testing.

#	Proposer Questions:	Covered California's Responses:
178	Are any in-scope environments authorized under the Federal Risk and Authorization Management Program (FedRAMP) such that control inheritance may be applied? If so, will inheritance documentation be made available?	Yes, the majority of the cloud platforms are FedRAMP authorized. Inheritance documentation may be available from the manufacturer.

Question about Cost Worksheet, Invoicing, and Payment

#	Proposer Questions:	Covered California's Responses:
179	Should the Cost Worksheet include every proposed labor category and estimated annual hours? May the estimated hours vary by contract year?	Yes and yes, if that is what proposers choose to include in the bid.
180	**COST PROPOSAL** Section 1.5 caps base-term costs at $12,500,000 and total-with-options at $17,500,000. Should the Cost Proposal (Attachment 1 / Exhibit B) reflect only the five-year base term, or include the two optional years?	The two optional years should be included.
181	**COST PROPOSAL** Section 3.6 states the Contractor may invoice only after acceptance of deliverables, while Sections 2.5 and 4.3.1 reference hourly rates and hours per week. Should the Cost Worksheet be structured as fully loaded hourly rates, fixed deliverable-based pricing, or a hybrid? Clarification of the intended pricing model would help ensure comparable submissions.	The expectation is an hourly rate for full-time and project-based work. The acceptance of contract deliverables stated in Section 3.6 does not apply to full-time operational contractor staff.
182	What pricing model is preferred for operational support services (resource-based, managed services, or milestone-based)?	The expectation is an hourly rate for full-time and project-based work.
183	Are annual rate escalations permitted during the base and optional contract terms?	Rate escalations are permitted in the option years not to exceed the total contract amount of $17,500,000.
184	Please clarify whether the approximately $2.5 million per year referenced in Section 1.5 is an anticipated annual expenditure, a maximum annual authorization, or a planning estimate within the $12.5 million five-year ceiling. May expenditures vary between contract years while remaining within the five-year maximum, and may unused base-term funding be applied to later-year projects or surge requirements?	The $2.5 million is an estimated maximum annual authorization. Any unused funding may be applied to later-year projects with CISO, finance, and board approval.
185	**Cost and Contract** Section 1.5 states that proposals shall not exceed $12,500,000 for the base term.	Authorized travel expenses shall be reimbursed in accordance with Exhibit E – Travel Reimbursement.

#	Proposer Questions:	Covered California's Responses:
	Does this cap include or exclude reimbursable travel expenses under Exhibit E – Travel Reimbursement?	Yes, the cap includes travel.
186	**Contract & Commercial** Are travel expenses reimbursable for work outside the Sacramento headquarters?	Authorized travel expenses shall be reimbursed in accordance with Exhibit E – Travel Reimbursement. Only pre-approved travel expenses to Sacramento and San Diego offices will be reimbursed.
187	**Cost and Contract** Section 3.6 states the Contractor may invoice only after successful completion and acceptance of deliverables. For ongoing services such as operational security monitoring and GRC support, are these invoiced monthly as recurring deliverables, or on a different basis?	The acceptance of contract deliverables stated in Section 3.6 does not apply to full-time operational vendor staff.
188	What is the annual budget allocated for this RFP?	Please see RFP Section 1.5 Contract Amount for the proposed cost of this of this contract. https://hbex.coveredca.com/solicitations/#RFP-2026-01
189	What is the total budget for this contract?	Please see RFP Section 1.5 Contract Amount for the proposed cost of this of this contract. https://hbex.coveredca.com/solicitations/#RFP-2026-01
190	The Cost Worksheet (Exhibit B, Attachment 1) estimates hours per year will not exceed 2,000 "for all personnel." Is that 2,000 hours per personnel title, or 2,000 total across the team?	The 2,000 hours is an estimate for the full-time individuals.
191	Section 3.6 states that invoices may be submitted only after successful completion and acceptance of contract deliverables. Given that the Scope of Work includes ongoing operational support through dedicated full-time personnel, can Covered California clarify what constitutes an invoiceable deliverable for recurring operational services? For example, should proposers assume that recurring operational support will be invoiced on a monthly basis following acceptance of	The acceptance of contract deliverables stated in Section 3.6 does not apply to full-time operational contractor staff.

#	Proposer Questions:	Covered California's Responses:
	monthly services, while project-specific activities (e.g., independent assessments, penetration testing, digital forensics) will be invoiced upon completion of their respective deliverables?	
192	**Rate Structure Across Contract Years** The Cost Worksheet provides a single hourly-rate column for the five-year base term, and Exhibit A states that funding for any contract extension will use the rates provided in the Contractor's proposal. May Proposers submit year-specific hourly rates, including escalation, by adding columns or rows to the Cost Worksheet? Additionally, should the rates proposed for Year 5 apply to option years six and seven?	Yes, proposers should modify the Cost Worksheet as applicable to reflect your proposed rates for the bid.

Questions about Remote Work and Resources

#	Proposer Questions:	Covered California's Responses:
193	Are the three to four full-time professionals expected to perform on-site in Sacramento five days per week, or may Covered California authorize hybrid or remote performance for designated roles and activities?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
194	**SCOPE & ENVIRONMENT** Section 3.5(1) references key staff working on-site during business hours, and Exhibit E addresses travel reimbursement. Is the work expected to be on-site, hybrid, or remote, and what is the primary work location for staffing and travel-cost purposes?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
195	Are remote, hybrid, and offshore delivery models acceptable? Are any roles required to be U.S.-based?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
196	Please clarify the location and coverage requirements for the core project team, including required on-site frequency, whether hybrid or remote performance is permitted, any California or United States location requirements, and the required availability and response expectations for on-call support outside Covered California's normal 8:00 a.m. to 5:00 p.m. Pacific Time business hours.	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month. Availability outside of business hours must be occasional and only necessary to meet a compliance deadline or respond to an incident.
197	**Staffing** What percentage of work is expected to be performed onsite versus remotely?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
198	**Scope of Work and Environment** Section 2.1.3 states the Contractor's team must function as an extension of Covered California's Information Security Office (ISO), including maintaining coverage during core business hours. Is Covered California's primary work location Sacramento, and are	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.

#	Proposer Questions:	Covered California's Responses:
	the three required full-time security professionals expected to work on-site, remotely, or in a hybrid arrangement?	
199	Work will be onsite or remote?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
200	Can Covered California clarify which services may be performed remotely versus onsite?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
201	**Staffing Location Requirements** Are any services required to be performed onsite in California, and are there restrictions or preferences regarding remote, offshore, or hybrid delivery models?	Offshore work is not allowed for this engagement. All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
202	Is remote work allowed?	All work is remote within the United States during Pacific Time business hours. Full-time vendor staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
203	Are there restrictions on offshore work?	Offshore work is not allowed for this engagement. All vendor staff must be in the United States.
204	Can vendor provide entire services from offshore location (outside US geography)	Offshore work is not allowed for this engagement. All vendor staff must be in the United States.
205	**Onsite Resource Model** Is Covered California seeking a dedicated resident engineer assigned exclusively to this engagement, or may the onsite requirement be fulfilled through a team-based support model utilizing multiple resources?	Full-time staff are expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
206	Please clarify onsite support expectations, including travel requirements and any mandatory onsite presence.	Full-time staff will be expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.

#	Proposer Questions:	Covered California's Responses:
207	On a percentage basis, how much of the work would they expect to be completed on-site?	Full-time staff will be expected to be at the Covered California Sacramento office for two consecutive days each month. Usually, the first Wednesday and Thursday of the month.
208	**Contract & Commercial** Exhibit A defines a 10-business-day review window for Covered California and a 5-business-day turnaround for vendor revisions. What specific formal acceptance criteria or sign-off workflows are used to confirm deliverable completion prior to monthly invoice processing?	The acceptance of contract deliverables stated in Section 3.6 does not apply to full-time operational contractor staff.