

Blue Lake Rancheria — Consolidated Vendor Questions and Answers

These responses cover the Cybersecurity Plan Update and Penetration Testing Services RFPs. Award-specific FY 2024 THSGP requirements remain pending confirmation.

A. Questions Applicable to Both Engagements

1. NDA and access to confidential information

Question: How can proposers obtain the NDA, and when must it be executed?

Response: The Tribe's standard NDA is available upon request through the designated RFP contact. An executed NDA must be on file before a proposer may receive question responses, updates, or supporting information containing Confidential Information. Proposers without an executed NDA will receive only nonconfidential responses.

An executed NDA is not required to submit a proposal but must be completed before contract award.

2. Insurance requirements

Question: What professional liability and cyber insurance limits apply, and when must coverage be in place?

Response: For the Cybersecurity Plan Update, the contractor must maintain technology professional liability/errors and omissions and cyber liability coverage with limits of at least \$1 million per claim and annual aggregate. For Penetration Testing, the required limits are \$2 million per claim and annual aggregate. Separate policies or a combined technology errors and omissions/cyber liability policy meeting the applicable minimum limits are acceptable.

Coverage must apply to the contracted services and include third-party liability. For penetration testing, coverage must address liability arising from testing-related errors or omissions resulting in system interruption, data loss or corruption, or unauthorized disclosure of confidential information, subject to policy terms reviewed by the Tribe.

Proposers must identify current coverage and any necessary changes in their proposals. Evidence of compliant coverage is required before contract award, and coverage must be maintained throughout the engagement. BLR may request relevant policy provisions and endorsements to verify coverage.

3. Indian/Tribal preference and eligibility

Question: Will Indian/Tribal preference apply, and are non-Tribally owned firms eligible?

Response: Non-Tribally owned firms are eligible to compete for both awards. Indian/Tribal preference will serve as a tiebreaker when proposals receive equal final evaluation scores following the review committee's deliberations. Preference will not add points to a proposal's evaluation score.

Eligible businesses include both Tribally owned businesses and businesses owned by individual enrolled Tribal members. Proposers claiming preference must submit documentation establishing Tribal ownership or the individual owners' Tribal enrollment and ownership interests.

4. Subcontractors and qualifications

Question: May a prime contractor use subcontractors and rely on their experience, references, and certifications?

Response: Yes. Proposers may rely on qualified subcontractors' relevant experience, comparable-project references, and assigned personnel certifications to satisfy qualification requirements.

The proposal must clearly identify each proposed subcontractor, its relationship to the prime contractor, and its assigned scope and responsibilities. Subsequent changes must be disclosed to BLR before the subcontractor performs work.

The prime contractor remains responsible and liable for all subcontractor actions and omissions related to the engagement. Subcontractors and assigned personnel must be bound by the Tribe's NDA before accessing Confidential Information or performing testing.

5. Remote delivery

Question: Can the engagements be performed remotely?

Response: Both engagements may be performed entirely remotely. No onsite visits are required. Remote access and activities must be coordinated with BLR and comply with applicable confidentiality, security, and Rules of Engagement requirements.

6. Data residency and personnel location

Question: Are there restrictions on data storage or personnel location?

Response: All BLR data must remain within the United States, including copies, backups, testing evidence, and reports. All personnel performing work under either engagement, including subcontractors, must be physically located in the United States. Access to BLR data from outside the United States is prohibited.

7. Background checks and collaboration tools

Question: Are background checks or specific collaboration tools required?

Response: Any background-check requirements and approved collaboration tools will be established during contract finalization. All tools and access arrangements must comply with BLR's confidentiality, U.S. data residency, and U.S. personnel-location requirements.

8. Contract documents and certification forms

Question: When will standard contract terms and required federal certification forms be provided?

Response: BLR will provide these materials to the selected vendor during contract finalization. Proposers must still include the disclosures and certifications expressly required by the applicable RFP in their proposal responses.

9. Retention and disposal of confidential information

Question: What requirements apply to confidential materials and testing evidence?

Response: Contractors and subcontractors must return or securely destroy BLR Confidential Information, including testing evidence and retained copies, upon engagement completion or BLR's request. Any required retention exceptions must be identified and addressed in the contract. Retained information remains subject to NDA, U.S. data residency, and access restrictions.

10. Performance end date

Question: Please clarify the end date listed as April 31, 2028.

Response: The correct performance end date for both engagements is **April 30, 2028**. All work, deliverables, and invoicing must be completed within the period of performance.

11. Contract start and milestone timing

Question: What start date should proposers assume, and when do milestone timeframes begin?

Response: The anticipated contract start remains the first quarter of 2027. The exact date will be established during contract finalization. Deliverable timeframes are measured from contract execution and may be adjusted by mutual agreement within the period of performance, as stated in the RFPs.

12. Eligibility for both awards and information separation

Question: May one firm receive both awards?

Response: Yes. The same firm may receive both awards. The contractor must segregate information gathered through the Cybersecurity Plan Update from personnel and activities conducting penetration testing. This requirement also applies to subcontractors. Proposers seeking both awards must explain how they will maintain this separation.

Penetration-testing findings may be shared with the Cybersecurity Plan Update contractor for incorporation into the plan, subject to NDA requirements and availability. This does not permit information gathered through the plan update to be shared with penetration-testing personnel.

B. Cybersecurity Plan Update

13. Organizational scope

Question: Which organizations and business functions must the plan cover?

Response: The plan will primarily cover BLR Tribal government, including Administration, Finance, IT, Education, EPA, Police, OES, and Grants. The scope also includes infrastructure shared with other entities.

Details regarding shared infrastructure, organizational boundaries, specialized environments, and approximate counts of locations, users, endpoints, servers, cloud environments, and critical applications will be provided only to proposers with an executed NDA on file.

14. Current plan and supporting documentation

Question: When was the plan last updated, and what documentation will be available?

Response: The current Cybersecurity Plan was last updated in 2023 using NIST standards.

After executing the NDA, proposers may request the current plan and summary counts of hosts, users, and internal and external IP addresses, as needed to prepare their proposals. Other available supporting materials will be provided to the selected contractor upon contract signing, subject to applicable NDA requirements.

15. Required framework

Question: Which NIST Cybersecurity Framework version should be used?

Response: The updated plan must align with NIST CSF 2.0 and address all six functions: Govern, Identify, Protect, Detect, Respond, and Recover. This clarifies the RFP's reference to five functions.

16. Grant-specific requirements

Question: Are additional THSGP, FEMA, DHS, or CISA requirements, templates, reporting formats, or approval requirements applicable?

Response: These engagements are funded under FY 2025 THSGP award EMW-2025-SS-05194.

Contractors must comply with applicable federal contracting requirements, including suspension and debarment restrictions and restrictions on covered telecommunications and video-surveillance equipment and services. Applicable requirements must also be included in covered subcontracts.

Proposals must include the detailed cost breakdown required by the RFP. Resulting contracts will address required project-record retention and authorized access, applicable federal rights in grant-funded deliverables, funding acknowledgments, and termination provisions.

Contractors must provide documentation supporting their completed work and findings. Submission of BLR's federal grant reports is not part of either engagement.

17. Assessment methods and technical validation

Question: Does the gap analysis require independent technical testing or control validation?

Response: The gap analysis should rely on existing documentation, stakeholder interviews, supplied evidence, and available assessment findings. Independent vulnerability scanning, penetration testing, phishing exercises, hands-on configuration testing, and other technical validation are not required under this engagement. Penetration testing will be conducted under the separate engagement.

Relevant architecture, configuration, and control information may be reviewed as supplied evidence without independently testing implementation.

18. Updating existing content and developing missing content

Question: Is the final deliverable an update, replacement, or new strategic plan?

Response: The contractor must deliver a complete, updated Cybersecurity Plan, retaining useful existing content and developing missing content necessary to meet the agreed scope and NIST CSF 2.0 requirements. The final document will supersede the current Cybersecurity Plan.

19. Incident response, continuity, and recovery plans

Question: Must separate incident response, business continuity, and disaster recovery plans be developed or rewritten?

Response: No. These are separate BLR plans. Drafting or rewriting them is outside scope. The contractor should review available plans for alignment with the updated Cybersecurity Plan and identify gaps or recommended changes in the implementation roadmap.

Developing or updating critical services, recovery priorities, recovery time objectives, or recovery point objectives is not required under this engagement.

20. Third-party providers

Question: Must managed service providers, cloud providers, or other third parties be assessed?

Response: No. Assessment of those third-party providers is outside the scope of the Cybersecurity Plan Update engagement.

21. Maturity assessments and scoring

Question: Is an existing NIST maturity assessment available, and are maturity scores or control ratings required?

Response: BLR does not have an existing NIST maturity assessment available. The contractor must provide a current-state versus desired-state gap analysis aligned with NIST CSF 2.0, with prioritized recommendations. Separate numerical maturity scores or control ratings are not required.

22. Additional compliance obligations

Question: Are there other regulatory or compliance obligations to incorporate?

Response: Applicable obligations beyond the stated RFP and grant requirements will be identified in coordination with BLR during the project and addressed within the agreed scope.

23. Interviews, workshops, and stakeholder participation

Question: How many interviews and working sessions should proposers include, and who will participate?

Response: Proposers should identify and price the stakeholder interviews and working sessions needed to complete the project. BLR will designate a primary contact and facilitate participation by relevant leadership and operational departments. Individual participants will be coordinated through that contact.

The contractor is responsible for documenting and consolidating information and feedback gathered throughout the engagement.

24. Training, exercises, implementation, and remediation

Question: Are these activities included in the plan update?

Response: Facilitated tabletop exercises, staff training, hands-on remediation, and control implementation are outside scope. The contractor must provide recommendations and an implementation roadmap prioritizing proposed actions by risk, cost, and effort.

25. Roadmap horizon and detail

Question: What planning horizon, cost detail, and supporting recommendations are required?

Response: The roadmap must cover three years and prioritize actions by risk, cost, and effort. Estimated cost and effort ranges are acceptable; vendor-specific quotations are not required. Estimates must be supported by recent, credible data, with sources, dates, and key assumptions identified.

A proposed implementation schedule is not required. Staffing/resource recommendations and technology recommendations are optional.

26. Plan template and file formats

Question: Is there a preferred template, and are editable deliverables required?

Response: The contractor should use an appropriate NIST- or CISA-based cybersecurity planning template aligned with NIST CSF 2.0. The proposed template must be reviewed with BLR before drafting.

All written deliverables must be provided in editable Microsoft Word (.docx) and PDF formats. Any additional grant-specific template requirements remain pending confirmation.

27. Executive briefing

Question: How many leadership presentations are required, and what length and format are expected?

Response: Include one 60-minute executive briefing to BLR leadership, including questions and discussion. The briefing may be conducted remotely.

28. Early completion and support after delivery

Question: May the roadmap and briefing accompany the final plan at day 270, and may the engagement finish earlier?

Response: Yes. The roadmap and executive briefing may accompany the final plan at day 270 rather than waiting until the end of the performance period. Deliverables may also be completed

before day 270, subject to coordination with BLR and the required review and acceptance process.

The engagement is complete only after BLR has reviewed and accepted all required deliverables. Receipt alone does not constitute acceptance. After acceptance of all deliverables, no ongoing meetings, plan updates, or advisory support are required through the remaining performance period.

29. Review rounds and turnaround

Question: How many revision cycles and how much BLR review time should proposers allow?

Response: Include two consolidated review and revision rounds for each written deliverable. Allow 10 business days for BLR review of each submission. The contractor will consolidate feedback received through BLR's designated point of contact and incorporate agreed revisions.

The two-round allowance does not relieve the contractor of responsibility for correcting errors, omissions, or failure to meet agreed requirements. Deliverables remain subject to BLR's acceptance.

30. Review and approval authority

Question: Who approves deliverables, and is board or legal review required?

Response: The CIO or designated senior BLR IT staff will review interim deliverables, including the gap analysis and draft plan. The Tribal Administrator will approve final deliverables, including the final plan and roadmap, based on their advice.

Separate board approval is not required for acceptance. Legal review will occur only if BLR determines it is needed.

31. Pricing and payment

Question: Are fixed-price proposals and staged payments acceptable?

Response: Fixed-price proposals are acceptable, as provided in the RFP. Staged payments tied to deliverables and project activities are also acceptable. Proposers must include a proposed payment schedule. Final payment timing, schedule, and acceptance conditions will be established in the contract.

Cost proposals must include estimated hours by labor category and task or deliverable, labor rates, expenses, and the total proposed price. This requirement applies to fixed-price proposals as well.

32. Proposal format and page limits

Question: Is there a required proposal template, page limit, or packaging requirement?

Response: No prescribed proposal template or page limit applies. Proposers may use their own formatting but must follow the content requirements and section order in Section 7. Submit the complete proposal, including the cost proposal, resumes, certifications, references, and appendices, as a single PDF.

C. Penetration Testing Services

33. Organizational scope and target counts

Question: Which organizations and systems are covered, and what counts are available?

Response: Testing will cover BLR Tribal government and infrastructure shared with other entities, consistent with the organizational scope of the Cybersecurity Plan Update.

Detailed scope, exclusions, and counts—including public IP addresses, domains, hostnames, internal hosts, servers, workstations, other devices, physical locations, subnets/VLANs, isolated networks, and Active Directory domains and forests—will be provided only to proposers with an executed NDA on file.

Final authorized testing boundaries will be documented in the signed Rules of Engagement before testing begins.

34. Applications and specialized environments

Question: Does scope include dedicated web application/API testing, cloud, wireless, VPN/remote-access services, OT/ICS/SCADA, or physical-security systems?

Response: Details regarding inclusion, exclusions, quantities, authenticated roles, and expected testing depth will be provided only to proposers with an executed NDA on file. Final authorized scope will be documented in the contract and signed Rules of Engagement.

35. Internal foothold and testing access

Question: What infrastructure, connectivity, credentials, and starting positions will be provided?

Response: Proposers should identify their requested testing infrastructure, remote connectivity, credentials, and account requirements. BLR will provide two internal testing starting positions if required.

All access arrangements are subject to BLR approval, remote-access restrictions, and required monitoring tools. Final arrangements will be documented in the Rules of Engagement before testing begins.

36. Segmentation testing

Question: Is dedicated segmentation testing required beyond internal lateral-movement testing?

Response: Yes. Dedicated network segmentation testing is required in addition to internal lateral-movement testing. Details regarding the network boundaries to be validated will be provided only to proposers with an executed NDA on file. Final scope will be documented in the contract and signed Rules of Engagement.

37. Social engineering

Question: Which methods, participant counts, and campaigns should proposers include?

Response: Proposers may recommend social-engineering methods, participant counts, and the number of campaigns, with associated pricing. Final scope, permitted techniques, restrictions, and exclusions will be established in the contract and signed Rules of Engagement before testing begins.

38. Second-test scope

Question: Is Test 2 a targeted retest or another full assessment?

Response: Include one consolidated, targeted retest covering the original findings and assessing whether remediation changes introduced new vulnerabilities in affected systems or controls. A second full assessment is not required.

Repeat social engineering, unrelated newly added assets, and additional remediation-validation rounds are outside the base scope and require separate agreement with BLR. Final scope will be documented in the contract and Rules of Engagement.

39. Remediation responsibility

Question: Who performs remediation?

Response: BLR will evaluate the contractor's recommendations and perform remediation. The contractor must provide clear, actionable recommendations and validate remediation during Test 2. Hands-on remediation by the contractor is outside scope.

40. Testing dates and remediation interval

Question: When will the tests occur, and what remediation interval should proposers assume?

Response: Testing dates and the remediation interval between Test 1 and Test 2 will be established with BLR during contract finalization. Approved testing windows and blackout periods will be documented in the Rules of Engagement. All work must be completed within the period of performance ending April 30, 2028.

41. Testing hours

Question: Is a minimum number of hours required per test?

Response: No fixed minimum is prescribed. Proposers should identify and price the level of effort necessary to complete the required scope.

42. After-hours work, blackout periods, and disruptive methods

Question: Are there significant scheduling restrictions or security-control evasion requirements?

Response: There are no major after-hours testing requirements. Blackout periods will apply during critical operational periods within normal working hours.

Methods that could disrupt business operations must be expressly limited. Permitted security-control evasion techniques, prohibited activities, operational safeguards, and final testing windows will be defined in the signed Rules of Engagement before testing begins.

43. Notification and coordination

Question: Will all IT staff be notified of testing?

Response: Notification and coordination requirements will be defined in the Rules of Engagement. The CIO will be informed of all testing. Information about specific activities may be withheld from other personnel, including IT staff, as established in the Rules of Engagement.

44. Detection and response documentation

Question: Are detection and response measurements required?

Response: Yes. The contractor must document testing activity timelines, including the origin and start and end times, so BLR staff can correlate activities with internal detection and response records.

Detection and response measurements must be documented to support BLR's Incident Response Plan. Coordination and reporting details will be established in the Rules of Engagement.

45. Joint incident-response exercise

Question: Is a joint exercise required?

Response: A joint incident-response exercise is permitted but not required. Proposers may identify it as an optional activity and state any additional cost separately. Any exercise must be agreed upon with BLR and authorized through the contract and Rules of Engagement.

Required testing timelines and detection/response documentation remain part of the base scope.

46. Deliverable formats

Question: What formats are required for reports and supporting materials?

Response: Deliverables must use formats appropriate to their purpose. Reports may be provided as PDFs. Findings and remediation-tracking materials must also be provided in an editable format, such as an Excel spreadsheet, so BLR can track remediation progress. Other supporting materials should be provided in usable formats appropriate to their content.

47. Solicitation identifier

Question: Which RFP number should proposers use?

Response: Use **BLR-CYBER-PENTEST-2026-02-IT**, as shown on the RFP cover. The footer's omission of "-IT" is a typographical error.