



BLUE LAKE RANCHERIA

1 Aiyekwee Loop, Blue Lake, CA 95525

REQUEST FOR PROPOSAL

Penetration Testing Services

RFP No. [BLR-CYBER-PENTEST-2026-02-IT]

Issue Date: October 1st, 2026 | Proposals Due: November 30th, 2026 5:00 PM Pacific

Not-to-Exceed Budget: \$40,000

Funded in whole or in part by the Tribal Homeland Security Grant Program (THSGP)

Table of Contents

Table of Contents.....	2
1. Introduction and Background	3
2. Purpose and Objectives	3
Goal	3
Objective	3
Capability Gap Addressed	3
Intended Outcomes	3
3. Scope of Work	3
4. Rules of Engagement.....	4
5. Deliverables and Schedule.....	4
6. Period of Performance	5
7. Contractor Qualifications	5
8. Proposal Requirements.....	5
9. Cost Proposal	5
10. Evaluation Criteria.....	6
11. Submission Instructions and Timeline	6
12. Confidentiality and Non-Disclosure	6
13. Point of Contact	7
14. Terms and Conditions	7

1. Introduction and Background

Blue Lake Rancheria (“BLR” or the “Tribe”) is issuing this Request for Proposals (“RFP”) to solicit proposals from qualified firms (“Contractor”) to conduct two (2) penetration tests of the Tribe’s information technology (IT) systems. This engagement is supported by funding under the Tribal Homeland Security Grant Program (THSGP) and is intended to improve and secure BLR’s overall cybersecurity systems by identifying and safely exploiting vulnerabilities before malicious actors can.

The BLR IT Department is a skilled team of ten professionals with more than 70 years of combined experience across fields including defense and medical software development. The team manages all aspects of IT operations, including infrastructure, systems reliability, and security governance.

2. Purpose and Objectives

Goal

To improve and secure BLR’s overall cybersecurity systems.

Objective

Conduct two (2) penetration tests to identify and exploit vulnerabilities in BLR’s cyber systems during the period of performance (POP).

Capability Gap Addressed

BLR currently lacks validated detection and response capabilities for real-world attack scenarios. While the Tribe maintains controls such as firewalls, intrusion detection systems (IDS), endpoint protections, and incident response plans, these controls often go untested against realistic, evolving attack techniques. This creates a capability gap between perceived security and actual resilience.

Intended Outcomes

Penetration testing helps identify vulnerabilities in BLR’s cyber systems before malicious actors can exploit them. It also strengthens the Tribe’s overall security posture by testing response plans and improving incident detection and mitigation strategies.

3. Scope of Work

The Contractor shall plan and perform two (2) penetration tests of the Tribe’s IT systems. The Tribe anticipates an initial (baseline) test followed by a validation (retest) after remediation, though proposers may recommend an alternative structure that best fits the Tribe’s needs. The engagement shall cover, at a minimum:

- External network penetration testing of internet-facing systems, perimeter devices, and public-facing services.
- Internal network penetration testing, including lateral movement and privilege-escalation scenarios from an assumed internal foothold.
- Social engineering testing of staff (e.g., phishing or pretext-based techniques), conducted within agreed ethical and legal boundaries.

The Contractor shall:

1. Conduct testing in accordance with a recognized methodology (e.g., NIST SP 800-115, PTES, OSSTMM, and/or OWASP) and map findings to real-world adversary techniques (e.g., MITRE ATT&CK).
2. Identify, validate, and where authorized safely exploit vulnerabilities to demonstrate real-world impact, without causing damage to or disruption of Tribe systems or data.
3. Score and prioritize findings using CVSS (v3.1 or later) and provide clear, actionable remediation guidance for each finding.
4. Perform a second test to validate remediation of findings from the first test and confirm whether each issue is closed, partially mitigated, or accepted as residual risk.
5. Coordinate closely with the BLR IT Department and protect all Tribe data accessed during testing.

4. Rules of Engagement

All testing shall be governed by a written Rules of Engagement (ROE) document executed by both parties before any testing begins. The ROE shall define, at a minimum:

- Authorized scope and explicit exclusions (in-scope and out-of-scope systems, IP ranges, and assets).
- Formal written authorization to test the agreed-upon assets, protecting both parties from unauthorized-access claims.
- Approved testing windows and any blackout periods to avoid impact to Tribe operations.
- Permitted techniques and any prohibited actions (e.g., denial-of-service, destructive testing).
- Communication plan and emergency contacts on both sides, including escalation and stop-test procedures.
- Handling, storage, and disposal of sensitive data and findings, and incident-notification procedures for any critical vulnerability discovered.

5. Deliverables and Schedule

The Contractor shall provide the following deliverables. Timeframes are measured from contract execution and may be adjusted by mutual agreement within the period of performance.

#	Deliverable	Target Timeframe
1	Project kickoff, work plan, and signed Rules of Engagement (ROE)	Within [30] days of contract execution
2	Penetration Test #1 (initial/baseline) — execution and findings	[Per agreed schedule]
3	Detailed Test #1 report with CVSS-scored findings and remediation guidance	Within [30] days of Test #1
4	Penetration Test #2 (validation/retest after remediation)	[Per agreed schedule]
5	Final report including retest results and executive briefing	End of POP

Each report shall include, at a minimum: an executive summary; the methodology and standards applied; individual findings with affected asset, CVSS severity, evidence (e.g., screenshots, logs, proof of concept), risk narrative, and remediation recommendation; and an overall assessment of the Tribe's security posture.

6. Period of Performance

The anticipated period of performance is January 1st, 2027 through April 31st, 2028, consistent with the terms of the Tribal Homeland Security Grant Program award. All testing, deliverables, and invoicing must be completed within the period of performance.

7. Contractor Qualifications

- Demonstrated experience conducting penetration tests, preferably for tribal governments, public-sector entities, or critical-infrastructure organizations.
- Testers holding recognized certifications such as OSCP, GPEN, CEH, GWAPT, or CISSP.
- Use of recognized testing methodologies and standards (NIST SP 800-115, PTES, OSSTMM, OWASP, MITRE ATT&CK).
- Appropriate professional liability and cyber insurance, and willingness to execute the Tribe's confidentiality and data-protection terms, including an NDA.
- Ability to perform and complete all work within the period of performance.

8. Proposal Requirements

To be considered, proposals must include the following, in order:

6. Cover letter signed by an authorized representative, including firm name, address, and primary contact.
7. Statement of qualifications and relevant penetration-testing experience.
8. Technical approach and methodology, including standards used and how findings are scored and reported.
9. Proposed testing schedule aligned to the period of performance.
10. Key personnel resumes and certifications.
11. At least three (3) references for comparable penetration-testing work, including contact information.
12. Sample (redacted) penetration test report, if available.
13. Detailed cost proposal (see Section 9), including a not-to-exceed total.
14. Disclosure of any conflicts of interest and required federal certifications (debarment/suspension, lobbying, as applicable).

9. Cost Proposal

The total contract amount shall not exceed \$40,000 (forty thousand dollars), inclusive of all labor, expenses, and reimbursable costs. Proposers shall submit a detailed cost proposal that includes a total not-to-exceed price for both tests, a breakdown by task or deliverable, labor categories and rates, and any reimbursable expenses. Pricing must remain valid for at least [90]

days from the proposal due date. Because this Investment is grant-funded, all costs must be allowable, allocable, and reasonable under applicable federal cost principles (2 CFR Part 200).

10. Evaluation Criteria

Proposals will be evaluated by a Tribe review committee on the basis of the following weighted criteria.

Evaluation Criterion	Max Points
Demonstrated experience conducting penetration tests (tribal / government / critical infrastructure)	25
Technical approach, methodology, and recognized standards used (e.g., NIST SP 800-115, PTES, OSSTMM, MITRE ATT&CK)	25
Qualifications and certifications of assigned testers (e.g., OSCP, GPEN, CEH, CISSP)	20
Cost and value	15
Project schedule and ability to meet the period of performance	10
References and past performance	5
Total	100

11. Submission Instructions and Timeline

Proposals must be received no later than the due date and time below. Late proposals may be rejected. Submit one (1) electronic copy in PDF format to the contact listed in Section 13.

Milestone	Target Date
RFP issued	October 1 st , 2026
Deadline for written questions	October 15 th , 2026
Responses to questions posted	October 29 th , 2026
Proposals due	November 30 th , 5:00 PM Pacific
Evaluation and interviews (if any)	December 1 st – December 18 th
Anticipated notice of award	December 31 st
Anticipated contract start	1 st Quarter 2027

All dates are subject to change. Any changes will be issued by written addendum to all known proposers.

12. Confidentiality and Non-Disclosure

Because this RFP and the resulting engagement involve highly sensitive information about the Tribe's information technology infrastructure, security posture, and vulnerabilities, all proposers and recipients of this RFP are required to execute the Tribe's Non-Disclosure Agreement (NDA).

- As a condition of award, the selected Contractor and its personnel must sign and comply with the Tribe's NDA before accessing any nonpublic information regarding the Tribe's systems, networks, or security controls, and before any testing begins.
- Requests for information (RFIs) or any request for additional, sensitive, or non-public details about the Tribe's infrastructure may require the requesting party to sign an NDA before the Tribe will respond. The Tribe reserves the right to withhold sensitive information until an NDA is executed.
- Confidential Information — including all test results, findings, and reports — may be used solely for purposes of this RFP and any resulting contract. Recipients shall not copy, disclose, publish, or disseminate Confidential Information to any third party and shall take reasonable precautions to prevent unauthorized use or disclosure.
- Confidentiality obligations survive the RFP process and any resulting contract. Upon request or completion, recipients shall return or securely destroy all Confidential Information, including any data accessed during testing.

A copy of the Tribe's standard NDA is available upon request and will be incorporated into any resulting contract.

13. Point of Contact

All questions and proposals must be directed to the designated contact below. Proposers shall not contact other Tribe staff or officials regarding this RFP.

Robert Pollard

Blue Lake Rancheria

pentestrfp@bluelakerancheria-nsn.gov

1 Aiyekwee Loop, Blue Lake, CA 95525

14. Terms and Conditions

- This RFP does not commit the Tribe to award a contract or to pay any costs incurred in the preparation of proposals.
- The Tribe reserves the right to accept or reject any or all proposals, to waive informalities, and to cancel or reissue this RFP at any time.
- Any resulting contract is contingent upon the availability and terms of Tribal Homeland Security Grant Program funding and compliance with all applicable grant requirements.
- Indian/Tribal preference may be applied consistent with Tribal policy and applicable law.
- Award and the commencement of any testing are contingent upon execution of and compliance with the Tribe's Non-Disclosure Agreement (see Section 12) and a signed Rules of Engagement (see Section 4).
- The selected Contractor must comply with applicable federal requirements for grant-funded procurements, including 2 CFR Part 200, and execute the Tribe's standard contract terms, including confidentiality and data-protection provisions.
- Nothing in this RFP or any resulting contract shall be construed as a waiver of the Tribe's sovereign immunity.

[End of RFP]