



BLUE LAKE RANCHERIA

1 Aiyekwee Loop, Blue Lake, CA 95525

REQUEST FOR PROPOSAL

Cybersecurity Plan Update

RFP No. [BLR-CYBER-PLAN-2026-01-IT]

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

Not-to-Exceed Budget: \$60,000

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. Deliverables and Schedule.....	4
5. Period of Performance	4
6. Contractor Qualifications	4
7. Proposal Requirements.....	5
8. Cost Proposal	5
9. Evaluation Criteria.....	6
10. Submission Instructions and Timeline	6
11. Confidentiality and Non-Disclosure	6
12. Point of Contact	7
13. 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 or consultants (“Contractor”) to update the Tribe’s Cybersecurity Plan. This engagement is supported by funding under the Tribal Homeland Security Grant Program (THSGP) and is intended to strengthen the Tribe’s ability to detect, respond to, and recover from modern cyber threats.

The BLR Information Technology (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, and its expertise supports innovation, efficiency, and data protection across the Rancheria.

2. Purpose and Objectives

The purpose of this Investment is to prevent unauthorized access, data breaches, and malware infections affecting tribal assets by updating the Tribal Cybersecurity Plan. The selected Contractor will work with the Tribe’s planning team throughout the period of performance to produce a current, actionable plan.

Goal

Prevent unauthorized access, data breaches, and malware infections of tribal assets by updating the Tribal Cybersecurity Plan.

Objective

Use a qualified consultant to update the Plan in coordination with the Tribe’s planning team during the period of performance (POP).

Capability Gap Addressed

The absence of a regularly updated cybersecurity plan presents a significant capability gap in the Tribe’s ability to effectively detect, respond to, and recover from modern cyber threats. As the threat landscape evolves rapidly, an outdated plan fails to address current vulnerabilities, threat vectors, and regulatory requirements.

Intended Outcomes

An updated Cybersecurity Plan will ensure the Tribe is prepared to address current and emerging cyber threats effectively. This reduces the risk of security breaches, protects sensitive data, and helps maintain business continuity.

3. Scope of Work

The Contractor shall update the Tribe’s Cybersecurity Plan in alignment with recognized frameworks (e.g., the NIST Cybersecurity Framework and applicable CISA guidance) and the requirements of the Tribal Homeland Security Grant Program. At a minimum, the Contractor shall:

1. Review the Tribe’s current Cybersecurity Plan, related policies, and existing security controls, and conduct a gap analysis against current threats, vulnerabilities, and regulatory requirements.

2. Interview key IT and leadership stakeholders to understand the Tribe's systems, governance structure, risk tolerance, and operational priorities.
3. Update governance, roles, and responsibilities, including incident response, business continuity, and disaster recovery provisions.
4. Address current threat vectors, including ransomware, phishing, malware, and unauthorized access, and recommend updated controls and safeguards.
5. Align the Plan with the NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover) and applicable THSGP / CISA requirements.
6. Develop an implementation roadmap that prioritizes recommended actions by risk, cost, and effort.
7. Deliver a final, board-ready Cybersecurity Plan and present findings to Tribe leadership.

The Contractor shall coordinate with the BLR IT Department throughout the engagement, and shall protect all Tribe data and information in accordance with applicable confidentiality and data-handling requirements.

4. 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 meeting and work plan	Within [30] days of contract execution
2	Assessment of current Cybersecurity Plan and gap analysis	[90] days
3	Draft updated Cybersecurity Plan for Tribe review	[180] days
4	Final updated Cybersecurity Plan incorporating Tribe feedback	[270] days
5	Implementation roadmap and executive briefing	End of POP

5. 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 work, deliverables, and invoicing must be completed within the period of performance.

6. Contractor Qualifications

Proposers should demonstrate the following minimum qualifications:

- Demonstrated experience developing or updating cybersecurity plans, preferably for tribal governments, public-sector entities, or critical-infrastructure organizations.
- Working knowledge of the NIST Cybersecurity Framework, CISA guidance, and federal grant compliance requirements.

- Qualified personnel holding relevant certifications (e.g., CISSP, CISM, CISA, or equivalent).
- Ability to perform and complete the work within the period of performance.
- Appropriate professional liability and cyber insurance, and willingness to execute the Tribe's confidentiality and data-protection terms.

7. Proposal Requirements

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

8. Cover letter signed by an authorized representative, including firm name, address, and primary contact.
9. Statement of qualifications and relevant experience, including similar engagements.
10. Technical approach and methodology describing how the Scope of Work will be accomplished.
11. Proposed project schedule aligned to the period of performance.
12. Key personnel resumes and certifications.
13. At least three (3) references for comparable work, including contact information.
14. Detailed cost proposal (see Section 8), including a fixed price or fully loaded hourly rates and a not-to-exceed total.
15. Disclosure of any conflicts of interest and required federal certifications (debarment/suspension, lobbying, as applicable).

8. Cost Proposal

The total contract amount shall not exceed \$60,000 (sixty 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 all deliverables, 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).

9. 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 updating cybersecurity plans (tribal / government / critical infrastructure)	25
Technical approach and methodology	25
Qualifications and certifications of assigned personnel	20
Cost and value	15
Project schedule and ability to meet the period of performance	10
References and past performance	5
Total	100

10. 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 11.

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.

11. Confidentiality and Non-Disclosure

Because this RFP and the resulting engagement involve sensitive information about the Tribe's information technology infrastructure and security posture, 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.

- 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 may be used solely for the purpose of preparing a response to this RFP and performing 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.

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

12. 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

Cyberplanrfp@bluelakerancheria-nsn.gov

1 Aiyekwee Loop, Blue Lake, CA 95525

13. 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 continued access to Tribe information are contingent upon execution of and compliance with the Tribe's Non-Disclosure Agreement (see Section 11).
- 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]