



REQUEST FOR PROPOSALS

Rural Critical Access Hospital Cybersecurity Program

Shared Fractional CISO Governance and Grover C. Dils Security Infrastructure Deployment

RFP Information	Details
Issuing organization	Nevada Rural Hospital Partners Foundation, Inc. (NRHPF)
RFP name	RFP — RHIT Cybersecurity Program Proposal
Issue date	October 16, 2026
Questions due	Friday, October 23, 2026 at 11:59 p.m. Pacific Time
Proposal due	Friday, October 30, 2026 at 11:59 p.m. Pacific Time (NRHPF clock)
Anticipated performance period	Contract execution through August 30, 2027, subject to award and funding
Total not-to-exceed planning ceiling	\$398,000
Posted	https://nrhp.org
Contact for questions and submission	Procurement@nrhp.org

Issued by NRHPF for a federally/state-supported RHIT procurement under the Rural Health Transformation Program.

Contents

1. Notice and procurement summary
 2. Organization and project background
 3. Scope of services
 4. Deliverables, milestones, and reporting
 5. Budget and pricing requirements
 6. Minimum vendor qualifications
 7. Proposal format and submission instructions
 8. Evaluation and selection process
 9. Procurement terms and contract requirements
- Appendix A. Pricing schedule
- Appendix B. Vendor certifications

1. Notice and procurement summary

Nevada Rural Hospital Partners Foundation, Inc. (NRHPF) invites sealed written proposals from qualified and responsible information-technology and cybersecurity service providers to deliver an integrated rural cybersecurity program for four Nevada rural Critical Access Hospitals. NRHPF anticipates one contract covering both components described in this RFP.

This is a formal solicitation for a procurement exceeding \$25,000. NRHPF intends to obtain competitive proposals from at least three responsible vendors, if possible, and will evaluate all responsive proposals using the same published requirements and evaluation measures.

Milestone	Date / requirement
RFP posted	October 16, 2026
Deadline for written questions	October 23, 2026 at 11:59 p.m. Pacific Time
NRHPF answers/addenda, if issued	On or before October 27, 2026, by written addendum
Proposal deadline	October 30, 2026 at 11:59 p.m. Pacific Time, using the NRHPF clock
Anticipated evaluation and approval	November 2026, subject to NRHPF review and Board approval
Anticipated contract start	Upon contract execution and all required approvals

Late proposals

Proposals received after the stated deadline will be considered late and may be excluded from consideration. NRHPF will apply the stated deadline using the NRHPF clock. If a late proposal is received, NRHPF may mark it "Late Proposal," retain it unopened in the procurement file when applicable, and notify the submitting vendor.

2. Organization and project background

NRHPF is a Nevada nonprofit and the grant-holding and program-delivery affiliate of Nevada Rural Hospital Partners. NRHPF supports rural member hospitals through shared services, externally funded programs, and technology initiatives.

The project is designed for four geographically dispersed rural hospitals that do not currently have a dedicated Chief Information Security Officer (CISO): Humboldt General Hospital, South Lyon Medical Center, Grover C. Dils Medical Center, and the Mt. Grant General Hospital in Mineral County.

The project has two reinforcing components. Component A establishes shared executive cybersecurity governance and risk-management capacity. Component B deploys and operates a security-infrastructure pilot at Grover C. Dils Medical Center. The components are distinct and must be priced and reported separately so that no cost is charged twice.

The project supports HIPAA/HITECH security and rural cybersecurity objectives. It does not fund underlying clinical or electronic-health-record systems, network connectivity, or broadband infrastructure.

3. Scope of services

The selected contractor shall provide the personnel, expertise, tools, managed services, implementation, documentation, reporting, and transition support necessary to complete both components. Delivery will be primarily remote, with on-site risk assessments and milestone visits as needed and as approved by NRHPF.

3.1 Component A — Shared fractional CISO program

The contractor shall provide a qualified fractional Chief Information Security Officer (CISO) function shared across the four participating hospitals. The contractor shall tailor work to each hospital while maintaining common governance, reporting, and documentation standards.

- Conduct recurring HIPAA-aligned risk assessments across operations, systems, and compliance obligations.
- Provide vulnerability-assessment and vulnerability-management oversight.
- Develop a hospital-specific, prioritized five-year security roadmap aligned to each hospital's budget cycle.
- Develop, review, and maintain HIPAA/HITECH compliance frameworks, policies, supporting documentation, and audit-readiness materials.
- Provide monthly executive reports and leadership meetings for each participating hospital.
- Provide internal staff cross-training and knowledge transfer.
- Provide technical governance and oversight of Component B at Grover C. Dils Medical Center.

Planning allocation for BP1 is 120 CISO hours per month based on the size of each hospital: 40 hours per month for Humboldt General Hospital, 40 hours per month for South Lyon Medical Center, 20 hours per month for Grover C. Dils Medical Center, and 20 hours per month for Mt. Grant General Hospital. Vendors shall propose a transparent staffing and hour-allocation model and may recommend a different allocation if they demonstrate that all required outcomes will be achieved within the component ceiling.

3.2 Component B — Grover C. Dils security-infrastructure deployment

The contractor shall implement, operationalize, monitor, document, and transition a security-infrastructure model at Grover C. Dils Medical Center. Brand references below establish the current planning baseline; proposals may offer an equal or superior solution that meets the stated functional requirements.

Service area	Minimum performance requirement
Endpoint protection	Protect and monitor 80 workstations, including anti-malware/ransomware defense, policy management, alerting, and reporting.
Server protection	Protect and monitor 6 servers with managed detection, response, and operational reporting.
Patch management	Provide operating-system and third-party patch management, exception tracking, and monthly compliance reporting.
24/7 monitoring	Provide 24/7 NOC alert response, escalation, incident triage, and documented response records.
Breach detection	Provide managed breach detection for endpoints and servers, with investigation and remediation support.
Microsoft 365 identity	Provide managed Identity Threat Detection and Response for Microsoft 365 users.
Email security	Secure 45 Microsoft 365 mailboxes using Acronis Advanced Email Security or equal; tune policies and report outcomes.
Security management	Provide NEX Armor Advanced or equal expanded security-management capabilities, email-policy tuning, and incident-investigation support.
Proactive improvement	Provide monthly block hours for proactive improvement, remediation, and risk reduction.
Helpdesk integration	Integrate operational support and ticketing through Streamline IT or an equal interface, with a continuous record of requests, actions, and outcomes.
Implementation services	Assign an implementation project manager; transfer or create documentation; produce a technology roadmap; coordinate transition from existing tools; and complete a comprehensive onboarding security assessment.

3.3 Security, privacy, and data-protection requirements

- Use least-privilege and role-based access controls, multi-factor authentication for remote and privileged access, and encryption of data in transit and at rest.
- Maintain documented incident identification, containment, response, escalation, and notification procedures.
- Protect confidential hospital and patient-related information and comply with applicable HIPAA, HITECH, state privacy, breach-notification, and contractual requirements.
- Provide security logs, alert records, patch records, incident records, and other documentation reasonably requested by NRHPF for oversight and audit.
- Notify NRHPF promptly of suspected or confirmed security incidents affecting project systems, data, or services, and cooperate in investigation and remediation.
- Use subcontractors only with NRHPF's prior written approval and flow down all applicable security, confidentiality, audit, and federal/state requirements.

4. Deliverables, milestones, and reporting

The selected contractor shall submit a final project implementation plan within 30 calendar days after contract execution. The following minimum deliverables and milestones apply; NRHPF may refine dates in the executed work plan without materially changing the approved scope or budget.

Timeframe	Required milestone / deliverable	Required evidence
Months 1–2	Kickoff at all four hospitals; points of contact designated; CISO onboarding; implementation project manager assigned; documentation-transfer plan.	Kickoff agendas, contact list, implementation plan, risk/issues log.
Months 1–3	Complete HIPAA-aligned risk and vulnerability baselines for all four hospitals; complete Grover C. Dils onboarding assessment; begin deployment.	Four assessments, gap analyses, baseline report, deployment inventory, CISO review.
Months 3–4	Draft hospital-specific HIPAA/HITECH policy and compliance frameworks; deploy core endpoint, server, email, identity, patch, and monitoring capabilities at Grover C. Dils.	Draft policy packages, configuration records, deployment status report.
Months 4–6	Finalize frameworks and policy packages; deliver prioritized remediation plans and five-year roadmaps; begin security awareness and cross-training.	Final policy packages, four roadmaps, remediation trackers, training records.
Months 3–10	Operate 24/7 monitoring, managed breach detection, patch management, monthly improvement hours, helpdesk integration, executive reporting, and remediation oversight.	Monthly CISO reports, monthly operations reports, NOC/alert records, patch reports, ticket trends, incident/remediation logs.
Months 9–10	Confirm Grover C. Dils Year 2 transition terms and document a replicable consortium model.	Transition confirmation, Year 2 cost/terms summary, replication package.
By August 30, 2027	Complete BP1 annual performance and final deliverables.	Final report, final reconciliation, sustainability indicator, complete audit-ready record set.

Monthly reports must show hours by hospital, completed activities, risk and roadmap status, remediation oversight, material issues requiring escalation, and component-level cost allocation. For Grover C. Dils, monthly operations reports must also show service availability, alert volumes and dispositions, patch status, incidents, remediation actions, and helpdesk activity.

NRHPF will retain full grant, procurement, reporting, and sustainability accountability. The contractor shall provide full cooperation for quarterly executive reviews, State reporting, monitoring, and audit requests.

5. Budget and pricing requirements

The total planning ceiling for this procurement is \$398,000 for the funded BP1 period. The ceiling is not a guarantee of expenditure. All pricing must be reasonable, necessary, allocable, allowable, and supported by sufficient detail for NRHPF to perform a cost/price analysis.

Component	Planning ceiling	Pricing requirement
Component A — Shared fractional CISO	\$288,000	Provide labor category, hourly or unit rates, planned hours by hospital and month, travel/onsite assumptions, subcontractor costs, and total not-to-exceed price.
Component B — Grover C. Dils infrastructure deployment	\$110,000	Provide implementation, licensing/managed-service, monitoring, support, and transition costs by service line and month; identify one-time versus recurring costs.
Total	\$398,000	Provide a total not-to-exceed amount and a component-level subtotal. No cost may be charged to both components.

Vendors may propose different rates or a different mix of labor categories if the proposal demonstrates equivalent or better value and remains within the applicable ceiling.

The contractor shall identify any Year 2 recurring cost that Grover C. Dils Medical Center would assume after BP1. NRHPF estimates a recurring managed-service cost of approximately \$8,425.59 per month (approximately \$101,107 per year); this is a planning reference, not a guaranteed price or commitment.

6. Minimum vendor qualifications

- Demonstrated experience delivering cybersecurity governance, HIPAA/HITECH compliance support, risk assessments, and managed security services for healthcare organizations.
- Qualified CISO-level personnel with experience supporting rural, frontier, Critical Access Hospital, or similarly resource-constrained providers.
- Demonstrated ability to provide 24/7 NOC alert response and managed detection/response for endpoints, servers, email, and Microsoft 365 identities.
- Documented information-security, confidentiality, incident-response, business-continuity, and subcontractor-management practices.
- Sufficient financial and operational capacity to perform the work through August 30, 2027 and to support transition activities.
- At least three references for comparable healthcare cybersecurity or managed-service engagements, including scope, period, client contact, and outcome.
- Ability to comply with applicable federal and state grant requirements, 2 CFR Part 200 Subpart D, 2 CFR 200.327 contract provisions, and NRHPF policies.

NRHPF will check the System for Award Management (SAM) exclusion records before selecting a new consultant or contractor. Vendors must disclose any current suspension, debarment, exclusion, or proposed exclusion and any material conflict of interest.

7. Proposal format and submission instructions

To be considered responsive, a proposal must follow the order below and clearly identify any exceptions. Proposals should be concise but complete; page limits may be proposed by NRHPF in an addendum if needed.

Required section	Minimum content
A. Cover letter	Legal name, address, primary contact, authorized signer, proposal validity period of at least 90 days, and confirmation that the vendor can meet the deadline and contract period.
B. Executive summary	Brief description of the proposed solution, key differentiators, and approach to serving four rural hospitals.

C. Technical and management approach	Work plan for both components; methodology; staffing; escalation model; implementation plan; risk management; hospital coordination; and approach to avoiding duplication between Components A and B.
D. Deliverables and schedule	Map the proposal to every required deliverable and milestone in Section 4; identify dependencies and assumptions.
E. Personnel and experience	Resumes or bios of key personnel, roles, availability, certifications, relevant healthcare experience, and comparable projects.
F. Security and privacy	Controls, access management, encryption, logging, incident response, breach notification, data retention, subcontractor controls, and relevant attestations or certifications.
G. References and financial capacity	At least three references and a concise statement of financial/operational capacity.
H. Pricing	Completed Appendix A with component subtotals, unit rates, assumptions, one-time and recurring costs, and any optional items clearly separated.
I. Certifications and exceptions	Completed Appendix B; conflict disclosure; SAM/debarment disclosure; subcontractor list; and a list of any exceptions to this RFP.

Submission: Email one searchable PDF proposal and the completed pricing schedule to procurement@nrhp.org with the subject line “RFP — RHIT Cybersecurity Program Proposal.”

Questions must be submitted in writing to procurement@nrhp.org by the questions deadline. Vendors shall not contact participating hospitals, Board members, or other NRHPF staff about this solicitation except through the designated contact.

NRHPF may issue written addenda. Vendors are responsible for monitoring the designated posting location and acknowledging receipt of all addenda in the proposal.

8. Evaluation and selection process

NRHPF will first review proposals for administrative responsiveness. Responsive proposals will then be evaluated using the same criteria and scoring method. NRHPF may request clarification, conduct reference checks, and negotiate with the highest-ranked responsible vendor, but is not obligated to do so.

Evaluation criterion	Weight
Administrative responsiveness (pass/fail): required format, timely receipt, signed certifications, complete pricing, and acknowledgement of addenda.	Pass/fail
Adequacy of proposed methodology and work plan	20%
Qualifications and experience of key personnel	15%
Demonstrated company experience with comparable healthcare/rural cybersecurity work	15%
Technical solution, security controls, and functional compliance with the scope	15%
Project management, reporting, and ability to meet deadlines	10%
Cost, cost realism, and overall value	15%
Financial stability, references, and demonstrated commitment to the nonprofit/rural sector	5%
Small, minority, women-owned, or labor-surplus-area business participation and subcontracting plan	5%

The weights above operationalize the criteria in NRHPF’s procurement policy. NRHPF may adjust the weights only by written addendum before the proposal deadline. Each evaluator will use the same scoring grid, and the procurement file will document who participated in scoring, the scores, the basis for the decision, proposals received, and the final contract.

Final selection is subject to approval by the NRHPF President and Board of Directors/Council before contract execution. NRHPF will award to the responsible proposer whose proposal is most advantageous in terms of responsiveness, price, quality, delivery schedule, accountability, and fulfillment of the required services.

9. Procurement terms and contract requirements

Full and open competition: NRHPF will conduct the procurement to the maximum extent practicable through full and open competition. The scope is written in functional/performance terms and does not unduly restrict competition. A contractor that developed specifications, requirements, or a proposal for this procurement may not bid on the procurement.

Right to reject or cancel: NRHPF reserves the right to reject any or all proposals, cancel or amend the solicitation, waive minor informalities, request clarifications, and make no award when doing so is in NRHPF's best interest.

Cost/price analysis: NRHPF will review each cost element for reasonableness, allocability, and allowability and may request supporting documentation, competitive price information, market references, or other information.

Federal and state requirements: Federal and state grant procurement requirements supersede NRHPF policy when applicable. The selected contractor must comply with 2 CFR Part 200 Subpart D, including applicable requirements in §§200.317–200.327, and all grant-specific conditions.

Contract provisions: The final contract will include applicable federal/state flow-down provisions, nondiscrimination requirements, confidentiality and data-security obligations, breach notification, records access, termination and remedies, suspension/debarment representations, and any required lobbying or other federal-award clauses.

Right to audit: The final contract will include a right-to-audit clause permitting NRHPF staff or an auditor designated by NRHPF to access and review documentation and processes relating to the vendor's operations and documents maintained or processed on behalf of NRHPF, consistent with applicable law and confidentiality obligations.

Nondiscrimination: The vendor shall not discriminate against an employee or applicant for employment because of race, religion, color, sexual orientation, or national origin, except where a bona fide occupational qualification is reasonably necessary to normal operations, and shall provide required notices.

Small and diverse businesses: NRHPF will encourage participation by small businesses, minority businesses, women's business enterprises, and labor-surplus-area firms. Proposers shall identify such participation or explain good-faith outreach and any planned subcontracting.

Records and audit availability: NRHPF will maintain procurement and contract records and will make them available to the Federal or state awarding agency upon request. The vendor shall preserve supporting records for the period required by the award, contract, and applicable law.

Conflicts of interest: NRHPF will identify and address real or apparent conflicts. Vendors must disclose actual, potential, or apparent conflicts involving the vendor, proposed personnel, subcontractors, NRHPF, or participating hospitals.

Sole source and emergency exceptions: NRHPF may use a documented sole-source or emergency procurement only when permitted by applicable requirements. Any such action will require written justification, cost/price analysis, and any required funding-agency approval.

Metric and environmentally preferable practices: To the extent practicable and economically feasible, proposals should use metric units where relevant and identify services or products that conserve resources, protect the environment, or improve energy efficiency.

No commitment to future periods: The award is limited to the funded BP1 period. Future budget periods, renewals, or Year 2 service arrangements are not guaranteed.

Appendix A. Pricing schedule

Complete all applicable fields. Prices must be in U.S. dollars and remain valid for at least 90 days. If a cost is included in another line, state “included” and identify the line. Optional services must be separated from the required scope and will not be evaluated as required services.

Component A pricing item	Unit / basis	Quantity	Unit rate	Extended amount
Fractional CISO — Humboldt General Hospital	Hours per month	___	\$___	\$___
Fractional CISO — South Lyon Medical Center	Hours per month	___	\$___	\$___
Fractional CISO — Grover C. Dils Medical Center	Hours per month	___	\$___	\$___
Fractional CISO — Mt. Grant facility	Hours per month	___	\$___	\$___
Component A implementation / one-time setup	Lump sum	1	\$___	\$___
Component A travel / onsite costs	Lump sum or unit	___	\$___	\$___
Component A subtotal				\$___

Component B pricing item	Unit / basis	Quantity	Unit rate	Extended amount
Implementation project management	Lump sum	1	\$___	\$___
Endpoint protection and monitoring	Workstations	80	\$___	\$___
Server protection and monitoring	Servers	6	\$___	\$___
Patch management	Monthly managed service	10	\$___	\$___
24/7 NOC alert response	Monthly managed service	10	\$___	\$___
Managed breach detection	Monthly managed service	10	\$___	\$___
Managed Microsoft 365 identity protection	Users / monthly	___	\$___	\$___
Email security (Acronis Advanced Email Security or equal)	Mailboxes	45	\$___	\$___
Security management (NEX Armor Advanced or equal)	Monthly managed service	10	\$___	\$___
Monthly proactive-improvement block hours	Hours per month	___	\$___	\$___
Helpdesk integration (Streamline IT or equal)	Lump sum / monthly	___	\$___	\$___
Year 2 recurring continuation estimate	Monthly / annual	___	\$___	\$___
Component B subtotal				\$___

Summary	Amount
Component A subtotal	\$___
Component B subtotal	\$___
Total proposed not-to-exceed amount	\$___
Any proposed optional services (not included in total)	\$___

Pricing assumptions and exclusions:

Appendix B. Vendor certifications

The undersigned certifies that the vendor has reviewed this RFP and all acknowledged addenda and that the statements below are true and complete to the best of the signer's knowledge.

1. The proposal is submitted by an authorized representative and will remain valid for at least 90 days.
2. The vendor can perform the required work within the proposed schedule and budget.
3. The vendor has disclosed all actual, potential, or apparent conflicts of interest.
4. The vendor and proposed subcontractors are not suspended, debarred, or otherwise excluded from receiving Federal funds, except as disclosed below.
5. The vendor agrees to comply with applicable federal/state requirements, 2 CFR Part 200 Subpart D, and required contract flow-down provisions.
6. The vendor agrees to NRHPF's nondiscrimination, confidentiality, data-security, breach-notification, records-access, and right-to-audit requirements.
7. The vendor has not participated in developing the specifications or requirements for this procurement in a manner that would create an unfair competitive advantage.
8. The vendor will identify any exceptions to the RFP in a separate, clearly labeled attachment.

Exceptions, disclosures, or required explanations:

Legal name of vendor:

Authorized representative:

Title:

Signature:

Date:

Address:

Email / telephone:

End of Request for Proposals