



Rural Critical Access Hospital Cybersecurity Program RFP
Shared Fractional CISO Governance and Grover C. Dils Security Infrastructure Deployment
Addendum A: Responses to Questions
Published 10-27-2026

The following questions were received on or before 11:59 p.m. on Friday October 23rd, 2026, in compliance with the deadline provided in the Request for Proposals. The questions have been listed verbatim and grouped by topic area in no particular order.

References:

1. May the three required references from comparable healthcare cybersecurity engagements be satisfied by references for the proposed key personnel (e.g., the proposed fractional CISO) and/or by references from a proposed subcontractor, rather than only by the prime firm?

Yes, that is acceptable.

2. May the required three references for comparable healthcare cybersecurity or managed-service engagements be satisfied by (a) references for the proposed key personnel's individual work performed at prior employers, and/or (b) references from a proposed subcontractor or teaming partner for work that subcontractor will perform? Must all three be healthcare engagements, or do comparable non-healthcare managed-service engagements qualify?

Yes, that is acceptable. Comparable non-healthcare managed-service engagements will be accepted.

3. Section 6 requires three references for comparable healthcare cybersecurity or managed-service engagements. May the proposal include references from proposed delivery partners/subcontractors, clearly labeled as the partners' references, to demonstrate comparable delivery capacity?

Yes, that is acceptable.

Format:

4. Section 1 anticipates one contract for both components. Will NRHPF consider a proposal from a prime contractor that delivers Component A through a disclosed subcontracted CISO-level resource, and will the evaluation treat the subcontractor's personnel qualifications as the prime's?

Yes, that is acceptable.

5. Should the Appendix A pricing schedule be submitted as a separate file (and in what format), and will page limits apply?

The Appendix A pricing schedule could be submitted as a separate file but is not required to be separate. A page limit for the RFP response is being set by this Addendum at 50 pages. The Appendix A pricing schedule will not count toward the page limit.

6. Will NRHPF set a page limit or a required pricing-template format for Appendix A by addendum?

A page limit for the RFP response is being set by this Addendum at 50 pages.

7. No page limit is stated. Does NRHPF intend to issue page limits by addendum, and should resumes/bios in Section E be counted within any forthcoming limit?

A page limit for the RFP response is being set by this Addendum at 50 pages.

8. Section 7 asks for "one searchable PDF proposal and the completed pricing schedule." Should Appendix A be included inside the single PDF, or submitted as a second file (for example, a separate spreadsheet) alongside the PDF?

The Appendix A pricing schedule could be submitted as a separate file but is not required to be separate. A page limit for the RFP response is being set by this Addendum at 50 pages. The Appendix A pricing schedule will not count toward the page limit.

Component B:

9. For Component B, which Microsoft 365 licensing (for example Business Premium, E3/E5, Defender for Office 365 or Defender for Endpoint plans) is in place for the 45 mailboxes and 80 workstations? Will functionally equivalent Microsoft-native controls be accepted as "equal" to the named Acronis and NEX Armor products?

Microsoft 365 Business Standard is in place currently. Yes, functionally equivalent controls will be accepted as equal to the named products. The named products are for reference only.

10. Is there an incumbent provider for the current Grover C. Dils tooling, and what transition window is expected for moving off existing tools?

No, there is no incumbent provider, currently the services are provided in-house by Grover C. Dils.

11. Grover C. Dils environment: Please provide the current Microsoft 365 license tier, the existing endpoint/email security tools to be transitioned, and whether Streamline IT is an existing system at Grover C. Dils that the contractor must integrate with or a reference product only.

Microsoft 365 Business Standard is in place currently. The named products are for reference only.

12. For the named baselines (Acronis Advanced Email Security, NEX Armor Advanced, Streamline IT), will NRHPF evaluate proposed equals against functional requirements only, or is there additional equivalency documentation proposers should include? Is any of the named baseline tooling already deployed at Grover C. Dils today, and if so, is transition away from it expected during onboarding?

Functionally equivalent controls will be accepted as equal to the named products. Any documentation to help support the equivalency is appreciated but not required. The named products are for reference only.

13. The Component B scope names Acronis Advanced Email Security and NEX Armor Advanced as the planning baseline, with equal-or-superior solutions permitted. Are third-party product licenses (endpoint protection, email security, security management) expected to be procured by the contractor and included within the \$110,000 Component B ceiling, or does NRHPF or Grover C. Dils Medical Center procure licenses directly?

Yes, third-party product licenses are expected to be procured by the contractor and included within the \$110,000 ceiling.

14. Section 3.2 references transition from existing tools at Grover C. Dils Medical Center. Is there an incumbent managed-security provider whose tools will be transitioned, and will the incumbent cooperate with the transition?

No, there is no incumbent provider; currently the services are provided in-house by Grover C. Dils.

15. Appendix A leaves the quantity for "Managed Microsoft 365 identity protection" blank (users/monthly). How many Microsoft 365 users should proposers assume for that line at Grover C. Dils Medical Center, and is the tenant a single-organization tenant?

Vendors should assume for 51 users. The tenant is a single-organization tenant.

Travel:

16. Component A includes on-site risk assessments and milestone visits "as needed and as approved." For pricing the travel line, how many on-site visits per hospital should proposers assume during BP1?

Any proposed travel costs should be included within the \$398,000 ceiling. Contractors should plan for at least one on-site visit to each of the four hospitals during BP1.

17. Delivery is primarily remote, with on-site assessments as approved. Should proposed travel costs be included within the \$398,000 planning ceiling, and is there an expected number of on-site visits to the four hospitals during BP1?

Any proposed travel costs should be included within the \$398,000 ceiling. Contractors should plan for at least one on-site visit to each of the four hospitals during BP1.

18. Please confirm that primarily remote delivery with periodic onsite visits is acceptable, and indicate the minimum expected number of onsite visits per hospital during BP1 so that all vendors can price travel consistently.

Any proposed travel costs should be included within the \$398,000 ceiling. Contractors should plan for at least one on-site visit to each of the four hospitals during BP1.

19. How many on-site visits per hospital does NRHPF expect during BP1, and should travel be priced inside each component's ceiling?

Any proposed travel costs should be included within the \$398,000 ceiling. Contractors should plan for at least one on-site visit to each of the four hospitals during BP1.

Subcontracting:

20. (Sections 3.3 and 6): May the prime contractor deliver Component A with its own staff and subcontract the Component B managed security services (24/7 NOC, MDR, ITDR, email security), subject to NRHPF's prior written approval? Will a subcontractor's demonstrated 24/7 NOC/MDR capability be credited toward the Section 6 minimum qualifications?

Yes, that is acceptable. Yes, a subcontractor's demonstrated capabilities would count toward the qualification in section 6.

21. If we propose a managed security subcontractor for the Grover C. Dils infrastructure deployment component, should the request for NRHPF's written approval of that subcontractor be included in the proposal itself, or is it handled after selection?

That approval would occur after the selection process.

22. Section 3.3 requires NRHPF's prior written approval for subcontractors. Should proposers treat the subcontractor list in Proposal Section I, together with NRHPF's award, as that approval, or is a separate written approval required before the subcontractor begins work after award?

That approval would occur after the selection process.

Insurance:

23. The RFP does not state insurance requirements. Are there minimum insurance coverages (e.g., cyber liability, professional liability/technology E&O) the selected contractor must carry?

NRHPF will negotiate with the awarded vendor and the participating hospitals to ensure that there are no conflicts on minimum insurance coverages.

24. The RFP does not state minimum insurance limits. Will the contract require specific cyber-liability / technology E&O and general liability limits, and if so, what are they?

NRHPF will negotiate with the awarded vendor and the participating hospitals to ensure that there are no conflicts on minimum insurance coverages.

25. Will the contract require specific insurance coverages and limits (e.g., professional/technology E&O, cyber liability, general liability), a Business Associate Agreement, or other forms (e.g., W-9, lobbying certification)? If so, please specify them so they can be confirmed in the proposal.

NRHPF will negotiate with the awarded vendor and the participating hospitals to ensure that there are no conflicts on minimum insurance coverages.

Period of Performance/Budget Period 1:

26. Should the "Year 2 recurring continuation estimate" be included in the Component B subtotal and the \$110,000 ceiling, or provided for information only?

The Year 2 recurring continuation estimate should be provided for information only, and is not subject to the ceiling.

27. For pricing, should vendors assume a contract start of December 1, 2026, and 10 months of Component B recurring services as shown in Appendix A?

Vendors should assume a contract start date upon award during November with the month of November prorated by days. The project must be completed by August 31, 2027.

28. The performance period runs from contract execution through August 30, 2027, and Appendix A prices Component B monthly managed services at a quantity of 10 months. Should proposers plan on 10 months of service for both components (i.e., execution on or about November 1, 2026), and should the Component A fractional-CISO hours be priced over the same 10 months?

Vendors should assume a contract start date upon award during November with the month of November prorated by days. The project must be completed by August 31, 2027.

29. The performance period is contract execution through August 30, 2027, and Appendix A shows 10 monthly managed-service lines. If award occurs after December 2026, will BP1 be shortened, extended, or will the monthly quantities be adjusted?

Vendors should assume a contract start date upon award during November with the month of November prorated by days. The project must be completed by August 31, 2027.

30. Appendix A asks for a Year 2 recurring continuation estimate (with the RFP's ~\$8,425.59/month planning reference). Should that figure be presented separately as informational only, or included within the \$398,000 BP1 ceiling?

The Year 2 recurring continuation estimate should be provided for information only, and is not subject to the ceiling.

Other:

31. Contract form. Will NRHPF issue its own contract form? If so, can NRHPF publish it or its key terms (limitation of liability, indemnification, governing law, insurance requirements) as an addendum? May vendor standard terms be attached where they do not conflict?

NRHPF will not issue its own contract form but will negotiate with the awarded vendor on the contract provisions.

32. Business Associate Agreement. For services involving access to participating hospitals' protected health information, will the contractor sign a single Business Associate Agreement with NRHPF, separate BAAs with each participating hospital, or another structure? Will NRHPF or the hospitals provide the BAA form?

A Business Associate Agreement will be required between NRHPF, the vendor, and each of the four hospitals separately, and will be provided by NRHPF.

33. Subaward requirements. Can NRHPF provide the federal and state contract clauses required by its RHIT subaward from NVHA so proposers can confirm compliance in their proposals?

NRHPF will provide a comprehensive list during contract negotiations but many of the federal contract provisions may apply such as: Termination for Cause and Convenience; Equal Employment Opportunity; Davis-Bacon & Copeland Acts; Contract Work Hours & Safety Standards; Rights to Inventions; Clean Air & Federal Water Pollution Control Acts; Debarment & Suspension; Byrd Anti-Lobbying Amendment; and other applicable provisions.

34. CISO hour allocation: The RFP provides a 120-hour/month planning allocation for Component A and states vendors may propose a different allocation if all required outcomes are achieved within the component ceiling. Is a reduced allocation with the same deliverables genuinely acceptable, or is 120 hours/month the expected staffing level?

A reduced allocation with the same deliverables is acceptable.

35. Appendix A leaves the quantity blank for "Monthly proactive-improvement block hours." Is there a minimum or expected number of hours per month NRHPF has assumed for planning?

The expected number of hours per month will be up to the vendor.

36. For scoping the Component A risk assessments, can NRHPF share which electronic health record / core clinical systems are in use at each of the four hospitals (names only), and whether each hospital's assessment is expected to be conducted as a separate engagement with a separate report?

The Electronic Health Records for each hospital are:

Hospital	Electronic Health Record
Grover C Dils Medical Center	TruBridge
Humboldt General Hospital	Cerner
Mt. Grant General Hospital	Athena
South Lyon Medical Center	TruBridge

The assessment for each hospital is expected to be conducted under this engagement as a separate report.

-END-