New Mexico Educational Retirement Board

REQUEST FOR PROPOSALS (RFP)

Cybersecurity Managed Services



RFP# 27-352-1116-02719

RFP Release Date: November 16, 2026

Proposal Due Date: December 11, 2026

ELECTRONIC-ONLY PROPOSAL SUBMISSION

Table of Contents

I. INTRODUCTION 1

A. PURPOSE OF THIS REQUEST FOR PROPOSALS 1
B. BACKGROUND INFORMATION 1
C. SCOPE OF PROCUREMENT 1
D. PROCUREMENT MANAGER 2
E. PROPOSAL SUBMISSION 2
F. DEFINITION OF TERMINOLOGY 2
G. PROCUREMENT LIBRARY 6

II. CONDITIONS GOVERNING THE PROCUREMENT 7

A. SEQUENCE OF EVENTS 7
B. EXPLANATION OF EVENTS 7
1. Issue RFP 7
2. Acknowledgement of Receipt Form 7
3. Deadline to Submit Written Questions 8
4. Response to Written Questions 8
5. Submission of Proposal 8
6. Proposal Evaluation 9
7. Selection of Finalists 9
8. Oral Presentations 9
9. Best and Final Offers 9
10. Finalize Contractual Agreements 9
11. Contract Awards 10
12. Protest Deadline 10
C. GENERAL REQUIREMENTS 10
1. Acceptance of Conditions Governing the Procurement 10
2. Incurring Cost 10
3. Prime Contractor Responsibility 10
4. Subcontractors/Consent 11
5. Amended Proposals 11
6. Offeror's Rights to Withdraw Proposal 11
7. Proposal Offer Firm 11
8. Disclosure of Proposal Contents 11
9. No Obligation 12
10. Termination 12
11. Sufficient Appropriation 12
12. Legal Review 12
13. Governing Law 12
14. Basis for Proposal 12
15. Contract Terms and Conditions 12
16. Offeror's Terms and Conditions 13
17. Contract Deviations 13
18. Offeror Qualifications 13
19. Right to Waive Minor Irregularities 14
20. Change in Contractor Representatives 14
21. Notice of Penalties 14
22. Agency Rights 14

23. Right to Publish *14*
24. Ownership of Proposals *14*
25. Confidentiality *14*
26. Electronic mail address required *15*
27. Use of Electronic Versions of this RFP *15*
28. New Mexico Employees Health Coverage *15*
29. Campaign Contribution Disclosure Form *15*
30. Letter of Transmittal *15*
31. Disclosure Regarding Responsibility *16*
32. New Mexico/Native American Resident Preferences *18*

III. RESPONSE FORMAT AND ORGANIZATION 19

A. NUMBER OF RESPONSES 19
B. ELECTRONIC SUBMISSION 19
ELECTRONIC SUBMISSION ONLY Responses *19*
C. PROPOSAL CONTENT AND ORGANIZATION 20

IV. SPECIFICATIONS 22

A. DETAILED SCOPE OF WORK 22
PERFORMANCE REQUIREMENTS AND SERVICE LEVELS 34
INCIDENT CLASSIFICATION, SEVERITY, ESCALATION, AND COMMUNICATIONS 35
DATA PROTECTION, PRIVACY, AND EVIDENCE HANDLING 35
DELIVERABLE ACCEPTANCE CRITERIA 36
CHANGE CONTROL AND EXIT REQUIREMENTS 36
CONTRACTOR SECURITY AND SUBCONTRACTOR REQUIREMENTS 37
B. TECHNICAL SPECIFICATIONS 37
1. Organizational Experience *37*
2. Organizational References *38*
3. Mandatory Specification *38*
4. Desirable Specification and Due Diligence Questions *39*
C. BUSINESS SPECIFICATIONS 41
1. Financial Stability *41*
2. Letter of Transmittal Form *41*
3. Campaign Contribution Disclosure Form *41*
4. Oral Presentation *41*
5. Cost *41*
6. New Mexico/Native American Resident Preferences *42*

V. EVALUATION 43

A. EVALUATION POINT SUMMARY 43
B. EVALUATION FACTORS 43
1. B.1 Organizational Experience (See Table 1) *43*
2. B.2 Organizational References (See Table 1) *43*
3. B.3 Mandatory Specifications *44*
4. B.4 Desirable Specifications *44*
5. C.1 Financial Stability (See Table 1) *44*
6. C.2 Letter of Transmittal (See Table 1) *44*
7. C.3 Campaign Contribution Disclosure Form (See Table 1) *44*
8. C.4 Oral Presentation (See Table 1) *44*
9. C.5 Cost (See Table 1) *44*
10. C.6. New Mexico/Native American Resident Preferences *45*
C. EVALUATION PROCESS 45

APPENDIX A **46**
ACKNOWLEDGEMENT OF RECEIPT FORM **46**
APPENDIX B **48**
CAMPAIGN CONTRIBUTION DISCLOSURE FORM **48**
APPENDIX C **51**
DRAFT CONTRACT **51**
APPENDIX D **52**
COST RESPONSE FORM **52**
APPENDIX E **53**
LETTER OF TRANSMITTAL FORM **53**
APPENDIX F **55**
ORGANIZATIONAL REFERENCE QUESTIONNAIRE **55**

I. INTRODUCTION

A. PURPOSE OF THIS REQUEST FOR PROPOSALS

The purpose of the Request for Proposal (RFP) is to solicit sealed proposals to establish a contract through competitive negotiations for the procurement of Managed Cybersecurity Services.

B. BACKGROUND INFORMATION

The Educational Retirement Act (ERA) established a retirement system (the "Educational Retirement Fund" or the "Retirement Fund") for employees of the public schools, colleges, universities, and selected state agencies in the State of New Mexico. The system was established in 1957 and operates under the authority of New Mexico Statutes, Sections 22-11-1 et seq. NMSA 1978, as amended. The Act is administered by the Educational Retirement Board and its staff (collectively "NMERB"). As of June 30, 2025, the plan has approximately 64,274 active members, 52,852 inactive members and 56,764 retirees. The monthly benefits paid out in fiscal year 2025 were $1.437 billion. Assets of the Educational Retirement Fund under management are valued at approximately $18.9 billion as of June 30, 2025.

C. SCOPE OF PROCUREMENT

The New Mexico Educational Retirement Board (NMERB) is seeking a qualified firm to provide comprehensive Managed Cybersecurity Services to protect NMERB's enterprise technology environment, including its cloud infrastructure, on-premises systems, network and firewall infrastructure, web applications, endpoints, and the pension administration system that supports New Mexico's educators. The selected Offeror will deliver security services spanning all levels of cybersecurity responsibility — from hands-on, practitioner-level security operations through strategic, advisory-level oversight — including security monitoring and operations, vulnerability and patch management, cloud and network security, incident response and digital forensics, 24/7/365 incident coverage, identity and access security, security awareness training, risk management, and adherence to the NIST 800-53 controls framework. NMERB leadership will retain full governance authority over its cybersecurity program; the Offeror will operate in an execution and advisory capacity.

The term of the resulting contract will be for two (2) years, with the option to extend for two successive one-year terms. In no case will the contract, including all amendments thereof, exceed a total of four (4) years in duration.

This RFP will result in a single award.

This procurement will result in a contractual agreement between two parties; the procurement may ONLY be used by those two parties exclusively.

D. PROCUREMENT MANAGER

NMERB has assigned a Procurement Manager who is responsible for the conduct of this procurement whose name, address, telephone number and e-mail address are listed below:

Name: Felicia Sena, Procurement Manager
Telephone: (505) 531-6751
Email: Felicia.sena@erb.nm.gov

1. **Any inquiries or requests** regarding this procurement must be submitted, in writing, to the Procurement Manager. Offerors may contact **ONLY** the Procurement Manager regarding this procurement. Other state employees or Evaluation Committee members do not have the authority to respond on behalf of the NMERB.

2. **Protests of the solicitation or award must be submitted in writing to the Protest Manager identified in Section II.B.12.** As a Protest Manager has been named in this Request for Proposals, pursuant to §13-1-172 NMSA 1978 and 1.4.1.82 NMAC, **ONLY protests delivered directly to the Protest Manager in writing and in a timely fashion will be considered to have been submitted properly and in accordance with statute, rule and this Request for Proposals.** Protests submitted or delivered to the Procurement Manager will **NOT** be considered properly submitted.

E. PROPOSAL SUBMISSION

Proposals in response to this RFP must be submitted via email to the Procurement Manager. If your submission is too large to send via email, please contact the procurement manager to inquire about other means to submit your proposal. If a submission is password protected, the password must be submitted via email to the Procurement Manager prior to the submission deadline indicated in Section II.A, Sequence of Events.

F. DEFINITION OF TERMINOLOGY

This section contains definitions of terms used throughout this procurement document, including appropriate abbreviations:

1. "**Agency**" means the New Mexico Educational Retirement Board.

2. "**Award**" means the final execution of the contract document.

3. "**Business Hours**" means weekdays (Monday – Friday) 8:00 AM thru 5:00 PM MST/MDT, whichever is in effect on the date given.

4. "**Close of Business**" means weekdays (Monday – Friday) 5:00 PM MST/MDT, whichever is in effect on the date given.

5. "**Confidential**" means confidential financial information concerning Offeror's organization and data that qualifies as a trade secret in accordance with the Uniform Trade Secrets Act §§57-3-A-1 through 57-3A-7 NMSA 1978,. See also NMAC 1.4.1.45. The following items may **not** be labelled as confidential: Offeror's submitted Cost response, Staff/Personnel Resumes/Bios (excluding personal information such as personal telephone numbers and/or home addresses), and other submitted data that is **not** confidential financial information or that qualifies under the Uniform Trade Secrets Act.

6. "**Contract**" means any agreement for the procurement of items of tangible personal property, services or construction.

7. "**Contractor**" means any business having a contract with a state agency or local public body.

8. "**Determination**" means the written documentation of a decision of a procurement officer including findings of fact required to support a decision. A determination becomes part of the procurement file to which it pertains.

9. "**Desirable**" – the terms "may," "can," "should," "preferably," or "prefers" identify a desirable or discretionary item or factor.

10. "**Electronic Submission**" means a successful submittal of Offeror's proposal to the procurement manager.

11. "**Electronic Version/Copy**" means a digital format consisting of text, images or both, readable on computers or other electronic devices, which includes all content that the Original document contains. The electronic version/copy CANNOT be emailed.

12. "**Evaluation Committee**" means a body appointed to perform the evaluation of Offerors' proposals.

13. "**Evaluation Committee Report**" means a report prepared by the Procurement Manager and the Evaluation Committee to support the Committee's recommendation for contract award. It will contain scores and written evaluations of all responsive Offeror proposals.

14. "**Final Award**" means, in the context of this Request for Proposals and all its attendant documents, that point at which the final required signature on the contract(s) resulting from the procurement has been affixed to the contract(s) thus making it fully executed.

15. "**Finalist**" means an Offeror who meets all the mandatory specifications of this Request for Proposals and whose score on evaluation factors is sufficiently high to merit further consideration by the Evaluation Committee, as explained in Section II.B.8.

16. "**Hourly Rate**" means the proposed fully loaded maximum hourly rates that include travel, per diem, fringe benefits and any overhead costs for contractor personnel, as well as subcontractor personnel if appropriate.

17. "**IT**" means Information Technology.

18. "**Mandatory**" – the terms "must," "shall" "will," "is required," or "are required," identify a mandatory item or factor. Failure to meet a mandatory item or factor may result in the rejection of the Offeror's proposal.

19. "**Minor Irregularities**" means anything in the proposal that does not affect the price, quality and/or quantity, or any other mandatory requirement.

20. "**Multiple Source Award**" means an award of a contract for one or more items of tangible personal property, services or construction to more than one Offeror.

21. "**Offeror**" is any person, corporation, or partnership who chooses to submit a proposal.

22. "**Price Agreement**" means a definite quantity contract or indefinite quantity contract which requires the contractor to furnish items of tangible personal property, services or construction to a state agency or a local public body which issues a purchase order, if the purchase order is within the quantity limitations of the contract, if any.

23. "**Procurement Manager**" means any person or designee authorized by a state agency or local public body with the responsibility, authority, and resources to conduct the RFP procurement, make written determinations regarding the RFP procurement, and/or enter into or administer contracts as a result of the RFP procurement.

24. "**Procuring Agency**" means all State of New Mexico agencies, commissions, institutions, political subdivisions and local public bodies allowed by law to procure items of tangible personal property, services or construction from the agreement(s) awarded as a result of this RFP.

25. "**Project**" means a temporary process undertaken to solve a well-defined goal or objective with clearly defined start and end times, a set of clearly defined tasks, and a budget. The project terminates once the project scope is achieved and project acceptance is given by the project executive sponsor.

26. "**Redacted**" means a version/copy of the Offeror's proposal with the information considered proprietary or confidential (as defined by §§57-3A-1 to 57-3A-7 NMSA 1978 and NMAC 1.4.1.45 and summarized herein and outlined in Section II.C.8 of this RFP) blacked-out <u>BUT NOT</u> omitted or removed.

27. "**Request for Proposals (RFP)**" means all documents, including those attached or incorporated by reference, used for soliciting proposals.

28. "**Responsible Offeror**" means an Offeror who submits a responsive proposal and who has furnished, when required, information and data to prove that his financial resources, production or service facilities, personnel, service reputation and experience are adequate to make satisfactory delivery of the services, or items of tangible personal property described in the proposal.

29. "**Responsive Offer**" or means an offer which conforms in all material respects to the requirements set forth in the request for proposals. Material respects of a request for proposals include, but are not limited to price, quality, quantity or delivery requirements.

30. "**Sealed**" means, in terms of electronic submission, an Offeror's proposal and all accompanying documents has been completely and successfully emailed to the procurement manager prior to the submission deadline stated in the RFP.

31. **"Single Source Award**" means an award of contract for items of tangible personal property, services or construction to only one Offeror.

32. "**SPD**" means State Purchasing Division of the New Mexico State General Services Department.

33. "**Staff**" means any individual who is a full-time, part-time, or an independently contracted employee with the Offerors' company.

34. "**State (the State)**" means the State of New Mexico.

35. "**State Agency**" means any department, commission, council, board, committee, institution, legislative body, agency, government corporation, educational institution or official of the executive, legislative or judicial branch of the government of this state. "State agency" includes the Purchasing Division of the General Services Department and the State Purchasing Agent but does not include local public bodies.

36. "**State Purchasing Agent**" means the Director of the Purchasing Division of the General Services Department.

37. "**Statement of Concurrence**" means an affirmative statement from the Offeror indicating its response to a required Section IV specification agreeing to comply and concur with the stated requirement(s). This statement shall be included in Offerors proposal, pursuant to Section III.C.1. (E.g. "We concur," "Understands and Complies," "Comply," "Will Comply if Applicable," etc.)

38. "**Unredacted**" means a version/copy of the proposal containing all complete information; including any that the Offeror would otherwise consider confidential, such copy for use only for the purposes of evaluation.

39. "**Written**" means typed in standard 8 ½ x 11 inch document format, by common electronic means (such as Microsoft Word, Adobe PDF, etc.). A larger size document is permissible for charts, spreadsheets, etc.

G. PROCUREMENT LIBRARY

A procurement library has been established at https://www.erb.nm.gov/requests-for-proposals/. Offerors are encouraged to review the material contained in the Procurement Library by selecting the link provided in this document through your own internet connection. The library contains information listed below:

Procurement Regulations 1.4.1 NMAC

Educational Retirement Act, NMSA 1978, §§ 22-11-1 to -55.

II. CONDITIONS GOVERNING THE PROCUREMENT

This section of the RFP contains the schedule of events, the descriptions of each event, and the conditions governing this procurement.

A. SEQUENCE OF EVENTS

The Procurement Manager will make every effort to adhere to the following schedule:

Action	Responsible Party	Due Dates
1. Issue RFP	Agency	November 16, 2026
2. Acknowledgement of Receipt Form	Potential Offerors	November 20, 2026 by 3:00 p.m.
3. Deadline to submit Written Questions	Potential Offerors	November 23, 2026 by 3:00 p.m.
4. Response to Written Questions	Procurement Manager	November 30, 2026
5. Submission of Proposal	***Potential Offerors***	***December 11, 2026 by 3:00 p.m.***
6.* Proposal Evaluation	Evaluation Committee	December 14-18, 2026
7.* Selection of Finalists	Evaluation Committee	December 18, 2026
8. * Oral Presentation(s)	Finalist Offerors	Optional
9.* Best and Final Offers	Finalist Offerors	Optional
10.* Finalize Contractual Agreements	Agency/Finalist Offerors	December 21, 2026, to January 15, 2027
11.* Contract Awards	Agency/ Finalist Offerors	January 19, 2027
12.* Protest Deadline	SPD	+15 days

*Dates indicated in Events 6 through 12 are estimates only and may be subject to change without necessitating an amendment to the RFP.

B. EXPLANATION OF EVENTS

The following paragraphs describe the activities listed in the Sequence of Events shown in Section II.A., above.

1. Issue RFP

This RFP is being issued on behalf of the New Mexico Educational Retirement Board on the date indicated in Section II.A, Sequence of Events.

2. Acknowledgement of Receipt Form

Potential Offerors may e-mail the Acknowledgement of Receipt Form (APPENDIX A), to the Procurement Manager, Felicia Sena at Felicia.Sena@erb.nm.gov, to have their organization placed on the procurement Distribution List. The form must be returned to

the Procurement Manager by 3:00 PM MST/ MDT on the date indicated in Section II.A, Sequence of Events.

The procurement distribution list will be used for the distribution of written responses to questions, and/or any amendments to the RFP. Failure to return the Acknowledgement of Receipt Form does not prohibit potential Offerors from submitting a response to this RFP. However, by not returning the Acknowledgement of Receipt Form, the potential Offeror's representative shall not be included on the distribution list and will be solely responsible for obtaining from the Procurement Library (Section I.G.) responses to written questions and any amendments to the RFP.

3. Deadline to Submit Written Questions

Potential Offerors may submit written questions to the Procurement Manager as to the intent or clarity of this RFP until 3:00 pm MST/MDT as indicated in Section II.A, Sequence of Events. All written questions must be addressed to the Procurement Manager as declared in Section I.D. Questions shall be clearly labeled and shall cite the Section(s) in the RFP or other document which form the basis of the question.

4. Response to Written Questions

Written responses to the written questions will be provided via e-mail, on or before the date indicated in Section II.A, Sequence of Events, to all potential Offerors who timely submitted an Acknowledgement of Receipt Form (Section II.B.2 and APPENDIX A).

The Questions and Answers will be posted to: https://www.erb.nm.gov/requests-for-proposals/

5. Submission of Proposal

Only **electronic** proposal submission is allowed. **Do not** submit hard copies until further notice.

ALL PROPOSALS MUST BE RECEIVED BY THE PROCUREMENT MANAGER OR DESIGNEE NO LATER THAN **3:00 PM MST/MDT ON THE DATE INDICATED IN SECTION II.A, SEQUENCE OF EVENTS**. **NO LATE PROPOSAL CAN BE ACCEPTED.** The date and time of receipt will be recorded on each proposal. Such electronic submissions will be considered sealed in accordance with statute.

Proposals must be submitted electronically via email to the Procurement Manager. Multiple emails may be sent if a file is too large to send in one email. The Procurement Manager will acknowledge receipt of the RFP through email. If you do not receive an email acknowledgement of receipt or if your file is too large to send via email, contact the Procurement Manager for further guidance. If a submission is password protected, the password must be submitted via email to the Procurement Manager prior to the submission deadline indicated in Section II.A, Sequence of Events. Proposals submitted by facsimile, or other electronic means will not be accepted.

Proposals will be opened and reviewed to verify the submission met the minimum requirements by the Procurement Manager and a witness within 24 hours of the deadline.

A log will be kept of the names of all Offeror organizations that submitted proposals. Pursuant to §13-1-116 NMSA 1978, the contents of proposals shall not be disclosed to competing potential Offerors during the negotiation process. The negotiation process is deemed to be in effect until the contract is awarded pursuant to this Request for Proposals. Awarded in this context means the final required state agency signature on the contract(s) resulting from the procurement has been obtained.

6. Proposal Evaluation

An Evaluation Committee will perform the evaluation of proposals. This process will take place as indicated in Section II.A, Sequence of Events, depending upon the number of proposals received. During this time, the Procurement Manager may initiate discussions with Offerors who submit responsive or potentially responsive proposals for the purpose of clarifying aspects of the proposals. However, proposals may be accepted and evaluated without such discussion. Discussions SHALL NOT be initiated by the Offerors.

7. Selection of Finalists

The Evaluation Committee will select, and the Procurement Manager will notify the finalist Offerors as per schedule Section II.A, Sequence of Events or as soon as possible thereafter. A schedule for Oral Presentation, if any, will be determined at this time.

8. Oral Presentations

Finalist Offerors, as selected per Section II.B.7 above, may be required to conduct an oral presentation at a venue to be determined as per schedule Section II.A., Sequence of Events, or as soon as possible thereafter. If Oral Presentations are held, Finalist Offerors may be required to make their presentations through electronic means (Microsoft Teams, Zoom, etc.). The Agency will provide Finalist Offerors with an agenda and applicable details (such as, scheduled presentation date and time, time limits, etc.); including an invitation to the event. Whether or not Oral Presentations will be held is at the sole discretion of the Evaluation Committee.

9. Best and Final Offers

Finalist Offerors may be asked to submit revisions to their proposals for the purpose of obtaining best and final offers by as per schedule Section II. A., Sequence of Events or as soon as possible. The most advantageous proposal may or may not have received the most points. Best and final offers may also be clarified and amended at finalist Offeror's oral presentation.

10. Finalize Contractual Agreements

After approval of the Evaluation Committee Report, any contractual agreement(s) resulting from this RFP will be finalized with the most advantageous Offeror(s), taking into consideration the evaluation factors set forth in this RFP, as per Section II.A., Sequence of Events, or as soon as possible thereafter. The most advantageous proposal may or may not have received the most points. In the event mutually agreeable terms cannot be reached

with the apparent most advantageous Offeror in the timeframe specified, the Agency reserves the right to finalize a contractual agreement with the next most advantageous Offeror(s) without undertaking a new procurement process.

11. Contract Awards

The award is subject to appropriate Department and State approval. Upon receipt of the signed contractual agreement, the Agency Procurement office will award as per Section II.A., Sequence of Events, or as soon as possible thereafter.

12. Protest Deadline

Any protest by an Offeror must be timely submitted and in conformance with §13-1-172 NMSA 1978 and applicable procurement regulations. As a Protest Manager has been named in this Request for Proposals, pursuant to §13-1-172 NMSA 1978 and 1.4.1.82 NMAC, ONLY protests delivered directly to the Protest Manager in writing and in a timely fashion will be considered to have been submitted properly and in accordance with statute, rule and this Request for Proposals. The 15 calendar day protest period shall begin on the day following the notice of award of contract(s) and will end at 5:00 pm MST/MDT on the 15th day. Protests must be written and must include the name and address of the protestor and the request for proposal number. It must also contain a statement of the grounds for protest including appropriate supporting exhibits and it must specify the ruling requested from the party listed below. The protest must be directed to:

Jacob Maule
Jacob.Maule@erb.nm.gov

PROTESTS RECEIVED AFTER THE DEADLINE WILL NOT BE ACCEPTED.

C. GENERAL REQUIREMENTS

1. Acceptance of Conditions Governing the Procurement

Offerors must indicate their acceptance to be bound by the Conditions Governing the Procurement, Section II.C, and Evaluation, Section V, by completing and signing the Letter of Transmittal form, pursuant to the requirements in Section II.C.30, located in APPENDIX E.

2. Incurring Cost

Any cost incurred by the potential Offeror in preparation, transmittal, and/or presentation of any proposal or material submitted in response to this RFP shall be borne solely by the Offeror. Any cost incurred by the Offeror for set up and demonstration of the proposed equipment and/or system shall be borne solely by the Offeror.

3. Prime Contractor Responsibility

Any contractual agreement that may result from this RFP shall specify that the prime contractor is solely responsible for fulfillment of all requirements of the contractual

agreement with a State Agency which may derive from this RFP. The State Agency entering into a contractual agreement with a vendor will make payments to only the prime contractor.

4. Subcontractors/Consent

The use of subcontractors is allowed. The prime contractor shall be wholly responsible for the entire performance of the contractual agreement whether or not subcontractors are used. Additionally, the prime contractor must receive approval, in writing, from the agency awarding any resultant contract, before any subcontractor is used during the term of this agreement.

5. Amended Proposals

An Offeror may submit an amended proposal before the proposal due date. Such amended proposals must be complete replacements for a previously submitted proposal and must be clearly identified as such in the transmittal letter. **Agency personnel will not merge, collate, or assemble proposal materials.**

6. Offeror's Rights to Withdraw Proposal

Offerors will be allowed to withdraw their proposals at any time prior to the deadline for receipt of proposals. The Offeror must submit a written withdrawal request addressed to the Procurement Manager and signed by the Offeror's duly authorized representative.

The approval or denial of withdrawal requests received after the deadline for receipt of the proposals is governed by the applicable procurement regulations, 1.4.1.5 & 1.4.1.36 NMAC.

7. Proposal Offer Firm

Responses to this RFP, including proposal prices for services, will be considered firm for one-hundred twenty (120) days after the due date for receipt of proposals or ninety (90) days after the due date for the receipt of a best and final offer, if the Offeror is invited or required to submit one.

8. Disclosure of Proposal Contents

The contents of all submitted proposals will be kept confidential until the final award has been completed by the Agency. At that time, all proposals and documents pertaining to the proposals will be available for public inspection, *except* for proprietary or confidential material as follows:

a. ***Proprietary and Confidential information is restricted to***:
    1. confidential financial information concerning the Offeror's organization; and
    2. information that qualifies as a trade secret in accordance with the Uniform Trade Secrets Act, §§57-3A-1 through 57-3A-7 NMSA 1978.

b. An additional but separate redacted version of Offeror's proposal, as outlined and identified in Section III.B.1.a, shall be submitted containing the blacked-out proprietary or confidential information, in order to facilitate eventual public inspection of the non-confidential version of Offeror's proposal.

IMPORTANT: The price of products offered or the cost of services proposed **SHALL NOT** be designated as proprietary or confidential information.

If a request is received for disclosure of proprietary or confidential materials, the Agency shall examine the request and make a written determination that specifies which portions of the proposal should be disclosed. Unless the Offeror takes legal action to prevent the disclosure, the proposal will be so disclosed. The proposal shall be open to public inspection subject to any continuing prohibition on the disclosure of proprietary or confidential information.

9. No Obligation

This RFP in no manner obligates the State of New Mexico or any of its Agencies to the use of any Offeror's services until a valid written contract is awarded and approved by appropriate authorities.

10. Termination

This RFP may be canceled at any time and any and all proposals may be rejected in whole or in part when the Agency determines such action to be in the best interest of the State of New Mexico.

11. Sufficient Appropriation

Any contract awarded as a result of this RFP process may be terminated if sufficient appropriations or authorizations do not exist. Such terminations will be affected by sending written notice to the contractor. The Agency's decision as to whether sufficient appropriations and authorizations are available will be accepted by the contractor as final.

12. Legal Review

The Agency requires that all Offerors agree to be bound by the General Requirements contained in this RFP. Any Offeror's concerns must be promptly submitted in writing to the attention of the Procurement Manager.

13. Governing Law

This RFP and any agreement with an Offeror which may result from this procurement shall be governed by the laws of the State of New Mexico.

14. Basis for Proposal

Only information supplied in writing by the Procurement Manager or contained in this RFP shall be used as the basis for the preparation of Offeror proposals.

15. Contract Terms and Conditions

The contract between an agency and a contractor will follow the format specified by the Agency and contain the terms and conditions set forth in the Draft Contract (APPENDIX C). However, the contracting agency reserves the right to negotiate provisions in addition to those contained in this RFP Draft Contract (APPENDIX C) with any Offeror. The

contents of this RFP, as revised and/or supplemented, and the successful Offeror's proposal will be incorporated into and become part of any resultant contract.

The Agency discourages exceptions from the contract terms and conditions as set forth in the RFP Draft Contract (APPENDIX C). Such exceptions may cause a proposal to be rejected as nonresponsive when, in the sole judgment of the Agency (and the Evaluation Committee), the proposal appears to be conditioned on the exception, or correction of what is deemed to be a deficiency, or an unacceptable exception is proposed which would require a substantial proposal rewrite to correct.

Should an Offeror object to any of the terms and conditions as set forth in the RFP Draft Contract (APPENDIX C) strongly enough to propose alternate terms and conditions in spite of the above, the Offeror must propose **specific** alternative language. The Agency may or may not accept the alternative language. General references to the Offeror's terms and conditions or attempts at complete substitutions of the Draft Contract are not acceptable to the Agency and will result in disqualification of the Offeror's proposal.

Offerors must provide a brief discussion of the purpose and impact, if any, of each proposed change followed by the specific proposed alternate wording.

If an Offeror fails to propose any alternate terms and conditions during the procurement process (the RFP process prior to selection as successful Offeror), no proposed alternate terms and conditions will be considered later during the negotiation process. **Failure to propose alternate terms and conditions during the procurement process (the RFP process prior to selection as successful Offeror) is an explicit agreement by the Offeror that the contractual terms and conditions contained herein are accepted by the Offeror.**

16. Offeror's Terms and Conditions

Offerors must submit with the proposal a complete set of any additional terms and conditions they expect to have included in a contract negotiated with the Agency. See Section II.C.15 for requirements.

17. Contract Deviations

Any additional terms and conditions, which may be the subject of negotiation (such terms and conditions having been proposed during the procurement process, that is, the RFP process prior to selection as successful Offeror), will be discussed only between the Agency and the Offeror selected and shall not be deemed an opportunity to amend the Offeror's proposal.

18. Offeror Qualifications

The Evaluation Committee may make such investigations as necessary to determine the ability of the potential Offeror to adhere to the requirements specified within this RFP. The Evaluation Committee will reject the proposal of any potential Offeror who is not a Responsible Offeror or fails to submit a Responsive Offer as defined in §13-1-83 and §13-1-85 NMSA 1978.

19. Right to Waive Minor Irregularities

The Evaluation Committee reserves the right to waive minor irregularities, as defined in Section I.F.19. The Evaluation Committee also reserves the right to waive mandatory requirements, provided that **all** of the otherwise responsive proposals failed to meet the same mandatory requirements and the failure to do so does not otherwise materially affect the procurement. This right is at the sole discretion of the Evaluation Committee.

20. Change in Contractor Representatives

The Agency reserves the right to require a change in contractor representatives if the assigned representative(s) is (are) not, in the opinion of the Agency, adequately meeting the needs of the Agency.

21. Notice of Penalties

The Procurement Code, §§13-1-28 through 13-1-199 NMSA 1978, imposes civil, and misdemeanor and felony criminal penalties for its violation. In addition, the New Mexico criminal statutes impose felony penalties for bribes, gratuities and kickbacks.

22. Agency Rights

The Agency in agreement with the Evaluation Committee reserves the right to accept all or a portion of a potential Offeror's proposal.

23. Right to Publish

Throughout the duration of this procurement process and contract term, Offerors and contractors must secure from the agency written approval prior to the release of any information that pertains to the potential work or activities covered by this procurement and/or agency contracts deriving from this procurement. Failure to adhere to this requirement may result in disqualification of the Offeror's proposal or removal from the contract.

24. Ownership of Proposals

All documents submitted in response to the RFP shall become property of the State of New Mexico. If the RFP is cancelled, all responses received shall be destroyed by the Agency or SPD.

25. Confidentiality

Any confidential information provided to, or developed by, the contractor in the performance of the contract resulting from this RFP shall be kept confidential and shall not be made available to any individual or organization by the contractor without the prior written approval of the Agency.

The Contractor(s) agrees to protect the confidentiality of all confidential information and not to publish or disclose such information to any third party without the procuring Agency's written permission.

26. Electronic mail address required

A large part of the communication regarding this procurement will be conducted by electronic mail (e-mail). Offeror must have a valid e-mail address to receive this correspondence. (See also Section II.B.4, Response to Written Questions).

27. Use of Electronic Versions of this RFP

This RFP is being made available by electronic means. In the event of conflict between a version of the RFP in the Offeror's possession and the version maintained by the agency, the Offeror acknowledges that the version maintained by the agency shall govern. Please refer to: https://www.erb.nm.gov/requests-for-proposals/

28. New Mexico Employees Health Coverage

A. If the Offeror has, or grows to, six (6) or more employees who work, or who are expected to work, an average of at least 20 hours per week over a six (6) month period during the term of the contract, Offeror must agree to have in place, and agree to maintain for the term of the contract, health insurance for those employees if the expected annual value in the aggregate of any and all contracts between Contractor and the State exceed $250,000 dollars.

B. Offeror must agree to maintain a record of the number of employees who have (a) accepted health insurance; (b) decline health insurance due to other health insurance coverage already in place; or (c) decline health insurance for other reasons. These records are subject to review and audit by a representative of the state.

C. Offeror must agree to advise all employees of the availability of State publicly financed health care coverage programs by providing each employee with, as a minimum, the following web site link to additional information: https://bewellnm.com.

D. For Indefinite Quantity, Indefinite Delivery contracts (price agreements without specific limitations on quantity and providing for an indeterminate number of orders to be placed against it); these requirements shall apply the first day of the second month after the Offeror reports combined sales (from state and, if applicable, from local public bodies if from a state price agreement) of $250,000.

29. Campaign Contribution Disclosure Form

Offeror must complete, sign, and return the Campaign Contribution Disclosure Form (APPENDIX B) as a part of their proposal. This requirement applies regardless whether a covered contribution was made or not made for the positions of Governor and Lieutenant Governor or other identified official. **Failure to complete and return the signed, unaltered form will result in Offeror's disqualification.**

30. Letter of Transmittal

Offeror's proposal must be accompanied by the Letter of Transmittal Form located in APPENDIX E, which must be **signed** by the individual authorized to contractually obligate the company, identified in #2 below.

Provide the following information:

1. Identify the submitting business entity; Name, Mailing Address, Phone Number, Federal Tax ID Number (TIN), and New Mexico Business Tax ID Number(BTIN, formerly CRS);
2. Identify the Name, Title, Telephone, and E-mail address of the person authorized by the Offeror's organization to (A) contractually obligate the business entity providing the Offer, (B) negotiate a contract on behalf of the organization; and/or (C) provide clarifications or answer questions regarding the Offeror's proposal content *(A response to B and/or C is only necessary if the responses differs from the individual identified in A)*;
3. Identify any subcontractor/s that may be utilized in the performance of any resultant contract award;
4. Identify any other entity/-ies (such as State Agency, reseller, etc., that is not a sub-contractor identified in #3) that may be used in the performance of this awarded contract; and
5. The individual identified in #2 above, must sign and date the form, attesting to the veracity of the information provided, and acknowledging (a) the organization's acceptance of the Conditions Governing the Procurement stated in Section II.C.1, (b) the organizations acceptance of the Section V Evaluation Factors, and (c) receipt of any and all amendments to the RFP.

Failure to submit the signed Letter of Transmittal Form located in Appendix E will result in Offeror's disqualification.

31. Disclosure Regarding Responsibility

A. Any prospective Contractor and any of its Principals who enter into a contract greater than sixty thousand dollars ($60,000.00) with any state agency or local public body for professional services, tangible personal property, services or construction agrees to disclose whether the Contractor, or any principal of the Contractor's company:
   1. is presently debarred, suspended, proposed for debarment, or declared ineligible for award of contract by any federal entity, state agency or local public body;
   2. has within a three-year period preceding this offer, been convicted in a criminal matter or had a civil judgment rendered against them for:
      a. the commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) contract or subcontract;
      b. violation of Federal or state antitrust statutes related to the submission of offers; or
      c. the commission in any federal or state jurisdiction of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violation of Federal criminal tax law, or receiving stolen property;
   3. is presently indicted for, or otherwise criminally or civilly charged by any (federal state or local) government entity with the commission of any of the offenses enumerated in paragraph A of this disclosure;

4. has, preceding this offer, been notified of any delinquent Federal or state taxes in an amount that exceeds $3,000.00 of which the liability remains unsatisfied. Taxes are considered delinquent if the following criteria apply.
   a. The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge of the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.
   b. The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.
   c. Have within a three-year period preceding this offer, had one or more contracts terminated for default by any federal or state agency or local public body.)

B. Principal, for the purpose of this disclosure, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity or related entities.

C. The Contractor shall provide immediate written notice to the State Purchasing Agent or other party to this Agreement if, at any time during the term of this Agreement, the Contractor learns that the Contractor's disclosure was at any time erroneous or became erroneous by reason of changed circumstances.

D. A disclosure that any of the items in this requirement exist will not necessarily result in termination of this Agreement. However, the disclosure will be considered in the determination of the Contractor's responsibility and ability to perform under this Agreement. Failure of the Contractor to furnish a disclosure or provide additional information as requested will render the Offeror nonresponsive.

E. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the disclosure required by this document. The knowledge and information of a Contractor is not required to exceed that which is the normally possessed by a prudent person in the ordinary course of business dealings.

F. The disclosure requirement provided is a material representation of fact upon which reliance was placed when making an award and is a continuing material representation of the facts during the term of this Agreement. If during the performance of the contract, the Contractor is indicted for or otherwise criminally or civilly charged by any government entity (federal, state or local) with commission of any offenses named in this document the Contractor must provide immediate written notice to the State Purchasing Agent or other party to this Agreement. If it is later determined that the Contractor knowingly rendered an erroneous disclosure, in addition to other remedies available to the Government, the State Purchasing Agent or Central Purchasing Officer may terminate the involved contract for cause. Still further the State Purchasing Agent

or Central Purchasing Officer may suspend or debar the Contractor from eligibility for future solicitations until such time as the matter is resolved to the satisfaction of the State Purchasing Agent or Central Purchasing Officer.

32. New Mexico/Native American Resident Preferences

To ensure adequate consideration and application of §13-1-21 NMSA 1978 (as amended), **Offeror must submit a copy of its valid New Mexico/Native American Resident Preference Certificate or its valid New Mexico/Native American Resident Veteran Preference with its proposal.** Certificates for preferences must be obtained through the New Mexico Department of Taxation & Revenue http://www.tax.newmexico.gov/Businesses/in-state-veteran-preference-certification.aspx.

In accordance with §13-1-21(H) NMSA 1978, an agency shall not award any combination of New Mexico/Native American Resident Preferences.

In accordance with §13-1-21(J) NMSA 1978, the New Mexico/Native American Resident Preferences shall not apply if the expenditures for this RFP includes federal funds.

III. RESPONSE FORMAT AND ORGANIZATION

A. NUMBER OF RESPONSES

Offerors shall submit only one proposal in response to this RFP.

B. ELECTRONIC SUBMISSION

ELECTRONIC SUBMISSION ONLY Responses

Any proposal that does not adhere to the requirements of this **Section II.B** and **Section III.C Proposal Content and Organization** may be deemed non-responsive and rejected on that basis.

Proposals in response to this RFP must be submitted via email to the Procurement Manager:

The Offeror need only submit one single electronic copy of each portion of its proposal (Technical and Cost) as outlined below.

If a submission is password protected, the password must be submitted via email to the Procurement Manager prior to the submission deadline indicated in Section II.A, Sequence of Events.

Proposals must be submitted in the manner outlined below. Technical and Cost portions of Offerors proposal **must** be submitted in separate documents as indicated below in this section and **must** be prominently identified as "Technical Proposal" or "Cost Proposal".

1. **Technical Proposals –** One (1) ELECTRONIC document must be organized in accordance with **Section III.C. Proposal Content and Organization**. All information for the Technical Proposal **must be combined into a single file/document.** The Technical Proposals **SHALL NOT** contain any cost information.

    a. **Confidential Information**: If Offeror's proposal contains confidential information, as defined in Section I.F.5 and detailed in Section II.C.8, Offeror **must** submit **two (2) separate ELECTRONIC technical documents:**

        i. One (1) ELECTRONIC version of the requisite proposals identified in Section III.B.1.a above as **unredacted** (def. Section I.F.38) versions for evaluation purposes; and

        ii. One (1) **redacted** (def. Section I.F.26) ELECTRONIC for the public file, in order to facilitate eventual public inspection of the non-confidential version of Offeror's proposal. Redacted versions **must** be clearly marked as "REDACTED" or "CONFIDENTIAL" on the first page of the electronic file;

2. **Cost Proposals –** One (1) ELECTRONIC document of the proposal containing **ONLY** the Cost Proposal. All information for the cost proposal **must be combined into a single file/document.**

The ELECTRONIC proposal submission **must be emailed** by the submission deadline in Section II.B.5.

It is the Offeror's responsibility to ensure all documents are submitted electronically via email to the Procurement Manager by the deadline set forth in this RFP. *A submission that is not both: (1) fully complete; and (2) received, via email to the Procurement Manager by the deadline, will be deemed late.* ***If a submission is password protected, the password must be submitted via email to the Procurement Manager prior to the submission deadline indicated in Section II.A, Sequence of Events or it will be deemed late.*** *In accordance with statute and rule,* ***NO LATE OFFER CAN BE ACCEPTED****.*

Any proposal that does not adhere to the requirements of this Section and **Section III.C. Proposal Content and Organization** may be deemed non-responsive and rejected on that basis.

C. PROPOSAL CONTENT AND ORGANIZATION

All proposals must be submitted as follows:

Direct reference to pre-prepared or promotional material may be used if referenced and clearly marked. Promotional material must be minimal. Within each section of the proposal, Offerors must organize and address the RFP requirements in the order indicated below. All forms provided in this RFP must be thoroughly completed and included in the appropriate section of Offeror's proposal. **Any and all discussion of proposed costs, rates or expenses must occur ONLY in the Cost Proposal.**

Technical Proposal – DO NOT INCLUDE ANY COST INFORMATION IN THE TECHNICAL PROPOSAL.

1. Signed Letter of Transmittal
2. Signed Campaign Contribution Disclosure Form
3. Table of Contents
4. Proposal Summary (Optional)
5. Response to Contract Terms and Conditions (from Section II.C.15)
6. Offeror's Additional Terms and Conditions (from Section II.C.16)
7. Response to Specifications **(except Cost information which shall be included ONLY in Cost Proposal)**
   a. Organizational Experience
   b. Organizational References (Optional: Offeror may include a list of its references)
   c. Mandatory Specification
   d. Desirable Specification
   e. Financial Stability –(Financial information considered confidential, as defined in Section I.F. and detailed in Section II.C.8, should be placed in the **Confidential Information** file, per Section III.B.1.a, as applicable)

f. New Mexico/Native American Resident Preferences (if applicable)

8. Other Supporting Material (if applicable)

Cost Proposal:

1. Completed Cost Response Form (APPENDIX D)

Within each section of the proposal, Offerors should address the items in the order indicated above. All forms provided in this RFP must be thoroughly completed and included in the appropriate section of the proposal. **Any and all discussion of proposed costs, rates or expenses must occur ONLY in the Cost Proposal.**

A Proposal Summary may be included in Offeror's Technical Proposal, to provide the Evaluation Committee with an overview of the proposal; however, this material will not be used in the evaluation process unless specifically referenced from other portions of the Offeror's proposal. **DO NOT INCLUDE COST INFORMATION IN THE PROPOSAL SUMMARY.**

IV. SPECIFICATIONS

A. DETAILED SCOPE OF WORK

Task Item	Description
Security Operations & Monitoring	Contractor will provide managed security operations services to support Procuring Entity's cybersecurity program through continuous monitoring, threat detection, investigation, and incident response coordination. The Contractor shall provide proactive security monitoring, threat intelligence, vulnerability management support, and operational reporting services to identify, assess, and mitigate cybersecurity risks before they adversely affect business operations. Contractor will monitor security events and alerts generated by Procuring Entity's security technologies, including Trend Micro Vision One, Fortinet security platforms, Microsoft 365 security services, cloud environments, and other approved security tools. Security events will be reviewed, triaged, and prioritized based on severity, business impact, and potential risk to Procuring Entity systems and data. Confirmed security incidents will be investigated and escalated to designated Procuring Entity personnel in accordance with established incident response procedures. The Contractor shall conduct ongoing reviews of threat intelligence sources, vendor advisories, vulnerability disclosures, and emerging cyber threats relevant to the Procuring Entity's environment. Activities shall include monitoring indicators of compromise (IOCs), newly disclosed vulnerabilities, ransomware activity, and significant cybersecurity events that may require defensive actions, risk mitigation measures, or further investigation. The Contractor shall perform threat investigation and analysis activities to determine the scope, impact, severity, and root cause of suspicious or malicious activity. The Contractor shall provide containment recommendations, remediation guidance, and incident response support, as appropriate, based on the nature and severity of the event. Security incidents, investigation findings, remediation activities, and identified trends shall be documented, tracked, and reported through resolution. Contractor will provide regular operational reporting that summarizes: • Security monitoring activities and alert volumes • Significant threats and incident investigations • Vulnerability and risk trends • Recommended remediation actions • Security program performance metrics • Emerging threats and strategic recommendations
Vulnerability & Patch Management	Contractor will provide a comprehensive vulnerability and patch management program designed to identify, prioritize, remediate, and validate security weaknesses across Procuring Entity's environment. The program will support continuous risk reduction through regular vulnerability assessments, remediation tracking, and managed patch deployment activities. Using Procuring Entity's approved vulnerability management platform, Contractor will perform routine reviews of vulnerability scan results and assess findings based on severity, exploitability, asset criticality, and potential business impact. Vulnerabilities will be

	prioritized using a risk-based methodology to focus remediation efforts on the highest-risk exposures first. Contractor will maintain and manage the vulnerability remediation lifecycle, including: • Reviewing vulnerability assessment results • Prioritizing remediation activities • Coordinating corrective actions with Procuring Entity staff • Tracking remediation status and aging • Validating completed remediation efforts • Reporting on program effectiveness and outstanding risks In accordance with Procuring Entity's expectations, Contractor will manage the patching platform and patch deployment process for supported systems. This includes evaluating vendor security updates, testing and deployment planning, scheduling maintenance activities, coordinating implementation with Procuring Entity personnel, validating successful installation, and resolving patch-related issues as they arise. The vulnerability and patch management program will address: • Operating systems • Servers • Workstations and endpoints • Network infrastructure • Security appliances • Third-party applications • Cloud-hosted resources • Pension Administration System (PAS) components, as applicable Contractor will maintain remediation tracking and Plan of Action and Milestones (POA&M) documentation for significant findings, ensuring that identified vulnerabilities are monitored through closure. Program status, remediation progress, outstanding risks, and patch compliance metrics will be communicated through regular reporting and management briefings. Through this approach, Contractor will help Procuring Entity reduce cyber risk, improve security posture, maintain regulatory alignment, and establish a sustainable vulnerability management process that supports ongoing operational maturity. Patching and configuration work may be scheduled during after-hours maintenance windows to minimize production impact
Cloud Security (AWS)	Procuring Entity's reliance on cloud-hosted services and AWS infrastructure requires continuous oversight to ensure security controls remain aligned with organizational requirements, industry best practices, and evolving threats. Contractor will serve as Procuring Entity's security advisor and operational partner for cloud security, focusing on governance, configuration management, threat prevention, and continuous improvement. The Contractor shall review cloud environments to identify configuration weaknesses, excessive permissions, insecure network exposure, logging deficiencies, and other

	conditions that may increase organizational risk. The Contractor shall support the Procuring Entity in maintaining secure cloud architectures through the implementation and assessment of hardening standards, least-privilege access principles, multi-factor authentication controls, and continuous monitoring practices. Special emphasis will be placed on AWS security engineering and cloud security posture management (CSPM) activities, including periodic reviews of identity and access management (IAM), logging and monitoring capabilities, network security configurations, key management practices, and backup and recovery protections. Where risks are identified, Contractor will provide prioritized remediation recommendations and support implementation efforts in coordination with Procuring Entity staff. Cloud security findings, trends, and recommendations will be incorporated into regular management reporting and broader cybersecurity governance activities to support informed decision-making and ongoing risk reduction.
Network Security	Contractor will help Procuring Entity maintain a secure and resilient network environment through firewall policy management, security architecture review, network segmentation guidance, and ongoing security monitoring activities. Consistent with Procuring Entity's operational model, Procuring Entity personnel will continue to perform routine operational firewall administration and business-driven configuration changes. Contractor's role will focus on the security aspects of network management, including firewall hardening, policy reviews, rule optimization, intrusion prevention tuning, web filtering strategy, secure remote access controls, and review of changes that may introduce cybersecurity risk. The network security program will include periodic assessment of firewall rulesets, network segmentation effectiveness, privileged access pathways, VPN configurations, and perimeter defense controls. Contractor will also review vendor security advisories, emerging threats, and significant vulnerabilities affecting network infrastructure and provide recommendations for remediation or defensive improvements. When security-related network incidents occur, Contractor will support investigation and response efforts by analyzing relevant logs, evaluating affected systems, identifying potential attack vectors, and recommending containment and recovery actions. Recommendations will be documented and tracked through Procuring Entity's risk management and remediation processes.
Web Application Security	Procuring Entity relies on web-based services and cloud-delivered security technologies to support daily operations and provide secure access to organizational resources. Contractor will work with Procuring Entity to ensure these controls remain effective, properly configured, and aligned with cybersecurity best practices. The Contractor shall review, administer, and optimize web security technologies used to protect users from malicious websites, phishing campaigns, malware distribution sites, and other internet-based threats. Activities shall include policy review, configuration assessment, security tuning, exception management, and ongoing monitoring and reporting of web security control effectiveness. Because Procuring Entity is currently evaluating its long-term web security architecture, Contractor will remain flexible in supporting either Cisco Umbrella or alternative solutions that may be adopted in the future. Services associated with web filtering, DNS-layer security, endpoint-based web protection, and secure remote access technologies will be adjusted as Procuring Entity finalizes these decisions.

	In support of Procuring Entity's defense-in-depth strategy, Contractor will also: • Evaluate web security policies and filtering effectiveness • Review web-based threat detections and trends • Identify excessive or unnecessary access to high-risk internet resources • Recommend improvements to protect against phishing, malware, command-and-control communications, and other web-borne threats • Assist with the investigation of web-related security incidents when necessary Web security performance, notable threats, and recommended improvements will be incorporated into regular cybersecurity reporting, helping ensure leadership maintains visibility into emerging internet-based risks.
Identity and Access Security	Effective identity management is foundational to every cybersecurity program. Contractor will help Procuring Entity strengthen identity security by focusing on access governance, privileged account management, authentication controls, and ongoing reviews of user access rights. Rather than treating identity management as a standalone activity, Contractor approaches IAM as a continuous risk management function. User accounts, administrative privileges, service accounts, and authentication mechanisms all represent potential attack paths that must be regularly reviewed and maintained. Contractor will work with Procuring Entity to evaluate the effectiveness of existing identity controls, including Microsoft 365, Active Directory, cloud platforms, and enterprise applications. Areas of focus may include privileged access management, role-based access controls, multi-factor authentication adoption, account lifecycle management, and periodic access reviews. Special attention will be given to: • Administrative and privileged accounts • Shared or generic accounts • Remote access authentication controls • Third-party and vendor access • Service account security • Excessive permissions and privilege creep • Separation of duties concerns Where improvements are identified, Contractor will provide practical recommendations that balance security requirements with operational needs. Findings and recommendations will be tracked through Procuring Entity's broader risk management process and reviewed during governance and compliance discussions. This approach helps ensure that only authorized individuals maintain access to systems and information necessary to perform their responsibilities while reducing opportunities for misuse, credential compromise, and unauthorized access.

Incident Response and Digital Forensics	The Contractor shall serve as the Procuring Entity's primary cybersecurity incident response service provider and shall provide investigative, coordination, and advisory support throughout the incident response lifecycle. The Contractor shall support the identification, containment, eradication, recovery, and post-incident review of cybersecurity events affecting the Procuring Entity's systems, applications, cloud services, networks, and data. When suspicious activity is identified through Trend Micro, Fortinet, AWS, Imperva, Tenable, or other security platforms, Contractor will investigate the event to determine scope, severity, and potential impact. Contractor will coordinate response activities with Procuring Entity staff, provide actionable recommendations, and assist with documentation and communications as appropriate. For significant incidents, Contractor may perform forensic analysis activities including: • Log and artifact collection • Timeline reconstruction • User and system activity analysis • Malware and indicator-of-compromise review • Root cause determination • Documentation of findings and lessons learned Contractor will also maintain and periodically review Procuring Entity's Computer Security Incident Response Plan (CSIRP), ensuring procedures remain aligned with organizational requirements, evolving threats, and industry best practices. Support for tabletop exercises, after-action reporting, and continuous improvement activities will be integrated into the overall incident response program.
Threat Intelligence and Security Automation	Contractor shall supplement operational security activities with ongoing threat intelligence analysis and automation initiatives designed to increase visibility, improve response times, and reduce operational overhead. The Contractor shall continuously monitor and evaluate threat intelligence sources, vendor security advisories, MS-ISAC notifications, New Mexico Office of Cybersecurity communications, threat research publications, and emerging vulnerability disclosures to identify threats and risks relevant to the Procuring Entity's environment. The Contractor shall assess, prioritize, and translate applicable intelligence into actionable recommendations to support security monitoring, vulnerability management, patching, incident response, and risk mitigation activities. To improve operational efficiency, threat intelligence findings will be incorporated into security monitoring and automation activities. Contractor will develop and maintain security workflows, playbooks, and automated response processes where appropriate. Particular focus will be placed on integration between key security platforms within Procuring Entity's environment, including Trend Micro Vision One, Fortinet technologies, Tenable, AWS security services, and other approved tools. Examples of automation opportunities include alert enrichment, event correlation, vulnerability tracking, notification workflows, and response playbooks for recurring security events. As the environment evolves, Contractor will continue refining detection logic and response procedures to improve accuracy, reduce false positives, and strengthen Procuring Entity's overall security operations capability.

Security Awareness and Training	Cybersecurity awareness remains a critical component of Procuring Entity's overall security program. While technical controls help prevent and detect threats, informed users play an equally important role in reducing organizational risk. Consistent with Procuring Entity's operating model, responsibility for day-to-day administration of the security awareness program will remain with Procuring Entity personnel. Contractor will provide advisory support designed to strengthen program effectiveness, improve user preparedness, and align training efforts with current threat conditions. Contractor's support may include review of security awareness metrics, phishing simulation results, training participation statistics, and other performance indicators to identify trends and opportunities for improvement. Based on these reviews, Contractor will provide recommendations regarding awareness campaigns, targeted training topics, executive education, and emerging cybersecurity risks. Particular areas of focus may include: • Phishing and social engineering awareness • Credential theft and account security • Business email compromise (BEC) • Remote work and mobile device security • Artificial intelligence (AI) usage risks and governance • Data handling and privacy responsibilities • Ransomware prevention and response awareness Awareness program observations and recommendations will be incorporated into regular governance discussions to support continuous improvement and encourage a security-conscious culture throughout the organization.
Audit, Compliance, and Risk Management	Contractor will assist Procuring Entity in maintaining a mature cybersecurity governance program by supporting ongoing risk management, regulatory compliance, audit readiness, and cybersecurity program oversight. The Contractor shall support the Procuring Entity's cybersecurity governance, risk management, and compliance activities through the application of NIST 800-53 controls and the ongoing assessment of risks that may affect the Procuring Entity's operations, systems, members, or data. Compliance activities shall be integrated into day-to-day security operations to support the continued effectiveness of security controls as technologies, business requirements, and threat conditions evolve. As part of this effort, Contractor will maintain and update cybersecurity governance documentation, facilitate risk discussions, and assist with the evaluation of existing security controls. Identified risks will be documented, prioritized, tracked, and reported through a centralized risk management process that supports informed decision-making by management and key stakeholders. Key activities include: • Cybersecurity risk assessments and risk register maintenance • NIST 800-53 control review and maturity tracking • Audit preparation and audit response support

	• Security policy, standard, and procedure development • POA&M development and remediation tracking • Compliance reporting and status briefings • Coordination with external auditors and assessors • Executive and Board-level cybersecurity reporting To support long-term program maturity, Contractor will also provide strategic recommendations regarding security governance, investment priorities, policy enhancements, and remediation planning. Findings from vulnerability management, security operations, incident response, cloud security, and other cybersecurity activities will be incorporated into the broader risk management program to provide Procuring Entity leadership with a comprehensive view of organizational cyber risk.
Security Governance	Effective governance requires cybersecurity activities to remain aligned with organizational priorities, regulatory expectations, and operational realities. Contractor will assist Procuring Entity in maintaining security policies, standards, procedures, and related governance documentation while ensuring those materials remain practical and actionable. Security findings identified through monitoring activities, risk assessments, audits, vulnerability management, and incident investigations will be evaluated for policy and governance impacts. Where necessary, Contractor will recommend updates to existing standards, create supporting documentation, and assist with implementation planning. Contractor will also support cybersecurity roadmap development, executive briefings, governance committee discussions, and strategic planning efforts to ensure leadership maintains visibility into program maturity, emerging risks, and long-term cybersecurity objectives.
NIST 800-53 Framework Compliance	Procuring Entity has identified NIST 800-53 as the foundation of its cybersecurity program. Contractor will help maintain alignment with applicable controls by incorporating compliance considerations into day-to-day cybersecurity operations, governance activities, and technology reviews. Findings from vulnerability assessments, incident response activities, cloud security reviews, audit support efforts, and policy reviews will be evaluated against relevant NIST control requirements to identify gaps and remediation priorities. Contractor will assist with documentation updates, control assessments, POA&M development and maintenance, evidence collection, and audit preparation activities as needed. Regular reporting will provide Procuring Entity leadership with visibility into compliance status, outstanding risks, remediation progress, and opportunities for continued cybersecurity maturity improvement.
AI Governance and Oversight	Artificial intelligence capabilities are becoming increasingly embedded within enterprise applications, SaaS platforms, productivity tools, and business processes. As Procuring Entity evaluates and adopts AI-enabled technologies, cybersecurity, privacy, regulatory, and operational risks should be considered alongside the potential benefits. The Contractor shall support the Procuring Entity in establishing and maintaining governance processes for the evaluation, implementation, and ongoing oversight of artificial intelligence (AI) technologies. The Contractor shall assist in identifying and assessing the use of AI technologies within the organization, evaluating risks related to

	data exposure, model usage, third-party services, and regulatory requirements, and recommending appropriate governance, security, privacy, and risk mitigation controls. The Contractor shall provide advisory services related to the governance, evaluation, and secure adoption of artificial intelligence (AI) technologies. Services shall include the development and maintenance of AI-related policies, standards, and governance documentation; review and assessment of proposed AI use cases; evaluation of vendor-provided AI capabilities; and recommendations regarding the secure use of Microsoft Copilot and other AI-enabled technologies. The Contractor shall monitor developments in AI security, governance frameworks, regulatory requirements, and industry best practices and provide recommendations to support the Procuring Entity's AI governance, risk management, and compliance activities. Rather than treating AI as a standalone initiative, Contractor will incorporate AI governance considerations into Procuring Entity's broader cybersecurity, risk management, privacy, and compliance activities. This approach helps ensure that innovation can be pursued while maintaining appropriate oversight, accountability, and protection of sensitive information.
IoT and Physical Security Systems	Procuring Entity's physical security ecosystem includes connected technologies such as access control systems, video surveillance platforms, and other network-connected devices that require the same level of security oversight applied to traditional information systems. Because these systems often contain embedded operating systems, specialized firmware, and limited security controls, they can present unique cybersecurity risks if not properly managed. Contractor will provide security oversight for Procuring Entity's Internet of Things (IoT), operational technology (OT), and physical security environments to help ensure these systems remain appropriately protected and aligned with the organization's overall cybersecurity objectives. The Contractor shall periodically assess physical security systems and Internet of Things (IoT) and Operational Technology (OT) assets to identify vulnerabilities, insecure configurations, unsupported software or firmware, excessive network exposure, default credentials, and other conditions that may increase organizational risk. The Contractor shall document findings and provide recommendations for remediation, system hardening, risk reduction, and ongoing security improvements. Particular attention will be given to Procuring Entity's: • Physical access control systems • Video surveillance (CCTV) infrastructure • Network-connected security devices • Supporting management platforms and administrative interfaces A key component of this effort is ensuring that physical security technologies are appropriately segmented from the primary enterprise network. Contractor will review network architecture, connectivity paths, and access controls to help reduce the likelihood that a compromise of an IoT or physical security device could impact critical business systems. Because many IoT and physical security technologies require coordination with vendors, facilities personnel, or operational stakeholders, Contractor will work collaboratively with Procuring Entity and responsible third parties to support firmware updates, patching

	activities, configuration reviews, and system hardening efforts. Security risks, findings, and recommendations will be incorporated into Procuring Entity's broader vulnerability management and risk management processes to support ongoing improvement and visibility.
Incident Response & Tabletop Exercises	Effective incident response begins long before a security event occurs. To improve organizational readiness, Contractor will work with Procuring Entity to develop, maintain, and periodically update incident response playbooks that provide clear guidance for responding to the threats most relevant to the organization. Playbooks will establish response procedures, escalation paths, decision points, communication requirements, and recovery considerations for priority scenarios, including ransomware, business email compromise, data exfiltration, cloud security incidents, and events involving Procuring Entity's pension administration and business-critical systems. As Procuring Entity's environment evolves, playbooks will be reviewed and updated to reflect changes in technology, personnel, threat activity, and operational requirements. To validate procedures and improve organizational preparedness, Contractor will design and facilitate annual tabletop exercises involving Procuring Entity IT personnel, management, and other stakeholders as appropriate. These exercises are intended to simulate realistic cybersecurity events and evaluate decision-making, communications, escalation processes, roles and responsibilities, and overall incident response readiness. Each exercise will include: • Scenario development tailored to Procuring Entity's operating environment • Exercise planning and facilitation • Executive and participant briefings • Evaluation of response activities and decision-making processes • Documentation of observations, strengths, and improvement opportunities Following each tabletop exercise, Contractor will deliver an after-action report summarizing key findings, identified gaps, lessons learned, and recommended corrective actions. Playbooks, incident response procedures, and the Computer Security Incident Response Plan (CSIRP) will be updated as appropriate to incorporate exercise outcomes and support continuous improvement of Procuring Entity's incident response capabilities. This ongoing cycle of planning, testing, evaluation, and refinement helps ensure that Procuring Entity remains prepared to respond effectively to cybersecurity incidents while strengthening coordination between technical teams, leadership, and other stakeholders.
Knowledge Transfer & Staff Cross-Training	Contractor's objective is not only to provide cybersecurity services, but also to strengthen Procuring Entity's long-term internal capabilities. Throughout the engagement, the Contractor will work closely with Procuring Entity personnel to ensure critical security knowledge, procedures, and operational practices are effectively documented and transferred to internal staff. Knowledge transfer activities will be integrated into ongoing service delivery rather than treated as a separate project phase. As security processes are developed, refined, or updated, Contractor will create and maintain supporting documentation that enables Procuring Entity personnel to understand, support, and sustain key cybersecurity functions.

	Documentation may include: • Security runbooks and operational procedures • Standard operating procedures (SOPs) • Incident response workflows and escalation guides • Security tool administration references • System hardening and configuration standards • Patch management and vulnerability management procedures • Security architecture and technology documentation In addition to written documentation, Contractor will conduct periodic knowledge-sharing sessions with designated Procuring Entity personnel. These sessions may include walkthroughs of security tools, review of incident response activities, lessons learned from investigations, vulnerability management processes, governance activities, and emerging threats relevant to Procuring Entity's environment. Particular emphasis will be placed on ensuring Procuring Entity staff maintain sufficient familiarity with security technologies, operational procedures, and decision-making processes to support business continuity and successful transition planning. Should the engagement conclude or transition to another provider, Procuring Entity will retain the documentation, processes, and institutional knowledge necessary to continue operating and managing its cybersecurity program with minimal disruption. This collaborative approach reduces dependency on any single individual or service provider while helping Procuring Entity build and maintain internal cybersecurity expertise over time.
Collaboration & Meeting Participation	Successful managed cybersecurity services require ongoing coordination between Contractor and Procuring Entity personnel. Throughout the engagement, Contractor will maintain regular communication with Procuring Entity leadership and technical staff to ensure cybersecurity activities remain aligned with organizational priorities, operational requirements, and emerging risks. Contractor will participate in Procuring Entity's monthly IT department meetings to provide updates on security operations, ongoing initiatives, significant findings, remediation efforts, and strategic recommendations. These meetings also provide an opportunity to discuss emerging threats, planned technology changes, compliance activities, and other matters that may impact Procuring Entity's cybersecurity posture. To support collaboration and maintain a strong working relationship, Contractor will conduct periodic onsite visits to Procuring Entity's Santa Fe office. These visits may be used to facilitate planning sessions, conduct assessments, review security initiatives, support project activities, participate in tabletop exercises, and strengthen coordination with Procuring Entity personnel. The frequency and scheduling of onsite visits will be established as part of the final agreement. Contractor will maintain close working relationships with the CIO, Deputy CIO, and designated IT staff through regularly established communication channels. This collaborative approach enables timely decision-making, effective coordination of security activities, and visibility into organizational priorities and operational changes that may influence cybersecurity risk.

	During normal business operations, Contractor personnel will be available to discuss security concerns, provide guidance, coordinate remediation efforts, and support ongoing initiatives. In the event of a cybersecurity incident or other time-sensitive matter, communication and escalation procedures will be executed in accordance with established response processes to ensure appropriate stakeholders remain informed and engaged throughout the event. This continuous engagement model helps ensure cybersecurity remains integrated into Procuring Entity's daily operations while providing leadership and technical staff with direct access to trusted security advisors and operational support.
Governance and Authority	The Contractor shall provide subject matter expertise, operational support, and strategic advisory services; however, the Procuring Entity shall retain ownership of its cybersecurity program and authority for all risk, compliance, operational, and business decisions. Under this engagement, Contractor will operate in an advisory and execution capacity, working under the direction of authorized Procuring Entity personnel. Responsibility for establishing organizational priorities, approving security policies, accepting risk, allocating resources, and authorizing significant actions remains with Procuring Entity leadership, including the CIO, Deputy CIO, and other designated representatives. Contractor will provide recommendations regarding security controls, remediation strategies, incident response activities, governance matters, and technology investments; however, decisions involving risk acceptance, major configuration changes, exceptions to security requirements, operational disruptions, or other material business impacts will be elevated to Procuring Entity for review and approval. To support effective governance, Contractor will: • Provide timely information and recommendations to support informed decision-making • Escalate issues that exceed established authority thresholds • Clearly communicate significant risks, remediation options, and potential impacts • Document key recommendations, decisions, and action items when appropriate • Follow approved escalation and authorization procedures during security incidents and operational events In emergency situations where immediate action may be required to protect Procuring Entity systems, services, or data, Contractor will act in accordance with predefined incident response procedures and notify designated Procuring Entity personnel as quickly as practical. Outside of these circumstances, significant actions will be coordinated with and approved by authorized Procuring Entity representatives before implementation. This governance model establishes clear accountability, supports informed risk-based decision making, and ensures that cybersecurity activities remain aligned with Procuring Entity's operational and business objectives.
Deliverables & Timeline	The services described in this proposal represent an ongoing managed cybersecurity services engagement delivered throughout the contract term. Rather than a fixed-duration project, Contractor will provide recurring operational, advisory, governance, and security monitoring services designed to continuously mature and strengthen Procuring Entity's cybersecurity program.

Initial Onboarding and Service Transition

During the initial phase of the engagement, Contractor will:

• Review the results of Procuring Entity's cybersecurity risk assessment and validate security priorities

• Confirm service delivery procedures, escalation paths, communication protocols, and reporting requirements

• Establish recurring reporting templates and executive dashboard metrics

• Review existing security controls, policies, standards, and operational processes

• Finalize the cadence for governance meetings, status reporting, vulnerability reviews, and strategic planning activities

Ongoing Service Deliverables

Throughout the engagement, Contractor Secure will provide deliverables including, but not limited to:

Frequency	Tasks
Monthly Deliverables	• Security operations and threat monitoring summary • Vulnerability management status report • Security metrics and KPI dashboard • Security event and incident activity summary • Recommendations for remediation and risk reduction
Quarterly Deliverables	• Executive cybersecurity briefing • Cybersecurity roadmap review and update • Strategic risk and threat analysis • Compliance and governance status review
Annual Deliverables	• NIST 800-53 control assessment and maturity review • Security awareness program review • Incident response tabletop exercise and after-action report • Cybersecurity program recommendations and planning update
As Needed	• Incident response documentation • Investigation summaries and recommendations • Audit and compliance support documentation

	• Security advisory memoranda • Standard operating procedures, runbooks, and knowledge transfer materials Service Timeline Following contract award, services will transition from the initial onboarding and program establishment phase into steady-state operations. Recurring service activities, reporting, governance support, training, incident response readiness, and strategic advisory services will be delivered continuously throughout the term of the agreement.

Performance Requirements and Service Levels

The Contractor shall meet the following minimum performance requirements and service levels throughout the term of the engagement.

Coverage Hours. The Contractor shall provide security monitoring and operational coverage on a 24/7/365 basis. Routine advisory, consultation, and non-emergency support shall be available during the Procuring Entity's normal business hours, defined as 8:00 a.m. to 5:00 p.m. Mountain Time, Monday through Friday, excluding State holidays.

Scheduled and After-Hours Maintenance. Certain security maintenance activities — including but not limited to firewall updates, AWS security patching and configuration changes, and Pension Administration System (PAS) patching (including Linux operating system and database patching) and vulnerability mitigation — must frequently be performed outside of normal business hours to avoid disruption to production systems. The Contractor shall perform such planned maintenance activities during scheduled maintenance windows, including evenings and weekends, as required by the Procuring Entity and coordinated in advance. The Contractor shall treat performance of these activities during after-hours maintenance windows as a standard component of the services, not as emergency or incident-response activity.

Response Times. The Contractor shall acknowledge and respond to requests and events according to the following minimum service levels, measured from the time of detection or notification:

Severity	Description	Response Time
Critical	Active incident, confirmed or suspected compromise, or system outage with security impact	1 hour or less
High	Suspected compromise, major vulnerability, or significant security event	4 hours or less
Moderate	Security investigation support or non-urgent security issue	Next business day
Advisory	Planning, consultation, or routine request	As scheduled

Reporting. The Contractor shall provide reporting at the frequencies defined in the Deliverables and Timeline section, including monthly operational reporting, quarterly executive briefings, and annual program assessments. All reports shall be delivered in a format acceptable to the Procuring Entity.

Escalation. The Contractor shall maintain and adhere to a documented escalation procedure, including designated points of contact and after-hours escalation paths, to be established with the Procuring Entity upon contract commencement and reviewed at least annually.

Incident Classification, Severity, Escalation, and Communications

The Contractor shall classify, escalate, and communicate security incidents in accordance with the following requirements.

Classification and Severity. The Contractor shall assign a severity level to each security incident based on its scope, impact, sensitivity of affected systems or data, and potential harm to the Procuring Entity, its operations, or its members. Severity levels shall align with the tiers defined in the Performance Requirements and Service Levels section (Critical, High, Moderate, Advisory).

Escalation. The Contractor shall escalate incidents according to severity, notifying designated Procuring Entity personnel within the applicable response time. Critical and High severity incidents shall be escalated immediately to the Procuring Entity's designated incident response contacts, including the CIO or Deputy CIO.

Communication. The Contractor shall maintain clear and timely communication with the Procuring Entity throughout the incident lifecycle, including initial notification, status updates at intervals appropriate to the severity, and a formal notification upon containment and resolution. The Contractor shall comply with all applicable incident-reporting obligations, including notification to the New Mexico Office of Cybersecurity and other authorities as required by state or federal law or Procuring Entity policy.

Documentation. The Contractor shall document each incident, including classification, actions taken, root cause, and recommendations, and shall provide incident documentation to the Procuring Entity in accordance with the Deliverables requirements.

Data Protection, Privacy, and Evidence Handling

Data Protection and Privacy. The Contractor shall protect all Procuring Entity data, systems, and member information accessed or handled in the course of the engagement. The Contractor shall maintain the confidentiality, integrity, and availability of such data and shall not access, use, disclose, or retain Procuring Entity data except as necessary to perform the services. The Contractor shall handle all sensitive, financial, and member data, including personally identifiable information (PII), in accordance with applicable state and federal laws, regulations, and Procuring Entity policies.

Evidence Handling. In the course of incident response and forensic activities, the Contractor shall preserve, handle, and document digital evidence in a manner that maintains its integrity and defensibility. The Contractor shall maintain appropriate chain-of-custody documentation for any evidence collected, and shall handle, store, and transmit evidence securely. The Contractor shall support the Procuring Entity's legal, regulatory, and reporting requirements related to such evidence.

Data Return and Destruction. Upon request or at the conclusion of the engagement, the Contractor shall return or securely destroy all Procuring Entity data in its possession in accordance with Procuring Entity direction, and shall certify such return or destruction in writing

Deliverable Acceptance Criteria

The Contractor shall submit all deliverables in accordance with the schedule defined in the Deliverables and Timeline section. Deliverables shall meet the following acceptance criteria:

- Deliverables shall be complete, accurate, and consistent with the requirements of this Scope of Work;
- Deliverables shall be provided in a professional format acceptable to the Procuring Entity;
- Reports shall contain sufficient detail to be actionable and to allow the Procuring Entity to understand the Contractor's findings, activities, and recommendations.

The Procuring Entity shall review each deliverable and, within a reasonable period, either accept the deliverable or provide written notice of deficiencies. Upon receipt of such notice, the Contractor shall correct the identified deficiencies and resubmit the deliverable within a mutually agreed timeframe at no additional cost. A deliverable shall be considered accepted only upon written acceptance by the Procuring Entity's designated representative.

Change Control and Exit Requirements

Change Control. Any change to the scope, deliverables, or terms of this Scope of Work shall be made only through a written, mutually agreed change process. The Contractor shall not perform work outside the defined scope, or incur costs beyond those authorized, without prior written authorization from the Procuring Entity's designated representative. Each change request shall document the nature of the change, its rationale, and any impact on cost, schedule, or deliverables.

Transition and Exit. Upon expiration, termination, or non-renewal of the contract, the Contractor shall support an orderly transition of services to the Procuring Entity or its designated successor. Transition support shall include:

- Knowledge transfer of relevant operational, configuration, and procedural information;
- Delivery of current documentation, runbooks, reports, and records related to the services;
- Return or secure destruction of all Procuring Entity data and credentials in accordance with the Data Protection requirements;
- Revocation of the Contractor's access to Procuring Entity systems, facilities, and data;
- Reasonable cooperation to ensure continuity of security operations and no lapse in coverage during the transition.

The Contractor shall provide transition support for a period of up to 60 days following contract conclusion, as directed by the Procuring Entity.

Contractor Security and Subcontractor Requirements

Contractor Security. The Contractor shall ensure that all personnel assigned to the engagement meet the Procuring Entity's security and suitability requirements. The Contractor shall ensure that personnel execute any required confidentiality, nondisclosure, and acceptable-use agreements prior to accessing Procuring Entity systems or data. The Contractor shall promptly notify the Procuring Entity of any change in assigned personnel and shall revoke access for any personnel no longer supporting the engagement.

Subcontractor Requirements. The use of subcontractors is permitted only with the prior written approval of the Procuring Entity. The Contractor shall remain fully responsible for all work performed by subcontractors and for ensuring that subcontractors comply with all requirements of this Scope of Work, including the data protection, confidentiality, security, and performance requirements herein. The Contractor shall ensure that any subcontractor with access to Procuring Entity systems or data is bound by confidentiality and data-protection obligations no less restrictive than those imposed on the Contractor.

B. TECHNICAL SPECIFICATIONS

1. Organizational Experience

Offeror **must**:

a) provide a detailed description of relevant corporate experience with state government and private sector. The experience of all proposed subcontractors must be described. The narrative **must** thoroughly describe how the Offeror has supplied expertise for similar contracts and must include the extent of their experience, expertise and knowledge as a provider of managed cybersecurity services. All managed cybersecurity services provided to private sector will also be considered;

b) provide a detailed resume and bio of all key personnel Offeror proposes to use in performance of the resulting contract, should Offeror be awarded. Key personnel is identified as any individual the Offeror proposes to perform or directly oversee the services described in Section IV.A, Detailed Scope of Work — including, at minimum, the engagement/account lead, the lead security analyst(s) or security engineer(s) responsible for day-to-day hands-on operations, the incident response lead, and any individual serving in a strategic or advisory (vCISO-level) capacity. Offeror must include key personnel education, work experience, relevant/applicable certifications/licenses, and demonstrated, hands-on operational experience with the specific technologies and platforms identified in the Detailed Scope of Work (e.g., AWS, Fortinet, EDR, WAF, vulnerability management, and incident response).

c) describe at least two project successes and two project challenges of managed cybersecurity services engagements. Include how each experience improved the Offeror's services.

2. Organizational References

Three (3) external references from similar projects/programs, performed for private, state, or large local government clients within the last three (3) years should be received by the designee identified on APPENDIX F, Organizational Reference Questionnaire ("Questionnaire"). Any submitted references must be received by the deadline stated on APPENDIX F.

The references to whom the Offeror provides the Questionnaire **must submit the Questionnaire directly to the designee identified on APPENDIX F. The references must not return the completed Questionnaire to the Offeror.** It is the Offeror's responsibility to ensure the completed Questionnaires are submitted **on or before the deadline stated on APPENDIX F. NO LATE QUESTIONNAIRES CAN BE ACCEPTED.**

Offerors are encouraged to request that their chosen references provide detailed and informative comments.

The Offeror, itself, does not need to submit anything for this Specification in its proposal. The Offeror may, if it chooses, include a list of all organizations to whom Offeror sent the Organizational Reference Questionnaire (APPENDIX F).

3. Mandatory Specification

The following are mandatory requirements that relate to the core functions of the Scope of Work (Section IV.A). These specifications are pass/fail. An Offeror that cannot meet any one of the mandatory requirements will be deemed non-responsive and disqualified from award consideration. The Offeror must confirm its ability and willingness to perform each of the following:

M1. Provide continuous security operations and monitoring across a hybrid cloud and on-premises environment, including security event monitoring, alert triage, and escalation.

M2. Provide cybersecurity incident response, including detection, containment, eradication, and recovery, with 24/7/365 availability and committed response times based on incident severity.

M3. Manage a vulnerability and patch management program, including the patching platform and deployment process, risk-based prioritization, and remediation tracking to closure.

M4. Provide cloud security services for an Amazon Web Services (AWS) environment, including configuration review, identity and access management (IAM) review, and cloud security monitoring.

M5. Provide network and firewall security within a Fortinet environment, including security policy management, rule review, and network segmentation.

M6. Provide endpoint detection and response (EDR) security, including policy management, detection tuning, and alert investigation.

M7. Provide identity and access security, including access reviews, privileged account oversight, and multi-factor authentication (MFA) governance.

M8. Maintain the agency's security program in adherence to the NIST 800-53 controls framework, including control review, POA&M tracking, and audit support.

M9. Provide web application security, including protection and monitoring of hosted web applications and the pension administration system and its supporting infrastructure.

M10. Provide qualified personnel with demonstrated, hands-on operational experience across the agency's core security technologies; provide periodic onsite support at the agency's Santa Fe office to become familiar with the on-premises environment and collaborate with agency staff; and provide knowledge transfer to agency IT staff while the agency retains final governance authority.

M11. The respondent must have provided virtual Chief Information Security Officer (vCISO) services to at least three public pension organizations within the past five years. The assigned project lead must have experience providing vCISO services to a public pension organization. The assigned project team must have experience penetration testing releases of pension administration software.

4. Desirable Specification and Due Diligence Questions

The following specifications are not mandatory to perform the Detailed Scope of Work but are desirable. Offerors who demonstrate the following will be awarded additional points. Each specification corresponds to an Evaluation Factor in Section V.

D1. Experience securing a Pension Administration System (PAS) or comparable web-based retirement, benefits, or mission-critical public-facing financial platform, including protection of the application layer and sensitive member and financial data.

D2. Experience securing and managing Internet of Things (IoT) and physical security systems, such as access control systems and video surveillance (CCTV) infrastructure, including device assessment, segmentation, and hardening.

D3. Experience providing managed cybersecurity services to public sector agencies, government retirement or pension systems, or other regulated entities handling sensitive financial or member data.

D4. Relevant organizational and personnel certifications, such as CISSP, CCSP, CISA, CISM, AWS Certifications, Fortinet NSE, or GIAC credentials.

DUE DILIGENCE QUESTIONS

Questions regarding data protection and due diligence, Agency will require answers to data protection and due diligence questions on a semi-annual basis:

1. Describe your firm's disaster recovery plan as it relates to the equipment, software, data, and personnel that would be used in providing the services required by NMERB.

2. Does the organization routinely perform penetration tests utilizing a qualified third-party vendor, and if so, how often are tests performed and when was the last test performed?

3. What technical prevention measures are in place to secure and monitor your network?

4. Is multi-factor authentication utilized for network remote access? If so, what type of authentication?

5. How is data protected in transit between the vendor and NMERB and where is NMERB data stored (including geographic location and cloud provider)? Additionally, how is data at rest protected on servers and backup media? Describe the complete lifecycle of NMERB data, including collection, storage, transmission, backup, retention, access controls, sharing, and destruction.

6. Is there a formal security incident response program in place, and if so, how often is the incident response program tested? Do you have a Chief Information Security Officer and cybersecurity insurance? Describe your breach notification process, including notification timelines for incidents involving NMERB data.

7. Over the past five years, has your organization, your parent organization or any of its affiliates or any officer or principal been involved in any business litigation or regulatory proceedings? If so, provide an explanation and indicate the status of the action.

8. Describe employee training programs of your organization including software, security, cyber security, artificial intelligence, and technology training that would be used in providing the services required by NMERB.

9. Have you had a SOC 2, Type 2, audit conducted, and are you willing to share that report with NMERB?

10. How and where do you use Artificial Intelligence (AI), Generative AI, AI Agents,

or Model Context Protocol (MCP) integrations within your products, services, operations, or support processes? Do you maintain a formal AI governance policy and AI risk management process? If so, provide copies to NMERB.

11. Can your AI system access, modify, transmit or make decisions regarding pension member data without meaningful human review? Is NMERB data used to train AI models?

C. BUSINESS SPECIFICATIONS

1. Financial Stability

Offerors must submit copies of the most recent years independently audited financial statements and the most current 10K, as well as financial statements for the preceding three years, if they exist. The submission must include the audit opinion, the balance sheet, and statements of income, retained earnings, cash flows, and the notes to the financial statements. **If independently audited financial statements do not exist, Offeror must state the reason and, instead, submit sufficient information (e.g., D & B report). Failure to submit audited financial statements as described herein results in Offeror's disqualification.**

2. Letter of Transmittal Form

The Offeror's proposal **must** be accompanied by the Letter of Transmittal Form located in APPENDIX E. The form **must** be completed and must be signed by the person authorized to obligate the company. **Failure to submit a signed form will result in Offeror's disqualification.**

3. Campaign Contribution Disclosure Form

The Offeror must complete an unaltered Campaign Contribution Disclosure Form and submit a signed copy with the Offeror's proposal. This must be accomplished whether or not an applicable contribution has been made. (See APPENDIX B). **Failure to complete and return the signed, unaltered form will result in Offeror's disqualification.**

4. Oral Presentation

If oral presentations are held, finalist Offeror(s) may be required to explain, demonstrate, detail, and/or clarify any aspect of its submitted proposal, to which the Evaluation Committee may ask questions and/or seek clarifications. Pursuant to Section II.B.9, Oral Presentations may held at the sole discretion of the Evaluation Committee and may be virtual or in person.

5. Cost

Offerors must complete the Cost Response Form in APPENDIX D. Cost will be measured by

a. Please provide your fee structure as it pertains to this proposal. Cost should be broken down by the monthly and annual rate.

b. Please identify any additional charges you would impose for other specific services and/or research materials.

6. New Mexico/Native American Resident Preferences

To ensure application of § 13-1-21 NMSA 1978 (as amended), an Offeror **MUST** submit a copy, in this section, of its valid New Mexico/Native Resident Preference Certificate or its valid New Mexico/Native American Resident Veteran Preference Certificate, as issued by the New Mexico Taxation and Revenue Department.

V. EVALUATION

A. EVALUATION POINT SUMMARY

The following is a summary of evaluation factors with point values assigned to each. These weighted factors will be used in the evaluation of individual potential Offeror proposals

Evaluation Factors *(Correspond to Sections IV.B and IV.C)*	**Points Available**
B. Technical Specifications	
B. 1. Organizational Experience	325
B. 2. Organizational References	75
B. 3. Mandatory Specification	Pass/Fail
B. 4. Desirable Specification	300
C. Business Specifications	
C.1. Financial Stability	Pass/Fail
C.2. Letter Of Transmittal	Pass/Fail
C.3. Campaign Contribution Disclosure Form	Pass/Fail
C.4. Oral Presentations	100
C.5. Cost	200
TOTAL POINTS AVAILABLE	**1,000**
C.6. New Mexico / Native American Resident Preference	**80**
C.6. New Mexico / Native American Resident Veteran Preference Points per Section IV C.6	**100**

Table 1: Evaluation Point Summary

B. EVALUATION FACTORS

1. B.1 Organizational Experience (See Table 1)

Points will be awarded based on the thoroughness and clarity of Offeror's response in this Section. The Evaluation Committee will also weigh the relevancy and extent of Offeror's experience, expertise and knowledge; and of personnel education, experience and certifications/licenses. In addition, points will be awarded based on Offeror's candid and well-thought-out response to successes and failures, as well as the ability of the Offeror to learn from its failures and grow from its successes.

2. B.2 Organizational References (See Table 1)

Points will be awarded based upon an evaluation of the responses to the questions provided on the Questionnaire (APPENDIX F). Offeror will be evaluated on references that show positive service history, successful execution of services and evidence of satisfaction by each reference. References indicating significantly similar services/scopes of work and comments provided by a submitted reference will add weight and value to a recommendation during the evaluation process. Points will be awarded for each individual response up to 1/3 of the total points for this category. References not received by the stated deadline on

APPENDIX F will earn zero (0) points. For example: if two (2) references are received, the Offeror would only be eligible for a maximum of two-thirds (2/3) the total available points.

The Evaluation Committee may contact any or all business references for validation of information submitted. If this step is taken, the Procurement Manager and the Evaluation Committee must all be together on a conference call with the submitted reference so that the Procurement Manager and all members of the Evaluation Committee receive the same information at the same time.

3. B.3 Mandatory Specifications

The Mandatory Specification found in Section IV.B. are pass/fail. No points assigned.

4. B.4 Desirable Specifications

Evaluation of Desirable Specification will be based on full consideration of all information provided in response to Section IV.B.

5. C.1 Financial Stability (See Table 1)

Pass/Fail only. No points assigned.

If the required response is met by the submission, the evaluation committee will perform a review of the financial statements providing a financial opinion on the stability of the Offeror. If a review of the Offeror's financial statements clearly demonstrates that an Offeror is in bankruptcy proceedings to include any bankruptcy filings, the Offeror is not a Responsible Offeror under Section 13-1-83 NMSA 1978 and will not be considered for an award.

6. C.2 Letter of Transmittal (See Table 1)

Pass/Fail only. No points assigned.

7. C.3 Campaign Contribution Disclosure Form (See Table 1)

Pass/Fail only. No points assigned.

8. C.4 Oral Presentation (See Table 1)

Points will be awarded based on the quality, organization and effectiveness of communication of the information presented, as well as the professionalism of the presenters and technical knowledge of the proposed staff. Prior to Oral Presentation, Agency will provide the Offeror a presentation agenda. (If no Oral Presentations are held all Offerors will receive the maximum amount of total points for this Evaluation Factor).

9. C.5 Cost (See Table 1)

The evaluation of each Offeror's cost proposal will be conducted using the following formula

$$\frac{\text{Lowest Responsive Offeror's Cost}}{\text{Each Offeror's Cost}} \times \text{Available Award Points}$$

10. C.6. New Mexico/Native American Resident Preferences

Percentages will be determined based upon the point-based system outlined in § 13-1-21 NMSA 1978 (as amended).

A. **New Mexico Resident Business Preference / Native American Resident Preference**

If an Offeror has provided a copy of its New Mexico Resident Preference Certificate or Native American Resident Preference Certificate, the points awarded will be calculated as 8% of the total points available in this RFP.

B. **New Mexico/Native American Resident Veteran Preference**

If an Offeror has provided a copy of its New Mexico Resident Veteran Preference Certificate or Native American Resident Veteran Preference Certificate the points awarded will be calculated as 10% of the total points available in this RFP.

C. EVALUATION PROCESS

1. All Offeror proposals will be reviewed for compliance with the requirements and specifications stated within the RFP. Proposals deemed non-responsive will be eliminated from further consideration.

2. The Procurement Manager may contact the Offeror for clarification of the response as specified in Section II. B.6.

3. Responsive proposals will be evaluated on the factors in Section IV, which have been assigned a point value in Section V. The responsible Offerors with the highest scores may be selected as finalist Offerors, based upon the proposals submitted. In accordance with §13-1-117 NMSA 1978, the responsible Offerors whose proposals are most advantageous to the State taking into consideration the Evaluation Factors in Section V will be recommended for award (as specified in Section II.B.10). Please note, however, that a serious deficiency in the response to any one factor may be grounds for rejection regardless of overall score.

APPENDIX A

ACKNOWLEDGEMENT OF RECEIPT FORM

APPENDIX A

REQUEST FOR PROPOSAL

NMERB Request for Cybersecurity Managed Services
27-352-1116-02719

ACKNOWLEDGEMENT OF RECEIPT FORM

This optional Acknowledgement of Receipt Form establishes a distribution list to be used for the distribution of written responses to questions, and/or any amendments to the RFP. Failure to return the Acknowledgement of Receipt Form does not prohibit potential Offerors from submitting a response to this RFP. However, by not returning the Acknowledgement of Receipt Form, the potential Offeror's representative shall not be included on the distribution list and will be solely responsible for obtaining from the Procurement Library (Section I.G.) responses to written questions and any amendments to the RFP.

The information below will be used for all correspondence related to the Request for Proposal. Only one contact per Offeror is permitted.

ORGANIZATION: _____

CONTACT NAME: _____

TITLE: _____ PHONE NO.: _____

E-MAIL: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP CODE: _____

Submit Acknowledgement of Receipt Form to:
To: Felicia Sena
E-mail: Felicia.Sena@erb.nm.gov
Subject Line: NMERB Cybersecurity Managed Services, RFP# 27-352-1116-02719

APPENDIX B

CAMPAIGN CONTRIBUTION DISCLOSURE FORM

Pursuant to the Procurement Code, Sections 13-1-28, et seq. NMSA 1978 and § 13-1-191.1 NMSA 1978 (2006), as amended by Laws of 2007, Chapter 234, a prospective contractor subject to this section shall disclose all campaign contributions given by the prospective contractor or a family member or representative of the prospective contractor to an applicable public official of the state or a local public body during the two years prior to the date on which a proposal is submitted or, in the case of a sole source or small purchase contract, the two years prior to the date on which the contractor signs the contract, if the aggregate total of contributions given by the prospective contractor or a family member or representative of the prospective contractor to the public official exceeds two hundred fifty dollars ($250) over the two-year period. A prospective contractor submitting a disclosure statement pursuant to this section who has not contributed to an applicable public official, whose family members have not contributed to an applicable public official or whose representatives have not contributed to an applicable public official shall make a statement that no contribution was made.

A prospective contractor or a family member or representative of the prospective contractor shall not give a campaign contribution or other thing of value to an applicable public official or the applicable public official's employees during the pendency of the procurement process or during the pendency of negotiations for a sole source or small purchase contract.

Furthermore, a solicitation or proposed award for a proposed contract may be canceled pursuant to Section 13-1-181 NMSA 1978 or a contract that is executed may be ratified or terminated pursuant to Section 13-1-182 NMSA 1978 if a prospective contractor fails to submit a fully completed disclosure statement pursuant to this section; or a prospective contractor or family member or representative of the prospective contractor gives a campaign contribution or other thing of value to an applicable public official or the applicable public official's employees during the pendency of the procurement process.

The state agency or local public body that procures the services or items of tangible personal property shall indicate on the form the name or names of every applicable public official, if any, for which disclosure is required by a prospective contractor.

THIS FORM MUST BE INCLUDED IN THE REQUEST FOR PROPOSALS AND MUST BE FILED BY ANY PROSPECTIVE CONTRACTOR WHETHER OR NOT THEY, THEIR FAMILY MEMBER, OR THEIR REPRESENTATIVE HAS MADE ANY CONTRIBUTIONS SUBJECT TO DISCLOSURE.

The following definitions apply:

"**Applicable public official**" means a person elected to an office or a person appointed to complete a term of an elected office, who has the authority to award or influence the award of the contract for which the prospective contractor is submitting a competitive sealed proposal or who has the

authority to negotiate a sole source or small purchase contract that may be awarded without submission of a sealed competitive proposal.

"**Campaign Contribution**" means a gift, subscription, loan, advance or deposit of money or other thing of value, including the estimated value of an in-kind contribution, that is made to or received by an applicable public official or any person authorized to raise, collect or expend contributions on that official's behalf for the purpose of electing the official to statewide or local office. "Campaign Contribution" includes the payment of a debt incurred in an election campaign, but does not include the value of services provided without compensation or unreimbursed travel or other personal expenses of individuals who volunteer a portion or all of their time on behalf of a candidate or political committee, nor does it include the administrative or solicitation expenses of a political committee that are paid by an organization that sponsors the committee.

"**Family member**" means a spouse, father, mother, child, father-in-law, mother-in-law, daughter-in-law or son-in-law of (a) a prospective contractor, if the prospective contractor is a natural person; or (b) an owner of a prospective contractor;

"**Pendency of the procurement process**s" means the time period commencing with the public notice of the request for proposals and ending with the award of the contract or the cancellation of the request for proposals.

"**Prospective contractor**" means a person or business that is subject to the competitive sealed proposal process set forth in the Procurement Code [Sections 13-1-28 through 13-1-199 NMSA 1978] or is not required to submit a competitive sealed proposal because that person or business qualifies for a sole source or small purchase contract.

"**Representative of a prospective contractor**" means an officer or director of a corporation, a member or manager of a limited liability corporation, a partner of a partnership or a trustee of a trust of the prospective contractor.

Name(s) of Applicable Public Official(s) if any:_____

DISCLOSURE OF CONTRIBUTIONS BY PROSPECTIVE CONTRACTOR:

Contribution Made By: _____

Relation to Prospective Contractor: _____

Date Contribution(s) Made: _____
_____

Amount(s) of Contribution(s) _____
_____

Nature of Contribution(s) _____
_____

Purpose of Contribution(s) _____
_____

(Attach extra pages if necessary)

_____ _____
Signature Date

_____
Title (position)

--OR—

NO CONTRIBUTIONS IN THE AGGREGATE TOTAL OVER TWO HUNDRED FIFTY DOLLARS ($250) WERE MADE to an applicable public official by me, a family member or representative.

_____ _____
Signature Date

_____
Title (Position)

APPENDIX C

DRAFT CONTRACT

The Agreement included in this Appendix C represents the contract the Agency intends to use to make an award. The State of New Mexico and the Agency reserve the right to modify the Agreement prior to, or during, the award process, as necessary.

The contract template can be found at the following website under Contract and Amendment Templates titled AGENCY Large IT Agreement Form.

https://www.generalservices.state.nm.us/state-purchasing/contracts-review-bureau/

APPENDIX D

COST RESPONSE FORM

Use the format designated below to provide cost response:

a. Please provide your fee structure as it pertains to this proposal. Cost should be broken down by the monthly and annual rate.

b. Please identify any additional charges you would impose for other specific services and/or research materials.

Year 1	**Monthly**	**Annual (12 Months)**
Rate		
Gross Receipts Tax		
Total Fee		
Year 2		
Rate		
Gross Receipts Tax		
Total Fee		
Year 3		
Rate		
Gross Receipts Tax		
Total Fee		
Year 4		
Rate		
Gross Receipts Tax		
Total Fee		

APPENDIX E

LETTER OF TRANSMITTAL FORM

APPENDIX E
Letter of Transmittal Form

Please complete this form in its entirety. Failure to **sign and/or submit** this form will result in the disqualification of Offeror's proposal.

RFP#: 27-352-1116-02719

1. **Identify the following information for the submitting organization**:

Offeror Name	
Mailing Address	
Telephone	
FED TIN#	
NM BTIN#	

2. **Identify the individual(s) authorized by the organization to (A) contractually obligate, (B) negotiate, and/or (C) clarify/respond to queries on behalf of this Offeror**:

	A **Contractually Obligate**	**B** **Negotiate***	**C** **Clarify/Respond to Queries***
Name			
Title			
E-mail			
Telephone			

* If the individual identified in Column A also performs the functions identified in Columns B & C, then no response is required for those Columns. If separate individuals perform the functions in Columns B and/or C, they must be identified.

-

3. **Will any subcontractor/s be used in the performance of any resultant contract?** (Select one):
____ No.
____ Yes. Identify subcontractor/s: _____

4. **Will any other entity/-ies (such as a State Agency, reseller, etc., that is not a subcontractor identified in #3 above) be used in the performance of any resultant contract**? (Select one)
____ No.
____ Yes. Identify entity/-ies: _____

By signing the form below, the Authorized Signatory attests to the accuracy and veracity of the information provided on this form, and explicitly acknowledges the following:

- On behalf of the submitting-organization identified in item #1, above, I accept the Conditions Governing the Procurement, as required in Section II.C.1. of this RFP;
- I concur that submission of our proposal constitutes acceptance of the Evaluation Factors contained in Section V of this RFP; and
- I acknowledge receipt of any and all amendments to this RFP, if any.

Sign: _____ Date: _____
(*Must be signed by the individual identified in item #2.A, above*.)

APPENDIX F

ORGANIZATIONAL REFERENCE QUESTIONNAIRE

The State of New Mexico, as a part of the RFP process, requires Offerors to list a minimum of three (3) organizational references in their proposals. The purpose of these references is to document Offeror's experience relevant to the Section IV.A, Detailed Scope of Work in an effort to evaluate Offeror's ability to provide goods and/or services, performance under similar contracts, and ability to provide knowledgeable and experienced staffing.

Offeror is required to send the following Organizational Reference Questionnaire to each business reference listed in its proposal, as per Section IV.B.2. The business reference, if it chooses to respond, is required to submit its response to the Organizational Reference Questionnaire directly to: Felicia Sena at Felicia.Sena@erb.nm.gov no later than 3:00 pm MST on December 11, 2026, for inclusion in the evaluation process. The Questionnaire and information provided will become a part of the submitted proposal. Businesses/Organizations providing references may be contacted for validation of content provided therein.

RFP # 27-352-1116-02719

ORGANIZATIONAL REFERENCE QUESTIONNAIRE FOR:

Offeror, your name goes here

This form is being submitted to your company for completion as a reference for the organization listed above. Submit this Questionnaire to the New Mexico Educational Retirement Board via e-mail to:

Name: Felicia Sena, Procurement Manager
Email: Felicia.Sena@erb.nm.gov

Forms must be submitted no later than 3:00 pm MST on December 11, 2026, and **must not** be returned to the organization requesting the reference. References are **strongly encouraged** to provide thorough comments in response to the questions asked. The comments you provide will help the State of New Mexico evaluate the above-referenced Offeror's service history, successful execution of services, and evidence of customer/client satisfaction.

For questions or concerns regarding this form, please contact the State of New Mexico **Procurement Manager** at 505-531-6751 or Felicia.Sena@erb.nm.gov. When contacting the Procurement Manager, include the Request for Proposal number provided at the top of this page.

Organization providing reference	
Contact name and title/position	
Contact telephone number(s)	
Contact e-mail address	
Project/Service description	
Project/Service dates (start and end dates)	
Technical environment for the project your providing a reference (i.e., Software applications, Internet capabilities, Data communications, Network, Hardware);	

QUESTIONS:

1. In what capacity have you worked with [Offeror name] in the past?

2. How would you describe [Offeror name]'s knowledge and expertise?

3. How would you describe [Offeror name] flexibility relative to changes in the project scope and timelines?

4. How satisfied are you with the materials/documentation produced by [Offeror name]?

5. How would you describe the dynamics/interaction between [Offeror name]'s personnel and your staff?

6. By name, please identify who are/were [Offeror name]'s principal representatives involved in your project. How would you describe your satisfaction with each representative, individually? Please provide a brief comment on the skills, knowledge, behaviors, or other factors on which you based your satisfaction.

7. How satisfied are/were you with the services rendered and/or products developed by [Offeror name]? Please provide a brief explanation as to why you were or were not satisfied.

8. With which aspect(s) of [Offeror name]'s services are/were you most satisfied? Please provide a brief explanation as to why you were satisfied.

9. With which aspect(s) of [Offeror name]'s services are/were you least satisfied? Please provide a brief explanation as to why you were dissatisfied.

10. Would you recommend [Offeror name]'s services to your organization again? Why or why not?

11. Is there any other information you wish to share regarding [Offeror name]?