NEW MEXICO TECH
SCIENCE • ENGINEERING • RESEARCH UNIVERSITY

Purchasing Services Office
801 Leroy Place
Socorro, NM 87801
(575) 835-5881

Letter of Addendum

TO:	All Proposers	
FROM:	Kimela Miller, CPO	
DATE:	June 5, 2023	
RE:	RFP Number:	RFP# 2305011C
	Commodity:	virtual Information Security Officer (vISO)

Q1) Section 2.1 Approach, Page 5: Do you expect the vendor to provide dedicated primary and secondary CISOs?
A2) Require no, but it would be useful as most folks do take vacations. The same people each time would better as we'd need to start from nearly scratch each time we chatted.

Q2) Scope of Work, Page 12: Do you expect the VCISO to be based in the US, or can a global delivery model be utilized?
A2) The CISO must be a US citizen. All data must live in the US.

Q3) Scope of Work, Page 12, 13: Do you expect the vendor to assist NMIMT in implementing PCI DSS 4.0, FCI, GLBA, and CMMC 2.0 regulatory compliances?
A3) It depends on where you draw the line with the "assist NMIMT in implementing". Definitely provide guidance and examples of what does work and what will not work. The expertise is what we are looking for.

Q4) Scope of Work, Page 12, 13: Do you expect the vendor to propose a vulnerability scanning tool, or can they leverage NMIMT's current vulnerability scanning solution?
A4) They can recommend a tool or use what we currently use, if that is adequate.

Q5) Scope of Work, Page 12, 13: Do you have a security team? If yes, please provide information about the team's size and competencies.
A5) We are building our team, but require this service to complement us while we grow.

Q6) Scope of Work, Page 12, 13: How many vendors are included in the scope for third-party risk management?
A6) If you are referring to the vendor assessment, the catalog is incomplete, but 5 or more.

Q7) Scope of Work, Page 12, 13: Do you have a defined criteria for vendor risk management?
A7) That is still being developed.

Q8) Pg,12, Paragraphs 2 & 3: What is the anticipated amount of time NMIMT is looking to fill this role? Is the Institute seeking a part-time or full-time consultant over a set duration of time? If part-time, how many hours per week or month?
A8) We are unsure at this time. We do not expect a full FTE (40hrs a week), but there may be times that the person would need to put in quite a few hours and other times when they are not needed. You can quote flat-rate or hourly and we'll take that into account (flat-rate is always preferable as we can manage our costs better.)

Q9) Page 12, (table) Section NMIMT-002 - item 002.03 - *The vendor must sign Client Memorandum of Agreement or Interconnection Security Agreement prior to Contract Award*: Is this completed form required for this RFP submission? If so, please provide form.
A9) It is not required prior to submission, but would be required prior to final award.

Q10) Page 12, (table) Section NMIMT-003 – item 003.01 - *Vendor providing product and work must provide annual training on recognized and reported potential and actual user improvement, where applicable:* IS NMIMT expecting for offerors to provide security awareness training to all NMIMT employees? Does NMIMT have a platform to deliver training? If training is required, will the vendor be expected to track compliance or integrate with an existing Learning Management System?
A10) Not necessarily all, but appropriate if needed. We do not expect the vendor to track compliance, but if the vendor does that would be a point in their favor. The vendor may or may not provide a tool as part of the RFP.

Q11) Page 12, (table) Section NMIMT-004 – 004.02: Please clarify what the Institute means by "Contract Authority?" Is this required as part of the RFP submission?
A11) We must have a person that has the authority to execute the contract as a contact. This is not required for submission, but would be required if the RFP is awarded (and there is a contract).

Q12) Is there an incumbent who is currently providing these services? If yes, is the incumbent performing to the satisfaction of the New Mexico Institute of Mining and Technology (NMIMT)?
A12) NMIMT does use contractors for security services now, but not necessarily the same as this request.

Q13) Is the incumbent eligible to offer on this contract?
A13) Any contractor is eligible to offer on this including any NMIMT may be currently using.

Q14) Is there a reason for considering the replacement of the incumbent?
A14) This RFP process is required due to the expected cost of the services and length of term for the services. State procurement requirements require a RFP.

Q15) Can offshore personnel (outside the United States) work on this project?
A15) Data must be kept on US Soil and the work needs to be done by US Citizens.

Q16) Is there a budget for this project?
A16) Yes

Q17) Are you able to provide the budget estimate?
A17) No. Please offer your lowest price.

Q18) The Evaluation Criteria section 4.1.1 4.0 states the services will be remote. Can you clarify if the entire project will be done remotely?
A18) Depending on the service some may require on premise actions but that is not expected for this.

Q19) If any services are expected to be performed onsite, please describe the frequency of onsite visits.
A19) None currently expected.

Q20) The Evaluation Criteria section 4.1.1 4.0 states that in-state veterans will be preferred. Will there be any preference given to out-of-state veteran personnel?
A21) Only preference can be given to New Mexico residents and veterans who are registered with the New Mexico Taxation and Revenue.

Q21) Is there a template to use for pricing?
A21) As long as the pricing is clear for the services rendered, that is sufficient. It must be clear what is included and what would be additional costs.

Q22) Should pricing be submitted separately?
A22) It should be included with the offer, but easily separated for the purposes of evaluation. Ex. Not interspersed throughout the offer.

Q23) Did NMIMT receive 3rd party assistance in preparing this RFP?
A23) No.

Q24) Will IT/information security policies need to be drafted from scratch, or do existing policies require updates/development?
A24) Both.

Q25) Please provide a list of NMIMT's current information security policies, if allowed. Alternatively, please give the total count of existing information security policies if you cannot provide a list.
A25) This is difficult to answer as we are not sure of the final count. We are very light on official policies.

Q26) Is a CMMC assessment in scope?
A26) This is not an assessment, the service may aid NMIMT in an assessment.

Q27) Is CMMC readiness consulting in scope? Perhaps.
A27) CMMC or similar is a concern for NMIMT as many groups are modeling requirements similar to CMMC.

Q28) What are the security tools currently deployed at NMIMT?
A28) We will not discuss our current security poster. We may do so with the contracted firm.

Q29) Do you follow a specific security framework currently?
A29) We will not discuss our current security poster. We may do so with the contracted firm.

Q30) Can my firm submit a copy of its SOC 3 report in lieu of a SOC 2 report?
A30) You can initially and we understand why you may not want to submit an SOC2 without an NDA. If we want to fully consider your company we shall need the SOC3.

Q31) What are the most important expectations you have for a security partner?
A31) All aspects of the partnership would be important, as expected.

Q32) What are your top requirements for the solution provider you choose which will set them apart from other bidders?
A32) The requirements are stated within the RFP.

Q33) How is success defined for this project?
A33) Performance of the items within the RFP.

Q34) Who are the key stakeholders for this project?
A34) There will be different stakeholders based on the different phases of the projects. The primary contact will be the IT department of NMIMT.

Q35) Are you looking for managed services as part of the proposal? Not necessarily, but if you feel it to be important as part of your offer, your group may offer it.

Q36) Will your team require training for the proposed solution?
36A) That depends on the solution. I cannot answer that more directly.

Q37) Is this the first time you will contract a vendor(s) for the services in question? If not, would a copy of the final contract, amount, and hourly rates of the previous successful vendor(s) be available?
A37) This specific service is not under contract currently. This RFP is the first for this type of IT service. Some security services have been done, but not exactly like this.

Q38) Are wet signatures required, or will digital signatures suffice?
A38) Only wet signatures, no digital will be accepted.

Q39) May we submit a redacted copy of our response for public inspection under the Freedom of Information Act ("FOIA")?
A39) We require a complete un-redacted copy. Should we receive a request for information, we will work with the vendor to redact info at that time. If you wish to send a redacted copy along with the un-redacted copy you may.

All other terms and conditions of the RFP remain unchanged.

ALL Offerors are required to confirm the receipt of this amendment in their offer.

Xc: File