STATE OF ALASKA

Department of Military and Veterans Affairs
Division of Administrative Services

STATEWIDE CYBERSECURITY PLAN

RFP 250000010

Amendment 1

March 27, 2025

This amendment is being issued for informational purposes only. The contents of this amendment will contain questions and answers. This document does not need to be returned with your proposal.

Important Note to Offerors: You must sign and return this page of the amendment document with your proposal. Failure to do so may result in the rejection of your proposal. Only the RFP terms and conditions referenced in this amendment are being changed. All other terms and conditions of the RFP remain the same.

Jannah Cayetano

Jannah Cayetano
Procurement Specialist 3
Phone: (907) 428-7222
Email: MvaDasProcurement@alaska.gov

_____
COMPANY SUBMITTING PROPOSAL

_____
AUTHORIZED SIGNATURE

_____
DATE

Questions submitted by potential offerors and answers from the state:

Question 1: Dave will briefly explain the project details.

Answer: We are looking to update our Statewide Cybersecurity Plan as an emergency management coordinated type of plan. The plan should include the two brand new annexes – an Emergency Management Response Annex working through Division of Homeland Security and Emergency Management (DHSEM) and Office of Information Technology (OIT), and the second annex is an Information and Intelligence Sharing Annex which will be set up for all State of Alaska's agencies to participate. We're keeping it open to allow private critical infrastructure partners to access and utilize this plan if needed.

Question 2: Can we have a copy of the recorded meeting?

Answer: Yes, please reach out to MvaDasProcurement@alaska.gov if you would like to obtain a copy of today's meeting.

Question 3: Can you clarify which state agencies are in scope of this project?

Answer: This is required for all State of Alaska agencies to follow.

Question 4: Do you know how many IT policies and procedures are in scope for review?

Answer: It will be for all the Internet Service Provider (ISP) for State of Alaska.

Question 5: Are there specific statewide set of policies or are they specific to each agency?

Answer: It will be for state level ISP set, not the specific departmental set.

Question 6: Do you have a comprehensive business continuity plan in place or are you seeking to develop one for this project?

Answer: Each department manages its own continuity planning. Our department has a plan in place, which includes the State Emergency Operation Center (SEOC) to be used in the event of an attack.

Question 7: Will you be providing details about your IT environment that would help us with pricing? Specifically, what technologies are included in the risk assessment scope, such as the number of firewalls, IP addresses, or anything that you can tell us about the technology you use?

Answer: We will provide all the information that is required and available.

Question 8: Do you have a Security Information and Event Management (SIEM) in place?

Answer: Yes, we do.

Question 9: Are you using any intrusion detection prevention solutions?

Answer: Yes, we have Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology.

Question 10: Will you be providing some details about the cyber threat intelligence training sessions and drills that you're looking for?

Answer: I expect that those details will likely to be flushed out more thoroughly after the award. It would be tabletop type of training/drills.

Question 11: How many tabletop exercises are you expecting and how many agencies would be involved in this?

Answer: At least twice a year, potentially quarterly. The agencies involved would depend on the tabletop exercise and its scope.

Question 12: Do you have to be a registered business in Alaska to provide services for this contract?

Answer: No; however, if you are the selected awardee, you must obtain an Alaska Business License before signing the contract.

Question 13: Are there any specific constraints or deadlines for the project's completion that we should keep in mind?

Answer: Other than completion dates specified by the RFP process, we are not aware of any specific constraints or deadlines for the project's completion. This work is required and related to SLGCP funding so there may be federal requirements related to this that should be considered.

Question 14: What level of access will be provided to current documentation and cybersecurity infrastructure during the project?

Answer: Under the appropriate non-disclosure and confidentiality agreements, the selected vendor will be provided with access to system documentation and cybersecurity infrastructure to perform their duties under the scope of work.

Question 15: Are there any specific communication tools or platforms preferred for managing project collaboration and updates?

Answer: SOA currently uses Microsoft G5 licensing and M365 for communications related to business activities. That environment will be the basis for managing project collaboration and updates.

Question 16: Is there an existing list of critical assets and systems, or will this need to be developed from scratch?

Answer: There is a comprehensive list of critical assets and systems.

Question 17: Are there historical cybersecurity incidents or threats that should be reviewed as part of the risk assessment?

Answer: No. Historical cybersecurity incidents should be considered independent of updating the State Cybersecurity Plan. If they are deemed relevant to developing the plan, they will be shared with the selected vendor at that time.

Question 18: Are there particular state or federal compliance requirements that need additional emphasis in the updated plan?

Answer: The State of Alaska deals with a wide variety of regulatory compliance regimes. For example: CJIS, FTI, FERPA, HIPAA, etc. All of these should be considered in the development of a state level cybersecurity plan.

Question 19: Could you provide specific details on the existing performance metrics and benchmarks used to evaluate cybersecurity efforts?

Answer: Best practice cybersecurity performance metrics should be the focus for evaluating cybersecurity efforts.

Question 20: Are there pre-existing incident response protocols that should be integrated or replaced in the new annex?

Answer: Need clarification for the reference to pre-existing incident response protocols.

Question 21: What kinds of scenarios should table-top exercises simulate (e.g., ransomware, phishing attacks, etc.)?

Answer: Table-top exercises should include items such as ransomware, phishing and social engineering, insider threats, data breach response, and supply chain attacks. This is not a comprehensive list, and the selected vendor should work with SOA to determine the most appropriate table-top exercises to incorporate into any plan.

Question 22: Are there any privacy concerns or regulatory limitations related to sharing cyber intelligence data?

Answer: Yes. Potentially would depend on who it is being shared with.

Question 23: Will third-party tools or platforms for information sharing be integrated into the annex?

Answer: Need clarification for this question. We do currently utilize third-party tools to receive security related information. We do not have any current third-party tools for sharing information with others.

Question 24: What is the target audience size for the training sessions, and are there specific training outcomes expected?

Answer: Undetermined. Submitting vendors should evaluate the organizational structure of SOA and determine what they believe the training session audience and outcome specifics should be.

Question 25: Should the training materials be designed for multiple proficiency levels (beginner, intermediate, expert)?

Answer: Yes. We would expect that all proficiency levels could be brought into training and that it would incorporate elements that would benefit all levels.

Question 26: Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?

Answer: The Department of Military Veterans Affairs, Division of Administrative Services, Procurement section does not have a recorded contract on file for this service.

Question 27: Specify the VLAN details how many are included in the Scope?

Answer: This will not be shared until a vendor is selected and if it is deemed relevant to completion of the State Cybersecurity Plan.

Question 28: Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

Answer: This will not be shared until a vendor is selected and if it is deemed relevant to completion of the State Cybersecurity Plan.

Question 29: How much (%) of the infrastructure is in the cloud?

Answer: This will not be shared until a vendor is selected and if it is deemed relevant to completion of the State Cybersecurity Plan.

Question 30: In the IT department/environment, how many employees work?

Answer: This is not pertained to the RFP.

Question 31: Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Answer: SOA primarily utilizes 3rd-party datacenter services.

Question 32: Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

Answer: Per the RFP it is up to $150,000.

Question 33: Can we submit the proposals electronically?

Answer: Yes, please send your proposals to MvaDasProcurement@alaska.gov.

Changes to the RFP:

Change 1: The new Deadline for Receipt of Proposals is **April 8, 2025**, at **2:00 P.M**. AKST. Late proposals will not be accepted.

-END OF ATTACHMENT 1-