STATE OF ALASKA

Department of Military and Veterans Affairs
Division of Administrative Services

STATEWIDE CYBERSECURITY PLAN

RFP 250000010

Amendment 2

April 1, 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: How many endpoints (servers, workstations, laptops, mobile devices, etc.) will be included within the scope of the assessment?

Answer: No assessment is required. The scope of section 2 will be outlining how to perform an assessment.

Question 2: Could you provide an overview of the current IT infrastructure — is it primarily on-premises, cloud-based, or a hybrid environment.

Answer: Hybrid environment.

Question 3: What is the total number of internal and external IP addresses, systems, and applications that will be included in the VAPT scope?

Answer: This will be discussed with the awardee after the contract is awarded, however there is no assessment needed.

Question 4: Are there any cloud-based assets, SaaS applications, or hybrid environments that should be included in the testing?

Answer: This will be discussed with the awardee after the contract is awarded, however there is no assessment needed.

Question 5: Should the penetration test focus on network infrastructure, web applications, APIs, wireless networks, mobile applications, or all of the above

Answer: This will be discussed with the awardee after the contract is awarded, however there is no assessment needed.

Question 6: Does the state require both unauthenticated (black-box) and authenticated (gray-box or white-box) testing for applications and systems?

Answer: This will be discussed with the awardee after the contract is awarded.

Question 7: Should social engineering (e.g., phishing, pretexting, USB drops) be included in the penetration testing scope?

Answer: For training yes, they should be included, but no assessment is needed.

Question 8: Does the State require testing to be conducted outside of business hours to minimize disruption to critical systems?

Answer: Not applicable.

Question 9: How many state agencies will participate in the project and training?

Answer: Undetermined.

Question 10: How many representatives from Alaska's Cyber Group will participate in the project and training?

Answer: Undetermined.

Question 11: How many local, regional, and tribal governments will participate in the project and training?

Answer: Undetermined.

Question 12: How many state agencies are in scope for the Cybersecurity Risk Assessment?

Answer: No assessments are required; Task 2 will be outlining how to conduct an assessment.

Question 13: Should the Cybersecurity Risk Assessment be aligned with a framework, such as NIST SP 800-30?

Answer: No assessment required.

Question 14: When was the last time a Cybersecurity Risk Assessment of this nature was performed?

Answer: No assessment required.

Question 15: Are the State's policies and procedures aligned with a security/control framework, such as NIST SP 800-53?

Answer: This will be discussed with the awardee after the contract is awarded.

Question 16: How many agencies are included in the Cybersecurity Risk Assessment? Do all agencies rely on the State for IT services, or do they have their own IT infrastructures?

Answer: It will cover all agencies on a state level. Some agencies have their own IT, this can be discussed on award of contract.

Question 17: How many data centers and other physical facilities are in scope for the assessment?

Answer: No assessment is required; Task 2 is to outline how an assessment would be conducted.

Question 18: When was Annex W: Cybersecurity Incidents (within the State's Emergency Operations Plan) last reviewed and updated?

Answer: 2 years ago.

Question 19: Task 4, Cybersecurity Response Annex Development, requires the vendor to "integrate tabletop exercises and simulations within the annex to test response protocols." Is the vendor expected to lead tabletop exercises or simply provide a framework for the State to conduct these exercises internally? If it is the former, how frequent should the exercises be?

Answer: Provide framework for quarterly TTX.

Question 20: If the vendor is leading the tabletop exercises in Task 4, is it the State's expectation that the exercises will be on site? How many participants will there be?

Answer: Not applicable.

Question 21: With approximately how many external agencies and other entities will the State share threat intelligence information?

Answer: Approximately 20.

Question 22: Task 5, Development of the Intelligence, and Information Sharing Annex, requires that the vendor "implement training programs for agency personnel." Is the vendor expected to host a computer-based training platform, provide training content that can be integrated into the State's learning management system (LMS), or provide recommendations only?

Answer: Provide training to be implemented in regard to exercising the plan.

Question 23: Task 5 also requires tabletop exercises that simulate threat intelligence sharing across agencies during a cyber-attack. What is the expected frequency and of these exercises, annually or biannually?

Answer: Quarterly.

Question 24: Does the State want the tabletop exercises in Task 5 delivered on site? Approximately how many participants will there be?

Answer: Undetermined, vendor can choose what is best by their own assessment.

Question 25: For Task 6, Training and Stakeholder Engagement, how many training sessions are expected? How long should each session be, and how many participants?

Answer: Training should be on a quarterly basis and based on the vendor's guidance for length and participation numbers.

Question 26: Will you consider extending the deadline by two weeks to allow time for vendors to develop a thorough and compliant response?

Answer: The Amendment 1 was issued to answer questions from interested offerors and extend the deadline to April 8, 2025, at 2:00 p.m. AKST.

Question 27: How many other departments does the State envision being involved in the engagement?

Answer: Undetermined.

Question 28: Is the assessment and required deliverables to be focused on IT or will department specific plans need to be also created?

Answer: Focused on the state level, no department plans are required.

Question 29: What is the expected duration of the engagement?

Answer: This information is available on the RFP document SEC 3.02 CONTRACT TERM AND WORK SCHEDULE.

Question 30: Who has the State designated as the project sponsor?

Answer: The Department of Military and Veterans Affairs, Division of Homeland Security and Emergency Management.

Question 31: For the proposal formatting, do the responses have to be in the submittal form boxes that are provided in the RFP, or can the responder use their own template following the page limit requirements?

Answer: The vendor can use their own template following the page limit requirements.

-END OF ATTACHMENT 2-