DIVISION OF LEGISLATIVE AUDIT
RFP NUMBER 26-33-03
AMENDMENT NUMBER 2

Division of Legislative Audit
Attn: JC Kestel
State Capitol, 120 4th Street, Room 3
Juneau, AK 99801-1182

RFP TITLE: RFP 26-33-03 – Cyber Security Assessments of Select State IT Systems

RFP CLOSING DATE & TIME: 2:00PM Alaska Time on March 31, 2026

DATE AMENDMENT ISSUED: Monday, March 23, 2026

The following changes/additions/clarifications are made to the RFP:

A) The following questions were received from potential offerors.

1. *MyAlaska assessment boundary*
   For MyAlaska, when the State references a single IP, single subdomain, and single API set, does that include or exclude any WAF/CDN, load balancers, administrative paths, health endpoints, or other auxiliary public-facing components? Also, should all six production servers be considered in scope for assessment activity?

   Response: All six production servers are in scope. It does not include other components listed. Also see responses to questions 21 and 41 of this Amendment.

2. *Testing mechanics and authenticated access*
   Will the State provide test accounts, role-based credentials, seeded test data, allowlisting, and approved test windows for MyAlaska and the other in-scope public-facing systems?

   Response: Specific approaches to testing will be discussed at the entrance conference with each department; however, it is safe for Potential Offerors to assume that department officials will provide access to necessary information or accounts to perform the Scope of Work detailed in Section 5 (Scope of Work) of the RFP.

3. *Testing depth for systems other than MyAlaska*
   For New DAIS and the MyRnB / Employer Services / eReporting family, should offerors

assume vulnerability assessment and control validation only, or is manual exploitation expected where safely authorized?

Response: The RFP includes penetration testing where exploitation is expected, in alignment with other provisions around minimizing impacts to production environments detailed in paragraph 5.04 (Activities Excluded From Scope of Work) and coordination requirements detailed in paragraphs 5.02 (Scope of Work General Requirements) and 5.03 (Scope of Work – Specific Requirements). The RFP also includes vulnerability assessment and control validation within the Scope of Work.

4. *New DAIS timing*
   For New DAIS, what post-go-live stabilization window should offerors assume for the assessment? In addition, if the planned July 1, 2026 deployment changes, how should offerors assume the assessment schedule will be adjusted?

   Response: If unforeseen circumstances arise, DLA and contractor can arrange mutually agreeable modifications to the planned Scope of Work. For example, if the proposed July 1, 2026, deployment is significantly delayed, the assessment can be performed on existing pre-production environments with DLA approval. The post-go-live stabilization should be assumed to be 10 days or less for Potential Offerors proposals. Early testing may be available during this window, depending on conditions at the launch and coordination with department officials.

5. *Azure control boundary*
   For Azure, should the assessment be limited to subscription-level controls directly supporting the in-scope applications, or should it also include shared tenant-level IAM, logging, network, and security services that materially support those systems?

   Response: For Azure testing, testing tenant level controls would be appropriate as long as those controls are tied to NIST or CIS standards and relate to the Scope of Work detailed in Section 5 (Scope of Work) of the RFP.

6. *Evidence access model*
   By workstream, should offerors assume evidence will be provided through exports, read-only portal access, screen sharing, onsite observation, or vendor-mediated walkthroughs? If possible, it would be helpful to understand which areas may allow direct read-only access versus interview-based or document-based evidence collection.

   Response: Those details will be discussed at the entrance conference with department officials detailed in paragraphs 5.02 (Scope of Work General Requirements) and 5.03 (Scope of Work – Specific Requirements) of the RFP. DLA does not have a specific breakdown. Potential Offerors should assume a mix of various sources of evidence in their proposal.

7. *Vendor-managed environments*
   Will Wostmann & Associates and Applied Microsystems participate directly in interviews and evidence walkthroughs for the systems they support?

   Response: DLA expects State of Alaska Officials to be the primary source for answers to questions from the Successful Offeror; however, depending on the specific system and other factors, it may involve vendors needed to operate the system.

8. *Security awareness / phishing scope*
   Should the statewide security awareness and phishing component be treated as a policy and program review only, or should offerors assume sampling of execution, reporting, and performance metrics beyond the listed in-scope application families?

   Response: This requirement is a policy and program review.

9. *Physical security scope*
   How many facilities, data center locations, or recovery sites should offerors assume are in scope for physical security review, and are there any access constraints or blackout periods in Juneau or Anchorage that should be factored into planning?

   Response: The on-premises data center is located in Juneau. Blackout dates for intrusive testing include August 2nd to September 1st and September 13th to October 24th. Blackout dates do not prohibit non-intrusive testing that will have minimal impact to systems. Potential Offerors should plan to avoid September blackout dates given timelines detailed in paragraph 1.04 (Contract Term and Work Schedule) of the RFP. DLA and department staff have offices in Juneau and Anchorage; the precise number of visits is dependent upon the Sucessful Offerors' work plan. See answer to question 4 of this Amendment regarding New DAIS.

10. *Data handling expectations*
    May the contractor use a U.S.-hosted encrypted evidence repository for project materials, or must all evidence and deliverables remain solely within DLA-approved State-managed platforms?

    Response: The Successful Offeror can use their own secure platform provided it meets the baseline requirements outlined in State of Alaska security policy and the requirements specified in paragraph 5.02 (Scope of Work General Requirements) of the RFP and retention requirements noted in paragraph 1.28 (Ownership and Reuse of Documents) of the RFP.

11. *Pricing allocation expectations*
    Where pricing is requested by system or workstream, how would the State prefer offerors allocate shared project management, quality assurance, reporting, travel, and shared-control assessment effort across those pricing lines?

Response: Potential Offerors should review paragraphs 6.03 (Offeror's Schedule of Professional Hours and Fees) and 6.04 (Offeror's Total Cost Statement) when they prepare their Cost Proposal.

12. *Reporting structure*
Should offerors assume a single consolidated reporting package coordinated through DLA, or multiple tailored reporting packages for separate departments, divisions, or stakeholder groups?

Response: The final report should be consolidated through DLA. Additionally, sufficient information on department specific findings, format and content approved by DLA, will be necessary to communicate findings effectively to each department.

13. *Budget / funding requirements*
We did not identify a disclosed operating budget, not-to-exceed amount, target funding range, or any specific budgetary constraints in the RFP materials. If the State is able to share any budget parameters, funding ceiling, or cost expectations for this effort, that would help offerors align scope, staffing, and pricing appropriately.

Response: A budget has not been set.

14. *Page 33 of the RFP states that the project team must include a Certified Information Systems Security Professional (CISSP) and a Certified Cloud Security Professional (CCSP). If the project team does not have a CCSP, would other cloud services certifications, like Azure, be sufficent?*

Response: Yes, DLA will accept any cloud services certifications related to Azure and Oracle to meet the CSSP requirements. Other certifications requirements detailed in the RFP remain in place.

15. *Will the State provide current inventories/diagrams per application upfront, or are we building these from scratch?*

Response: DLA has some system inventory information that can be shared and departments will have additional information that can be provided. The Successful Offeror will not be starting from scratch.

16. *Are there any automated asset management mechanisms we can leverage (e.g., CMDB)?*

Response: DLA is aware that Transition Manager was in use as of 2025, but department staff can confirm if other tools are in use during the entrance conference.

17. *Is there a desired Implementation Group (IG) for the CIS Control framework?*

Response: All three implementation groups should be evaluated.

18. *Does the State have a risk prioritization methodology in place?*

    Response: Risk prioritization follows NIST 800-53 Rev. 5 controls to inform internal risk prioritization processes at the enterprise level.

19. *Is there a GRC tool in place?*

    Response: There is no GRC tool in place at the enterprise level. Departments can address specific additional questions relating to GRC tools during the entrance conference.

20. *How many IP addresses are in-scope for both Internal and External?*

    Response: New DAIS has two IPs, while MyPDF Info, Online Filing, and RPFI have six IPs and myAlaska has six internal IPs. MyRnB, Employer Services, and eReporting has approximately ten IPs.

21. *Will you provide current-state network diagrams (on-prem & cloud) and security standards up front, or should the assessment include diagram reconstruction?*

    Response: DLA can provide a network diagram for myAlaska after the contract is signed. Department staff can address current-state network diagrams for other systems during the entrance conference. State of Alaska Security standards can be provided to the Successful Offeror upon contract award.

22. *Will configuration reviews (e.g., firewall rules, IDS/IPS policies, VPN, SSO/MFA configs) expected? Or can this remain interview-based?*

    Response: This can be interview-based with supporting evidence. For example, if the control requires Multi-Factor Authentication (MFA) the team should validate the MFA control is in place but does not need to evaluate if this is the best configuration or solution for MFA. During the penetration test, the Successful Offerors' team would be expected to attempt to exploit poor configurations of various controls.

23. *Please provide the list of security tools to be assessed.*

    Response: The State of Alaska enterprise has several tools including, but not limited to, Defender, Sentinel, Rapid 7, and Zscaler. These tools are leveraged at the enterprise level to provide information such as log monitoring and vulnerability detection. Departments can provide additional information about security tools during the entrance conference.

24. *Which data classes / data privacy regulations apply? (e.g., PII, ePHI, CJIS)*

    Response: The systems include PII and ePHI.

25. *Should we conduct evidence collection to test data lifecycle trace (collection → use → share → retain → dispose) for each application? Or is this interview based?*

Response: For data life cycle, this can be interview-based with supporting evidence; however, a full data life cycle trace is not required for the Scope of Work. For example, confirming backup procedures are in place and processing, but not validating the backup data can restore the system.

26. *Is there a cloud security tool in place to leverage configuration scan reports?*

Response: Yes, the State of Alaska Enterprise uses tools to scan cloud configurations and provide reports on vulnerable configurations. The Successful Offeror can request this information during the entrance conference.

27. *Are there data residency constraints (regions) or Sovereign Cloud requirements we must verify against contracts/policy?*

Response: Yes, see paragraph 5.03(J.) (Cloud Security Assessment) of the RFP.

28. *How many sites (datacenters, offices, third-party facilities) require visits?*

Response: The Successful Offeror should expect to visit department offices in Anchorage and Juneau. Please review response to question 9 for Datacenters. Good coordination and planning will yield the most efficient use of time.

29. *Are the sites operated and managed by the State or a third party?*

Response: It depends on the system, but generally speaking the State of Alaska uses a combination of state hosted systems and cloud hosted systems. See paragraph 4.01 (Select State IT Systems) of the RFP for additional information.

30. *Which tooling is in scope (SIEM, EDR, NDR, cloud-native logs) and can we access use case inventories, parsers, and retention settings?*

Response: All the identified tools would be in scope. The State Security Office can provide detail as necessary at the entrance conference.

31. *Do you want hands-on validation (log generation to alert) for a sampled use case set, or interview based review only?*

Response: Interview-based with supporting evidence should be sufficient to address paragraph 5.03(N.)(Monitoring and Logging). Hands-on validation would provide a better-quality evaluation but may not be necessary for the Sucessful Offeror to reach a conclusion about the adequacy of monitoring and logging controls.

32. *Is there a vendor inventory list in place? How many vendors?*

Response: DLA does not have a vendor inventory list. Known vendors were included in response to question xiii in Amendment No. 1 of the RFP that was issued on March 12,

2026, but that list is not necessarily comprehensive. This topic can be addressed further at the entrance conference with departments.

33. *Are we expected to actually conduct the third party risk assessments? Or look at the efficacy of the program?*

    Response: The Scope of Work is to review the efficacy of the program.

34. *Is there a third party risk management tool in place?*

    Response: The State of Alaska does not have an enterprise third-party risk management tool in place. This topic can be addressed further at the entrance conference with departments.

35. *Has the State conducted a Business Impact Analysis (BIA) that encompasses the in-scope applications?*

    Response: The State of Alaska has not conducted an enterprise Business Impact Analysis for these systems. This topic can be addressed further at the entrance conference with departments.

36. *Do you require RTO/RPO validation against actual system capabilities (backup/restore timing, failover tests), or a policy-to-practice gap analysis only?*

    Response: A policy-to-practice gap analysis.

37. *Will DLA accept a proposal from a vendor that does not include a Certified Cloud Security Professional (CCSP)? If not, what other certifications may be sufficient as a replacement alternative to the CCSP?*

    Response: Please response to question 15 of this Amendment.

38. *Approximately, how many live IP addresses should we expect to be in scope of the external penetration testing associated with the three state systems listed in Section 4 of the RFP?*

    Response: New DAIS has two IPs, while MyPDF Info, Online Filing, and RPFI have six IPs and myAlaska has six internal IPs. MyRnB, Employer Services, and eReporting has approximately ten IPs.

39. *For each of the applications listed that are in scope, can you please provide for each of them the following:*
    - *Estimated number of static pages*
    - *Estimate number of dynamic pages*
    - *Estimated number of API endpoints*
    - *Number of user roles that will be tested*
    - *Will DLA provide full API/route documentation?*

Response: DLA or department officials will provide the necessary API information to perform this work after contract is awarded. DLA does not know the exact number of user roles that will be tested, but as noted in paragraph 5.03(H.) (Identity and Access Management (IAM) Report) of the RFP, Identity and Access Management, the Successful Offeror should evaluate at least privileged and non-privileged accounts.

The following estimates may differ from actual counts.

New DAIS, Online Filing, MyPFD Info, RPFI do not have any static pages. These systems have approximately 150 dynamic pages and 675 API end points, with the vast majority of each within New DAIS. For myAlaska, there is estimated to be fewer than 20 total static and dynamic pages and fewer than 20 API endpoints. DLA estimates MyRnB, Employer Services, and eReporting have a similar number of pages as New DAIS and myAlaska. MyRnB does not provide any APIs but does consume them from Oracle WebCenter Content and Spaces.

40. *Approximately how many individuals involved with the administration of the three systems in scope will require interviews?*

Response: DLA anticipates up to a dozen individuals will participate in interviews per department, but the actual number may differ, and some interviews may involve multiple staff at the same time.

41. *What would be the timing for the formal presentations of the final report?*

Response: This has not been determined and depends on the meeting availability of the Legislative Budget and Audit Committee and other legislative committees.

42. *Is there a particular budget amount that the vendor should keep in mind?*

Response: Potential Offerors should review the response to question 13 of this Amendment.

This space was intentionally left blank.

DIVISION OF LEGISLATIVE AUDIT
RFP NUMBER 26-33-03
AMENDMENT NUMBER 2

B) All other terms and conditions of RFP 26-33-03, as amended, will remain as written.

A signed copy of this amendment and any others issued, in addition to your proposal, must be received by the issuing office prior to the closing date and time for your proposal to be considered responsive.

JC Kestel, Procurement Manager
PHONE: (907) 465-6705
TTY: (907) 465-4980
EMAIL:LAA.Procurement@AKLeg.gov

_____
NAME OF COMPANY

_____
AUTHORIZED SIGNATURE

_____
TITLE

_____
PRINTED NAME

_____
DATE