DIVISION OF LEGISLATIVE AUDIT
RFP NUMBER 26-33-03
AMENDMENT NUMBER 1

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: Thursday, March 12, 2026

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

1. The following questions were received from potential offerors.

i. *How many servers, endpoints, databases, and network devices are included in the supporting infrastructure for each of the three in-scope applications?*

Response: The myAlaska production environment has 6 servers.

The New DAIS environment primarily uses Azure cloud-native and managed platform services, supplemented by a limited number of supporting application and document management components. Because of this design, traditional counts of discrete servers, endpoints, or network devices do not accurately represent the architecture. The production environment includes a public-facing application, multiple application services, managed databases, storage services, and supporting components.

MyRnB, eReporting, and Employer Services has 12 servers in scope in the production environment.

ii. *For the MyAlaska penetration test, what is the current production infrastructure footprint (number of IPs, subdomains, and APIs in scope)?*

Response: myAlaska (myalaska.gov) consists of a single IP, single subdomain, and single set of APIs.

iii. *New DAIS is scheduled for production deployment on July 1, 2026. Will the assessment be conducted on a pre-production or production environment, and how will that affect testing scope?*

Response: New DAIS is currently on schedule to be in production on July 1, 2026. The assessment is expected to occur following initial deployment and early operational stabilization.

Potential Offerors should review Authorization and Operational Safety & Coordination and Access described in paragraph 5.02 (Scope of Work General Requirements) of the RFP and Activities Excluded from Scope of Work relating to impacts on production environments described in paragraph 5.04 (Activities Excluded from Scope of Work) of the RFP. Work plans should account for this implementation timeline and should be coordinated with Department of Revenue technical staff to ensure assessment activities do not disrupt production services or system availability.

iv. *What cloud tenants and subscriptions are in scope for the Azure assessments (MyAlaska and New DAIS)? Is Oracle Cloud Infrastructure included for the MyRnB systems?*

Response: Potential Offerors are not required to assess the general security of cloud providers – only the security of specific applications and systems described in paragraph 4.01 (Select State IT Systems) of the RFP. The Azure assessment scope will focus on the State of Alaska enterprise Azure tenant. MyAlaska is contained on a single subscription within the larger State of Alaska tenant. New DAIS is also within this tenant on a separate subscription. The tenant has multiple out-of-scope systems on other subscriptions. The State's centralized identity service (myAlaska) is leveraged as an authentication dependency for public access to the New DAIS ecosystem. Additional tenant and subscription information may be requested from departments upon contract award.

v. *Are there separate network segments or VPNs for each department that will need to be tested individually?*

Response: Yes, each department has at least one network segment that will need to be tested individually from the other departments.

MyAlaska is on a single subnet.

The Department of Administration's MyRnB system will likely have a single network segment or range of subnets, but network segmentation is controlled by the Office of Information Technology.

From an external testing perspective, New DAIS exposes a small number of public-facing application entry points, associated with myPFD, myPFDInfo, and RPFI services. Internal components are deployed within segmented cloud environments.

Documentation and access necessary to perform the assessment will be provided following contract award, subject to coordination requirements noted in paragraphs 1.05 (Location of Work), 5.02 (Scope of Work General Requirements) and the exclusions noted in paragraph 5.04 (Activities Excluded from Scope of Work) of the RFP.

vi. *What is the current maturity of security documentation (policies, procedures, standards) across the three departments? Do current policies exist, or will the contractor be starting from a low baseline?*

Response: The State of Alaska has a statewide security policy and each department has additional security documentation. We assess maturity to be level 3: defined, according to the Capability Maturity Model Integration (CMMI) scale (0 to 5).

vii. *Has a prior NIST CSF or CIS Controls assessment been performed on any of these systems? If so, can prior results be shared to understand remediation status?*

Response: Not to our knowledge. Prior security assessments have been performed, but used other frameworks. DLA will share information relating to prior security assessments upon contract award. Additional documentation can be requested from departments upon contract award. Potential Offeror should assume they cannot rely upon prior assessments for this RFP.

viii. *Are there existing SOC 2 or FedRAMP reports for the cloud providers hosting these systems that the contractor can review?*
Response: Departments should have SOC 2 or FedRAMP reports available for request upon contract award.

ix. *What are the anticipated onsite dates and durations for field work in Juneau and Anchorage? Will both cities require concurrent visits, or are they sequential?*

Response: Dates can be determined by Potential Offeror to best meet the requirements of the RFP. Travel can be either sequential or concurrent. Travel should be coordinated in advance with DLA and department officials in accordance with paragraphs 1.05 (Location of Work) and 5.02 (Scope of Work General Requirements) of the RFP.

x. *How many stakeholder interviews and workshops are anticipated? How many state agency staff will be available to support the engagement?*

Response: The number of interviews is dependent upon the Potential Offeror's ability to efficiently perform the work detailed in the RFP. Agency officials have agreed to support this work in a timely manner and provide access to staff and materials.

xi. *What is the expected cadence and format for the weekly status meetings referenced in Section 5.02?*

Response: Weekly status meetings are anticipated to be 30-minute calls using Microsoft Teams. We will primarily discuss work progress and any barriers the Potential Offeror is facing. Meetings may require additional time at certain phases of the project, such as the start and close of the project. The specific dates and times of the calls will be mutually agreed upon between DLA, the departments, and the Potential Offeror.

xii. *Who are the designated points of contact at each of the three departments, and what level of availability can be guaranteed during the assessment?*

Response: Departments have committed to cooperating with this security assessment and prioritizing this work. Senior executives, including Chief Information Officer, Chief Information Security Officer, Chief Technology Officers, and IT managers will be among the primary contacts at the departments. During the course of the project, certain individuals or departments may have less availability than others. The Successful Offeror shall discuss timelines and availability with department staff during the entrance conference discussed in paragraph 5.02 (Scope of Work General Requirements) of the RFP. The Successful Offeror shall make adjustments to their work plan according to those discussions and throughout the project as needed.

xiii. *Will the contractor have direct access to system configurations, logs, and network diagrams, or will all information be provided through intermediaries?*

Response: The selected Contractor will be provided the documentation and technical information necessary to conduct the assessment, including relevant configuration details and system documentation, subject to appropriate coordination with department staff and applicable security controls. Obtaining the necessary information could include direct observation through screen sharing or on-site testing. The Successful Offeror should not plan to get direct administrator access to the systems, unless agreed to by department staff. Coordination and access specifics should be addressed further during entrance meetings as described in paragraph 5.02 (Scope of Work General Requirements) of the RFP. In certain circumstances, some information may be provided through an intermediary. For example, the Department of Administration uses Wostmann & Associates and Applied Microsystems Inc. as vendors to manage system development and Oracle Cloud implementation.

xiv. *What data classification and handling restrictions apply to working papers and findings shared outside of Alaska?*

Response: Data protection requirements are detailed in paragraph 5.02 (Scope of Work General Requirements) of the RFP. Alaska Information Security Policies can be found online at https://oit-int.alaska.gov/policy/information-security-policies/. Data should be protected by encryption in-transit and at-rest, with logical access granted only to those on project team, and data should remain in the United States. DLA has a secure file sharing platform available for use by the Successful Offeror that will meet these requirements,

while the files remain on the platform. Potential Offerors should also review paragraph 3.10 (Contract Personnel) of the RFP.

xv. *Please confirm that offerors not claiming the Alaska business preference can secure an Alaska business license upon receiving a notice of intent to award (as opposed to before proposal submission).*

Response: Yes, that is correct. Potential Offerors should review paragraph 2.10 (Alaska Business License, Legal Entity and Other Required Licenses) of the RFP.

2. All other terms and conditions of RFP 26-33-03 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