DIVISION OF LEGISLATIVE AUDIT
RFP NUMBER 26-33-03
AMENDMENT NUMBER 3

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 Friday, April 3, 2026

DATE AMENDMENT ISSUED: Wednesday, March 25, 2026

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

A) On page one (1) of the RFP, the first paragraph that describes the due date for receipt of proposals is amended to read as follows:

SEALED PROPOSALS MUST BE RECEIVED AT THE ABOVE ADDRESS OR MUST BE EMAILED TO LAA.PROCUREMENT@AKLEG.GOV BY 2:00 P.M. ALASKA TIME ON APRIL 3, 2026.

B) On page five of the RFP, in paragraph 1.04 (Contract Term and Work Schedule), the estimated RFP schedule is amended to read as follows:

The estimated RFP schedule is as follows:

March 6, 2026	Issue RFP
March 13, 2026	Pre-Proposal Teleconference
March 20, 2026	Deadline for Written Questions
April 3, 2026	**Deadline for Receipt of Proposals**
April 22, 2026	**DLA issues Notice of Intent to Award a Contract**
May 5, 2026	**Contract signed by DLA**

C) The following questions were received from potential offerors.

DIVISION OF LEGISLATIVE AUDIT
RFP NUMBER 26-33-03
AMENDMENT NUMBER 3

1. *Would the DLA consider extending the deadline by one week so that we can provide a more comprehensive proposal that incorporates updated requirements?*

   Response: Please review the revised Deadline for Receipt of Proposals on lines A and B of this Amendment.

2. *Are there any page limitations or formatting requirements?*

   Response: Please review section six (Proposal Format and Content) of the RFP.

3. *Is there an incumbent currently performing this work? If so, please provide the name of the contractor and the total contract value for the incumbent contract?*

   Response: No

4. *Does the State of Alaska, DLA have an approved budget for this contract?*

   Response: No, please review response to question 13 in Amendment No. 2 of the RFP.

5. *Reference: RFP Page 33/40 – "The project team must include a Certified Information Systems Security Professional (CISSP) and a Certified Cloud Security Professional (CCSP)." Question: Instead of requiring both, would DLA consider revising to allow for either a CISSP or a CCSP on the project team?*

   Response: No. A CISSP is required; however, please see response to question 14 in Amendment No. 2 of the RFP regarding alternatives for CCSP.

6. *Reference: RFP Page 33/40 – "The project team must include a Certified Information Systems Security Professional (CISSP) and a Certified Cloud Security Professional (CCSP)." Question: Would DLA accept the Azure Cloud Engineer certification for the CCSP?*

   Response: Yes.

7. *Reference: RFP Page 33/40 – "In total, three quarters (75 percent) of the Contractor's project team members must hold at least one or more of the following active certifications:*
   - *Certified Information Systems Auditor (CISA)*
   - *Certified Information Systems Security Professional (CISSP)*
   - *Certified Information Security Manager (CISM)*
   - *Certified Cloud Security Professional (CCSP)*
   - *Certified in Risk and Information Systems Control (CRISC)*
   - *Certified Ethical Hacker (CEH)*
   - *Other system security certifications as agreed to by DLA"*

Question: Would DLA consider adding the following relevant certifications to this list: Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT), and Certified Data Privacy Solutions Engineer (CDPSE)?

Response: Yes, to meet the 75% project team requirement, the certifications listed would be acceptable.

7. *Reference: RFP Page 35/40, 4. Relevant Firm Experience – "d) A minimum of two referrals and references from other agencies and owners. If possible, references should be from the projects listed above and should be limited to projects completed in the last five (5) years." Question: Can DLA please clarify what is required to be submitted for a "referral"?*

   Response: Potential Offerors shall provide referral letters from the references that are listed in the Offerors proposal.

8. *Reference: RFP Page 4/40, 1.02 Proposal Submission, Delivery, and Acceptance. Question: Can the DLA please confirm whether the Cost Proposal and Technical Proposal must be submitted in two (2) separate emails; or both PDFs may be attached to a single email, provided each document is clearly labeled in accordance with the instructions in Section 1.02?*

   Response: A single email with two clearly labeled PDFs is acceptable.

9. *Reference: RFP Page 13/40 - SECTION TWO Standard Proposal Information. Question: Should Section Two requirements be provided in the technical or the price section of the proposal response?*

   Response: Section two of the RFP applies to both TECHINICAL and COST proposals.

10. *Reference: Page 34/40, SECTION SIX Proposal Format and Content "(b) one PDF version via email per the instructions in section 1.02 (Proposal Submission, Delivery, and Acceptance). The proposal must be split into two parts: 1) a technical proposal and 2) a cost proposal." Question: Can DLA please clarify for an electronic/PDF submission via email should the proposal be provided with one (1) file containing both technical and price parts or if DLA wants two (2) individual PDF files?*

    Response: Please review response to question 8 of this Amendment.

11. *In order to effectively respond to the solicitation, can the government please provide a one-week extension once the Q/As are posted?*

    Response: Please review the revised Deadline for Receipt of Proposals on lines A and B of this Amendment.

12. *We would like to confirm the CCSP certification is indeed a hard requirement for RFP NO. 26-33-03. We currently hold all other certifications required for this RFP. We also have many AWS and Microsoft certifications, and we were curious if there are alternate certifications that would fulfill the CCSP requirement? If not, we can get the CCSP certification by the time the work starts if that is acceptable. We also have the option to use a subcontractor, but we would like to confirm what our options are.*

    Response: The CCSP certification is not a hard requirement. Please review response to question 14 in Amendment No. 2 of the RFP.

13. *Vendor inventory: Do you already have a complete list of vendors or third parties with access to the in-scope systems, or is the contractor expected to discover and compile it?*

    Response: DLA expects departments to provide vendor information to the Successful Offeror after the entrance conference. Please also review response to question 32 in Amendment No. 2 of the RFP.

14. *"Supporting environments" scope: Does this include only the three applications' direct components, or also shared enterprise platforms (IAM, logging and SIEM, network, hosting, DB platforms)?*

    Response: It includes shared enterprise platforms.

15. *Inherent risk model: Do you have an existing inherent-risk tiering model for vendors, or should the contractor define the risk criteria and thresholds?*

    Response: Potential Offeror should define the risk criteria and thresholds.

16. *Penetration Test Report: Are you expecting a separate penetration test report, or should it be incorporated in the final report?*

    Response: It should be incorporated into the final report.

17. *Third-party connectivity controls: Is the contractor expected to test and validate access controls and monitoring for third-party connections, or only review documentation?*

    Response: As noted in paragraph 5.03 (Scope of Work – Specific Requirements) of the RFP, the contractor is expected to examine access controls, data handling, and monitoring for third-party connectivity. The contractor should be able to collect sufficient evidence through interviews and review of supporting documentation.

18. *Reporting & escalation: Do you already have a defined process for vendor reporting/escalation, or should the contractor design it (cadence, SLAs, triggers)?*

Response: DLA expects some defined processes, but they may have gaps. This topic can be discussed in more detail during the project with departments.

19. *Identify all in-scope assets: Is the state missing an authoritative asset inventory for these applications, or is this a validation/cleanup of an existing inventory? Alternatively, is the vendor only being asked to assess the State's process maturity regarding asset inventory management?*

    Response: Validation and clean-up is expected. Please also review response to question 16 in Amendment No. 2 of the RFP.

20. *Classification criteria: Do you have an existing classification standard (sensitivity + business impact + regulatory), or should the contractor propose the scheme and mapping to NIST CSF/CIS?*

    Response: The State of Alaska has an existing Asset Classification and Control standard, which can be provided after contract award. This standard includes information (data) standards. Contractor may need to map to NIST CSF/CIS.

21. *Structured asset register: Do you want the contractor to populate an existing tool/register (e.g., CMDB/GRC), or deliver a new register/database? Any required fields/template?*

    Response: DLA does not know if an existing tool is available. Potential Offerors can work with DLA on required elements of specific deliverables during the project.

22. *Data flow diagrams (DFD): Do you already have DFDs/interface diagrams, and you want them updated or do you want the contractor to create net-new DFDs for each critical application?*

    Response: DLA does not have Data Flow Diagrams, but expects departments to have some information available that can be requested during the project. DLA does not anticipate Potential Offerors to start from scratch.

23. *DFD depth: What level of detail is required (high-level system context only vs. interface-by-interface with data types, trust boundaries, and transfer mechanisms)?*

    Response: High-level system context is sufficient.

24. *Vendor-branded report requirement: Do you require the final report(s) to be vendor-branded (logo/letterhead), or should deliverables be provided as State-branded (or unbranded) documents/templates?*

    Response: Vendor branded and addressed to DLA. DLA will incorporate the report into a final audit report.

25. *External sharing / audience: Will any deliverables be shared with external parties (e.g., legislators, oversight bodies, auditors, third parties, the public), and if so, which deliverables and at what classification level (public vs confidential)?*

    Response: Deliverables will be shared on a need-to-know basis and should be confidential.

26. *Redaction & public-records handling: If deliverables may be disclosed externally (including via public-records requests), do you require a redacted/public version in addition to a full confidential version? Who performs/approves redactions?*

    Response: Deliverables will be incorporated into audit work papers. Audit work papers are confidential and not subject to public records request. DLA will summarize any information needed for any public reporting, although at this time we anticipate a confidential audit report.

27. *Contracting: is the vendor expected to complete contracting using an Alaska SOW template or can vendor use our approved templates?*

    Response: DLA will be drafting a contract in conjunction with the Legislature's Division of Legal Services.

28. *Citizenship: Is the vendor required to use US Citizens for this work, or are off-shore resources permitted?*

    Response: No off-shore resources are permitted. United States Citizens or authorized workers are expected. Please review paragraph 5.02 (Scope of Work General Requirements) of the RFP for data protection requirements.

29. *4.01 Select State IT Systems; 5.03(D)(iii) Threat and Vulnerability Assessment, Threat and Vulnerability Assessment, Section 4.01 lists MyAlaska, MyRnB, Employer Services, eReporting, and New DAIS as in-scope. However, Section 5.03(D)(iii) specifically names penetration testing for "MyAlaska and supporting infrastructure."*

    Response: The penetration test is expected to be performed on myAlaska and its supporting environment and not the other systems listed in paragraph 4.01 (Select State IT Systems) of the RFP.

30. *5.03(M)(ii) Security Awareness and Training; 5.04 Activities Excluded, Activities Excluded, Does the State intend for the Offeror/Contractor to perform any active social engineering/phishing tests as part of this assessment (if yes then please clarify how many users approximately), or is the scope strictly limited to reviewing the results of the State's own past exercises?*

    Response: Section 5.03(M)(ii) (Security Awareness and Training) of the RFP involves a review of the results of the State's past exercises, if they were performed. Penetration

testing may involve limited social engineering, with prior approval from DLA and in coordination with state security officials.

31. *General Question, About Budget, Can DLA provide any information on the budget required to support these services? (E.g., budget details)*

    Response: No, please review response to question 13 in Amendment No. 2 of the RFP.

32. *General Question, About Single/multiple award contract, Does DLA plan to select a single vendor or multiple vendors to provide these services?*

    Response: DLA anticipates a single vendor; however, proposals can include the use of subcontractors as noted in paragraph 5.06 (Contractor Team Qualifications) of the RFP.

33. *5.03 Scope of Work – Specific Requirements, D. Threat and Vulnerability Assessment, How many critical third-party vendors or cloud service providers (CSPs) are expected to be part of the audit's third-party risk management review?*

    Response: DLA does not have a precise estimate but DLA is aware of two Cloud Service Providers and two other third-party vendors.

34. *5.03 Scope of Work – Specific Requirements, D. Threat and Vulnerability Assessment, Will contract reviews or direct interviews with vendor stakeholders be required?*

    Response: Please review response to question 7 in Amendment No. 2 of the RFP.

35. *5.03 Scope of Work – Specific Requirements, Audit Access & Mode, Will access to systems, personnel, and documentation be entirely remote, or should Inspira plan for onsite visits? If so, how many visits and for which locations?*

    Response: Please review paragraph 1.05 (Location of Work) of the RFP and see also response to question 9 in Amendment No. 2 of the RFP.

36. *5.03 Scope of Work – Specific Requirements, K. Security Policies and Procedures, How many security policies are in scope for review?*

    Response: The State of Alaska has 52 statewide security policies, but some are out of scope. the Successful Offeror will need to map policies to NIST CSF and CIS to determine how many are in scope. Policies are generally 2-3 pages in length.

37. *5.03 Scope of Work – Specific Requirements, Previous assessments, Have you done any assessments previously against any framework?*

    Response: Yes. DLA is aware of other security assessments that have been performed. That information can be provided during the project.

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

    Response: Please review response to question 40 in Amendment No. 2 of the RFP.

39. *5.03 Scope of Work – Specific Requirements, Control implementation documentation, Is there a documentation on security control implementation available? Would you like this to be updated or created if needed?*

    Response: There is documentation on security control implementation available from departments after contract award, but Potential Offerors should assume the information likely needs to be updated.

40. *5.03 Scope of Work – Specific Requirements, Volumetric for Pricing, Can you please provide the volume/details/number of policies, IP, physical location, BCP/DR systems/sites, third-party/contractors, monitoring and logging system, Security awareness and training policies, cloud systems, and users to calculate the professional hours and amount for cost statement?*

    Response: Please review response to question i., ii., iv., v., in Amendment No. 1 and also see responses to questions 1, 8, 9, 28, 29, 32, 38 and 39 from Amendment No. 2 and answers to question numbers 33-36, and 66 from this Amendment.

41. *5.03. B Asset Identification & Classification, To estimate infrastructure review effort, How many total servers (physical and virtual) support each of the three systems?*

    Response: Please review response to question i. in Amendment No. 1.

42. *5.03. B Asset Identification & Classification, To scope network architecture assessment, How many network devices (firewalls, routers, switches) are in scope?*

    Response: DLA does not know these specifics, but departments can share that information during the project. Please review response to question i. in Amendment No. 1 for known information.

43. *5.03. B Asset Identification & Classification, To estimate application security testing effort, How many web applications and APIs are included across all three systems?*

    Response: Please review response to question ii. from Amendment No. 1 and response to question 39 from Amendment No. 2 of the RFP.

44. *5.03. B Asset Identification & Classification, To scope database security review, How many databases support each system and what are their types/versions?*

Response: Please review response to question i. in Amendment No. 1 of the RFP.

45. *5.03. B Asset Identification & Classification, To assess discovery effort and leverage existing documentation, Are current network diagrams, architecture documentation, and asset inventories available and up-to-date?*

    Response: Yes, Potential Offerors should assume they will get access to existing documentation from DLA or departments during the project. The information may be incomplete or need updating in some areas**.**

46. *5.03. B Asset Identification & Classification, To determine cloud environment review scope, How many Azure subscriptions (MyAlaska/New DAIS) and OCI tenancies/compartments (MyRnB) are in scope?*

    Response: Please review response to question iv. in Amendment No. 1 of the RFP.

47. *5.03. B Asset Identification & Classification, To scope integration security review, How many system-to-system interfaces and third-party integrations exist across all systems?*

    Response: DLA does not know these specifics, but departments can share that information during the project. Please review response to question i., and iv., in Amendment No. 1 of the RFP and please review response to question 39 in Amendment No. 2 of the RFP for known information.

48. *5.03. C Risk Assessment Methodology, To leverage existing risk analysis and reduce discovery time, Has a formal risk assessment been conducted previously for these systems? If yes, can results be shared?*

    Response: Yes, risk assessments and security reviews have been performed on at least some systems and information relating to those reviews can be shared during the project.

49. *5.03. C Risk Assessment Methodology, To estimate facilitation and coordination effort, Approximately, How many stakeholders from each managing department (OIT, DRB, PFD) are available for risk workshops and interviews?*

    Response: Please review response to question xii. in Amendment No. 1 of the RFP and response to question 40 from Amendment No. 2 of the RFP.

50. *5.03. D Threat & Vulnerability Assessment, To understand baseline security posture and avoid duplication, Has penetration testing or vulnerability scanning been performed previously on these systems? If yes, when and can results be shared?*

    Response: Yes, penetration testing and vulnerability scanning has been performed, but it may not cover all aspects of the Scope of Work for this RFP. Information can be shared during the project. Potential Offeror should assume they will need to re-perform any work

previously completed to meet the obligations of this RFP; however, the information can be used to understand baseline security postures or to inform penetration testing.

51. *5.03. D Threat & Vulnerability Assessment, To define testing boundaries and Rules of Engagement, Are there any systems, environments, or timeframes that are excluded from active testing?*

    Response: Yes, some of those details will need to be addressed during the project with departments and throughout the project. Please review responses to questions 4 and 9 from Amendment No. 2 of the RFP for blackout dates and New DAIS implementation.

52. *5.03. D Threat & Vulnerability Assessment, To plan testing schedule and avoid delays, What is the timeline and process for obtaining written authorization for penetration testing and vulnerability scanning?*

    Response: DLA has assurance from department officials that this work will be prioritized so we anticipate an expedited process. Each department may have a different process to obtain written authorization.

53. *5.03. D Threat & Vulnerability Assessment, To determine testing scope and effort, Will all environments (production, UAT, development) be in scope, or production only?*

    Response: Production only.

54. *5.03. D Threat & Vulnerability Assessment, System deploys mid-project; clarifies timing, For New DAIS (deploying July 1, 2026), should assessment occur pre-production, post-production, or both?*

    Response: Post-production, but also review response to question 4 in Amendment No. 2 of the RFP.

55. *5.03. E Network Architecture & Security Assessment, To estimate network segmentation review effort, How many network segments/VLANs and security zones (DMZs) support these applications?*

    Response: DLA does not know how many security zones (DMZs) support these applications, but departments can share that information during the project. Please review response to question v. in Amendment No. 1 of the RFP for network segments.

56. *5.03. E Network Architecture & Security Assessment, To scope security tool configuration reviews, What perimeter security and monitoring tools are deployed (firewalls, IDS/IPS, WAF, SIEM)?*

    Response: Those tools are deployed, the details of which can be discussed during the project with departments.

57. *5.03. E Network Architecture & Security Assessment, To estimate firewall rule analysis effort, How many firewall rulesets require review?*

    Response: DLA does not have this information, but departments can provide the details during the project.

58. *5.03. E Network Architecture & Security Assessment, To reduce discovery effort, Are network diagrams and data flow diagrams current and available for review during the engagement? How up-to-date are they kept?*

    Response: Yes, this information should be available. DLA can provide information it has and the departments can supplement with additional information during the project. Information may need to be updated and details around processes used to update this information can be discussed with departments.

59. *5.03. F Application Security Assessment, To determine appropriate assessment methodology, Are these applications custom-developed, COTS, or hybrid?*

    Response: There is a mix of applications involved with these systems.

60. *5.03. F Application Security Assessment, To leverage existing findings and reduce redundant testing, Has application security testing (SAST, DAST, code review) been performed previously?*

    Response: Prior security assessments can be provided during the project, but Potential Offeror should assume they will need to revalidate any prior findings rather than solely rely upon those assessments. The information can be used to inform understanding of baselines and potential vulnerabilities for penetration testing.

61. *5.03. F Application Security Assessment, To scope authentication security review, What authentication mechanisms are used (SSO, MFA, local accounts)?*

    Response: There is a variety of authentication methods, including those listed.

62. *5.03. F Application Security Assessment, To determine code review feasibility and effort, Is source code available for review during the engagement, or will assessment be limited to black-box testing?*

    Response: Potential Offerors should assume black-box testing.

63. *5.03. G Database Security Review, To scope database access control review, How is database access controlled (application service accounts, direct DBA access, both)?*

Response: DLA does not have this information, but departments can provide the details during the project.

64. *5.03. G Database Security Review, To focus review on implemented controls, What database security controls are implemented (encryption at rest/in transit, audit logging, access controls)?*

    Response: Potential Offeror should assume those controls are in place, but will need to be validated to meet the Scope of Work.

65. *5.03. G Database Security Review, To assess backup security review scope, What are the backup frequencies and retention periods for each database?*

    Response: These vary and the details can be discussed with departments during the project.

66. *5.03. H Identity & Access Management (IAM) Review, To scope IAM review effort, How many total user accounts exist across all three systems (internal staff and external citizens)?*

    Response: The systems have up to an estimated 750,000 total user accounts, but it will vary by system, and some systems have far fewer user accounts. The details can be discussed with departments during the project. DLA does not expect the Successful Offeror to review the access of each account, but rather the controls related to Identity and Access Management.

67. *5.03. H Identity & Access Management (IAM) Review, To estimate privileged access management review, How many privileged/administrative accounts exist?*

    Response: These details vary by system which can be discussed with departments during the project. DLA does not expect each account to be reviewed, but rather what controls are in place to manage privileged/administrative accounts.

68. *5.03. H Identity & Access Management (IAM) Review, To scope directory services review, What identity platforms are in use (Active Directory, Azure AD, other)?*

    Response: There is a mix of directory services across the systems. These details can be discussed with departments during the project.

69. *5.03. H Identity & Access Management (IAM) Review, To assess IAM governance maturity, How frequently are access reviews/recertifications performed?*

    Response: These details can be discussed with departments during the project.

70. *5.03. H Identity & Access Management (IAM) Review, To determine PAM review scope, Is a Privileged Access Management (PAM) solution in use?*

Response: These details can be discussed with departments during the project.

71. *5.03. I Data Protection & Privacy , To scope data protection assessment, What types and volumes of PII/ePHI are processed by each system?*

    Response: These systems have an estimated up to 750,000 accounts each which contain PII and ePHI. Additional details can be discussed with departments during the project.

72. *5.03. I Data Protection & Privacy , To focus on existing controls, What data protection controls are implemented (encryption at rest/in transit, DLP, masking)?*

    Response: Please review response to question 64 in this Amendment.

73. *5.03. I Data Protection & Privacy , To determine compliance assessment scope, What privacy regulations apply (HIPAA, AS 45.48, others)?*

    Response: The Potential Offeror may identify additional compliance requirements during the project, but DLA is aware of HIPAA and AS.45.48**.**

74. *5.03. I Data Protection & Privacy , To leverage existing privacy analysis, Has a Privacy Impact Assessment (PIA) been conducted for each system? Can it be shared?*

    Response: DLA is not aware of an assessment being performed, but departments can address that during the project. If applicable, this information would be expected to be shared during the project.

75. *5.03. J Cloud Security Assessment, To scope cloud security review, What cloud governance and security tools are in use (Azure Policy, Azure Defender, OCI security services, CSPM)?*

    Response: Please review response to question 23 in Amendment No. 2 of the RFP.

76. *5.03.J Cloud Security Assessment, To determine IaC security review scope, Is Infrastructure-as-Code used for cloud deployments? If yes, what tools?*

    Response: DLA is not aware of any Infrastructure-as-Code use, but departments can provide additional information during the project.

77. *5.03.J Cloud Security Assessment, To scope cloud IAM assessment, How is cloud identity managed (Azure AD, OCI IAM, federated)?*

    Response: DLA does not have this information, but departments can provide the details during the project.

78. *5.03.J Cloud Security Assessment, To assess cloud monitoring review scope, Are cloud activity logs and security monitoring enabled and retained?*

    Response: DLA expects these controls are in place.

79. *5.03. K Security Policies and Procedures, To estimate policy review effort, How many security policies exist in the current policy framework?*

    Response: Please review response to question 36 of this Amendment.

80. *5.03. K Security Policies and Procedures, To assess policy currency, When were security policies last reviewed and updated?*

    Response: The policies have a rotating basis based on subject matter. They have varied frequencies of review.

81. *5.03. K Security Policies and Procedures, To scope standards and procedures review, Are technical security standards and operational procedures documented and available?*

    Response: Yes, that information will be available to the Successful Offeror during the project.

82. *5.03. I Physical Security Controls, To estimate site visit effort and logistics, How many physical locations (data centers, co-location facilities) require assessment?*

    Response: Please review response to question 9 in Amendment No. 2 of the RFP.

83. *5.03. I Physical Security Controls, To determine onsite vs. remote review feasibility, Can physical security documentation and access logs be provided for review during the engagement?*

    Response: Yes, DLA expects this information to be available.

84. *5.03. M Security Awareness & Training , RFP requires analysis of statewide training program, What is the security awareness training program structure (platform, frequency, content)?*

    Response: Per statewide policy "Executive Management must ensure that personnel receive the required training and that information security training and awareness activities are documented. ISOs, with the assistance of the SSO, will employ a variety of techniques in implementing security training and security awareness including, but not limited to:
    - Training at initial hiring;
    - Quarterly end user security training
    - Monthly phishing campaigns

- Annual review of Acceptable Use Policy
- Computer-based training for agency specific regulatory requirements; and
- Formal training courses, training in conjunction with employee evaluations and
- contract reviews; and
- Distribution of awareness information via e-mail, intranet or other written,
- electronic, or oral publications and communications.
- Implementation of remedial training requirements based on individual security
- awareness training performance."

85. *5.03. M Security Awareness & Training , To assess training effectiveness, What is the training completion rate for the past 12 months?*

    Response: DLA does not have this information, but departments can provide the details during the project.

86. *5.03. M Security Awareness & Training , RFP specifically requires phishing scheme effectiveness analysis, Is phishing simulation testing conducted?*

    Response: Statewide security policy outlines requirements for phishing campaigns, but DLA does not have the specifics.

87. *5.03. M Security Awareness & Training , Required for policy analysis, Can the statewide IT security training policy be provided during the engagement?*

    Response: Yes.

88. *5.03. N Monitoring and Logging, To scope SIEM and monitoring review, What SIEM or log aggregation platform is in use? How many log sources?*

    Response: DLA does not know these specifics, but departments can share that information during the project.

89. *5.03. N Monitoring and Logging, To determine IR plan review scope, Is there a documented incident response plan? Has it been tested?*

    Response: DLA expects an IR plan is in place and has been tested. This should be validated by the Successful Offeror.

90. *5.03. N Monitoring and Logging, To understand incident landscape, How many security incidents have been handled in the past 12 months?*

    Response: These details can be discussed with departments during the project. Potential Offerors should assume Alaska is exposed to the same type of threats and number of incidents as other government clients.

91. *5.03. N Monitoring and Logging, To scope security tool review, What threat detection tools are deployed (EDR, NDR, email security)?*

    Response: DLA does not know these specifics, but departments can share that information during the project.

92. *5.03. O Third-Party Risk Management and Vendor Oversight, To scope vendor risk assessment, How many third-party vendors have access to or integrate with the in-scope systems?*

    Response: Please review response to question number 32 in Amendment No. 2 of the RFP.

93. *5.03. O Third-Party Risk Management and Vendor Oversight, To leverage existing vendor assessments, Is there a vendor risk assessment process and documentation available?*

    Response: DLA expects departments perform vendor risk assessments and this information would be available during the project.

94. *5.03. O Third-Party Risk Management and Vendor Oversight, To determine cloud provider assurance review scope, What are the primary cloud service providers (already known: Azure, OCI) and what compliance certifications have been verified?*

    Response: DLA is aware of Azure and Oracle. DLA does not know what compliance certifications have been verified.

95. *5.03. P Business Continuity Planning and Disaster Recovery (BCP/DR), To scope BC/DR plan review, Does each system have documented BC/DR plans? When were they last tested?*

    Response: DLA expects these systems to have documented BC/DR plans that have been tested, but this should validated this during the project.

96. *5.03. P Business Continuity Planning and Disaster Recovery (BCP/DR), To assess recovery requirement adequacy, What are the defined RTO and RPO for each system?*

    Response: These details can be shared during the project.

97. *5.03. P Business Continuity Planning and Disaster Recovery (BCP/DR), To scope backup security review, What is the backup strategy (frequency, retention, geographic distribution, encryption)?*

    Response: These details can be shared during the project.

98. *Others. Change Management & Configuration Management Review, To scope change management review, Is there a formal change management process? What tool is used?*

    Response: DLA expects formal change management processes are in place, but does not know what tool is used.

99. *Others. Change Management & Configuration Management Review, To assess configuration management review scope, Is a configuration management database (CMDB) maintained and current?*

    Response: DLA expects a configuration management database is maintained.

100. *Others. Change Management & Configuration Management Review, To evaluate patch management review effort, What is the patch management process and average time to patch critical vulnerabilities?*

    Response: These details can be discussed with departments during the project.

101. *Will CypherIntel be granted read-only access to Azure B2C/Microsoft Entra ID configurations for MyAlaska, or will all evidence be gathered through screenshots and documentation provided by state staff?*

    Response: The level of access granted is dependent upon coordination with security officials at each department. DLA expects departments to provide the necessary information to perform the review.

102. *For New DAIS (scheduled July 1, 2026 production deployment), will the assessment be conducted against the pre-production/staging environment given the contract start date of June 1, 2026? Will a production environment be available before the September 14 draft deadline?*

    Response: Testing should be performed on production environment. Please review response to question 4 in Amendment No. 2 of the RFP.

103. *Will the Contractor receive access to network diagrams, system security plans (SSPs), or prior audit/assessment reports for all three in-scope systems prior to the kickoff meeting?*

    Response: Potential offeror should assume most information will be provided during the project.

104. *For Oracle Cloud Infrastructure (OCI), will temporary read-only IAM access be provided, or will reviews be evidence-based only?*

    Response: Please review response to question 101 in this Amendment.

105. *Does the "statewide" phishing/security awareness assessment require engagement across all executive-branch departments, or only those supporting the in-scope systems?*

Response: Potential Offeror will not need to engage with all executive branch departments. The Office of Information Technology will be the primary contact for statewide security awareness campaigns.

106. *How many physical facilities in Juneau and Anchorage are expected to require site visits, and are data centers state-owned or third-party hosted?*

Response: The State of Alaska uses a mix of state-owned and cloud hosted data centers. There is one state operated physical data center in Juneau.

107. *Will the final report be classified (e.g., CUI) or remain unclassified under NDA provisions?*

Response: The final report will be confidential.

108. *What is the expected timeline for agency responses to draft findings, and how does this align with the September 14 draft deadline?*

Response: DLA expects departments to respond quickly to draft findings. With proper planning and staggering work across systems, DLA believes the September 14th date is attainable.

109. *Will required presentations be consolidated into a single trip or conducted across multiple visits?*

Response: DLA expects the three presentations to take at least two trips; however, this is dependent upon Legislative scheduling and Potential Offerors should assume that multiple trips are possible.

110. *What is the preferred format and delivery mechanism for working papers, and are there data residency requirements?*

Response: DLA has a secure file transfer platform to facilitate delivery of working papers. The data is required to reside in the United States at all times. DLA can discuss details relating to working paper format during the project, but generally speaking Word, Excel, and PDF file formats are acceptable.

111. *Will the State provide a secure file transfer mechanism, or should the Contractor provision one?*

Response: DLA has a secure file transfer platform available for use and will accept a contractor provided platform if it meets State of Alaska security requirements and data residency requirements.

112. *Is there an internal budget range for this engagement?*

Response: No, please review response to question 13 in Amendment No. 2 of the RFP.

113. *Should the Schedule of Professional Hours be organized by task, system, or labor category?*

Response: Please review paragraph 6.03 (Offeror's Schedule of Professional Hours and Fees) of the RFP.

114. *Does "governmental organizations" include federal defense and intelligence community experience?*

Response: Yes.

115. *Will GIAC certifications (e.g., GPEN, GWAPT, GCIH) satisfy the certification requirement?*

Response: GIAC certifications will not replace the CISSP requirement, but can be used to meet the 75% threshold requirement. If the GIAC certification includes a focus on Cloud security, it can satisfy the CCSP requirement.

116. *Will classified federal engagements be acceptable as reference projects with limited disclosure?*

Response: Yes.

117. *Is an AICPA peer review required, or will equivalent certifications (e.g., ISO 27001, SOC 2) suffice?*

Response: An AICPA peer review is not required if the firm is not subject to audit standards. Other certifications, if applicable, will suffice for non-audit firms submitting bids.

118. *What level of state staff availability should be assumed during June–September?*

Response: Availability will depend on individual and department schedules and vacations; however, departments have committed to DLA to prioritize this work.

119. *Should onsite work be planned as a single mobilization or multiple trips?*

Response: The number of trips for onsite testing is up to the Successful Offeror and subject to coordination with departments; however, in addition to onsite testing, the Scope of Work

includes three presentations to legislative committees so at least 2 trips will be required for some members of the project team for those presentations.

120. *Are there restrictions or approval requirements for scanning/vulnerability tools?*

Response: Yes, these need to be coordinated with department security officials.

121. *What is the expected timing for NDAs/MOAs with participating agencies?*

Response: Please review response to question 52 in this Amendment.

122. *Will kickoff and entrance conferences be conducted in person or remotely?*

Response: Remotely.

123. *Will network operations teams be available during testing to prevent disruptions (e.g., IDS/IPS blocking)?*

Response: Yes, but this will require coordination with department security officials.

124. *Will vendor inventories and SOC reports be provided for third-party risk assessment?*

Response: Yes, the information that is available will be provided.

125. *Have recent BCP/DR tabletop exercises been conducted, and will after-action reports be available?*

Response: We expect BCP/DR tabletop exercises and after-action reports would be made available during the project if previously conducted.

126. *Will a HIPAA Business Associate Agreement (BAA) be required?*

Response: DLA would expect a HIPAA Business Associate Agreement may be required for systems with ePHI. Details can be discussed with department officials during the project.

127. *Will prior NIST CSF or CIS assessments be shared?*

Response: Yes, to the extent they have been conducted.

128. *Should findings be mapped to both NIST CSF 2.0 and CIS Controls v8.1, or is one primary?*

Response: It depends on the topic areas detailed in the scope of work. Sometimes the frameworks cover the same topics, while other times only one framework is relevant.

129. *Section 5.06 "Contractor Team Qualifications": To ensure full compliance with the certification requirements, could you please clarify whether the holding of a CISSP certification, along with other certifications such as a CISA and a CDPSE would satisfy the overall certification requirement for the project lead?*

    Response: Yes.

130. *Regarding the requirement that "The project team must include a Certified Information Systems Security Professional (CISSP) and a Certified Cloud Security Professional (CCSP)" (RFP pg. 33), would it be acceptable for a proposed team to have at least one of those certifications, rather than both?*

    Response: The CISSP requirement is firm; however, DLA will accept other cloud security related certifications to meet the CCSP requirement.

131. *Regarding the requirement that "The project team must include a Certified Information Systems Security Professional (CISSP) and a Certified Cloud Security Professional (CCSP)" (RFP pg. 33), would you consider accepting any alternate security certifications, such as those on the DoD Cybersecurity Workforce Certification List?*

    Response: No for CISSP, but yes for other certification requirements described in paragraph 5.06 (Contractor Team Qualifications) of the RFP. For meeting the CCSP requirement, alternative certifications must focus on cloud security.

D) 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