Subject: RFP-ACT-SACT-26-54 Secure Cloud Service

Reference: LOG 1- Q&A Questions and Answers

Date of Issue: 10 July 2026

The following questions were raised with respect to subject RFP-ACT-SACT-26-54 Secure Cloud Service. Responses are to provide clarification.

#	Questions from Bidders	Answers from HQ SACT
1	§F.1 Network Termination Equipment (on-prem HSM), p.31; Appendix A §1.3 Cryptography & Key Management (HSM-backed), p.41; Appendix A §1.7–1.8 (Lot 2 NATO Crypto Hardware) Would you confirm that HSM on-prem to be PFE / provided by Lot 1 bidders only? THE RFP requires the supplier to provide physical HSM for BYOK/HYOK use cases. The RFP states that the network conenctivity should be setup from two customer locations. Is it adequate to provide only one on-prem HSM or that has to be also redundant and be in two locations?	The HSM is a supplier-provided component and is not intended to be provided solely by Lot 1 or as customer-furnished equipment. The RFP does not prescribe a specific number of HSMs. However, given the requirement for connectivity from two customer locations, bidders should propose an HSM architecture that meets the required security, availability, and resilience objectives and does not introduce a single point of failure. It is the bidder's responsibility to determine and justify the appropriate HSM deployment model, including any redundancy required to satisfy the RFP requirements.
2	§C Secure (Direct) Connection Requirements + §C.1 Connection Specifications, p.25; §F.1 Network Termination Equipment (secure gateway/routers), p.31 Would you confirm that on-prem network equipment is PFE? We believe that site to site connectivity / secure VPN is only relevant for Lot 1 submissions - please confirm this is a correct assumption.	No. The RFP does not assume that on-premises network equipment will be provided as customer-furnished equipment (PFE/GFE) unless explicitly stated elsewhere in the solicitation. The secure connectivity requirements apply to the solution as a whole and are not limited exclusively to Lot 1. Bidders should propose the network equipment, connectivity, and associated components necessary to meet the security, performance, and operational requirements of their proposed solution. It is the bidder's responsibility to identify any on-premises equipment required and include it within their proposed architecture unless otherwise specified in the RFP.

3	§C.2 End-User Devices (laptops), p.26 vs §F.2 End-User Devices (thin-client/secure virtual desktop), p.31 Would you confirm the types of devices that we should suggest - considering cloud-PC as an option? Is it acceptable that we only provide cloud-based virtual devices / desktops which can be access from existing NATO devices?	Yes. Bidders may propose cloud-based virtual desktops or Cloud PC solutions, provided they meet the functional, security, performance, and user experience requirements defined in the RFP. The RFP does not mandate a specific end-user device model. Solutions that leverage existing NATO-managed endpoint devices to access secure virtual desktops are acceptable, provided the bidder demonstrates compliance with all applicable security, identity, connectivity, and operational requirements. Bidders should clearly identify any assumptions, dependencies, or endpoint requirements associated with their proposed solution. The final assessment will focus on the bidder's ability to meet the stated service and security objectives rather than a specific device implementation.
4	§1.d Firm Fixed Price Deliverables, p.4; §11.b Price Proposal (FFP), p.7; Enclosure 4 Mandatory Price Proposal, p.15; §4 Period of Performance options, p.21–22 For cloud products, can you confirm one of the following: (a) these must all be priced within the single fixed-price services contract - if the case, please provide the maximum estimated consumption foreseen for the services in this RFP (there is minimum sizing info in the tender documents); or (b) it is acceptable for a bidder to propose separate contractual vehicles (consumption-based) for cloud elements, referenced in the proposal?	SCS is a turnkey service all required elements must be included in the firm fixed price contract for it to be fully operational. We do not intend to establish a separate vehicle for cloud consumption services outside of the scope of this procurement. The prototype is however not intended for heavy operational use. Main objective is security accreditation and application migration. Please include a basic consumption for the services to operate based on the information indicated in the SOW, and on a separate sheet, please indicate price for additional consumption.
5	§1.d Firm Fixed Price Deliverables, p.4; §11.b Price Proposal, p.7; Enclosure 4, p.15 For Lot 2 hardware deliverables (end-user devices for testing) and software licenses, can you confirm one of the following: (a) these must all be priced within the single fixed-price services contract; or (b) it is acceptable for a bidder to propose separate contractual vehicles (distinct	All hardware, software licences, subscriptions, and services required to deliver the Lot 2 capability shall be included within the bidder's proposal and pricing. We do not intend to establish separate contractual vehicles for hardware supply, software licensing, or other non-services elements outside the scope of this procurement. Bidders shall propose a complete solution and clearly identify any assumptions related to the provision,

	hardware supply or licensing agreement) for non-services elements, referenced in the proposal but executed independently?	licensing, support, and lifecycle management of the required components. The RFP specifically requires the contractor to procure and configure the end-user devices required for the pilot
6	§12.e Prime Contractor Principle (prime solely liable), p.8; §12.f (subcontracting retains full liability), p.8; §12.g (consortium joint & several liability), p.8 if a bidder proposes to address hardware elements (end-user devices, hardware-based authentication tokens) through a named subcontractor, could ACT clarify the extent of the prime contractor's liability for that hardware scope? Specifically, is the prime contractor required to carry full joint and several liability for the hardware deliverables, or is it acceptable for hardware obligations to sit with the subcontractor and be referenced as a parallel commitment documented within the overall proposal?	As provided in the provisions of the RFP referenced in this question, The privity of contract is between HQ SACT and the prime contractor. The contractor is fully liable to HQ SACT for contract performance and all claims arising from it.
7	§18 Surge Capability (≤50% cap; same pricing structure as original contract), p.10 In relation to additional scope / change management where you say that the contractor must be able to accommodate additional manpower within the 50% of the original contract - given this is fixed price, how would the pricing for this additional scope be determined - based on the rates agreed at award or subject to seprate negotiation at the time the scope is adjusted?	This means HQ reserves the right to amend the contract up to 50% of its original value. Subsequent surge capability amendment would be subject to separate negotiation.

8	§C.2 End-User Devices (100 total / 50 per lot), p.26; §F.2 End-User Devices (FIDO2 / smart card, 50 per lot), p.31 For end-user devices and hardware based authentication devices (FIDO keys) in a split-lot scenario - will each vendor that gets a lot be indepdendently required to provide the full complement of user devices and hardware based authentication devices (FIDO keys) for their prototype environment or would a single set of devices be used across lots?	In a split-lot scenario, each lot shall be capable of operating independently and demonstrating the full required functionality of its respective prototype environment.
9	§1.e HQ SACT General Terms & Conditions (15 Jan 2026), p.4; §15.c(5) Acceptance of General T&Cs, p.9; §17.c (negotiate minor deviations), p.9–10; Enclosure 2 Compliance Statement, p.13 Can ACT confirm if a contractor may, as part of the proposal, reference an existing and in-force NATO contractual framework instead of the RFP Terms shared?	No, the compliance statement shall be submitted for this HQ SACT RFP governed by HQ SACT Terms and Conditions dated 15 January 2026.
10	§16 Proposal Clarifications, p.9; §17 Award, p.9; §15 Bid Evaluation, p.9 Will the contract be awarded directly on the basis of the submission (proposal as a binding offering) or does ACT reserve the right to enter post-submission negotiations?	Evaluation and award shall be based on the submitted technical and financial offers.
11	Enclosure 2 Compliance Statement (variations allowed if functional/performance requirements met; minor deviations acceptable), p.13; §15.c(2) (mandatory compliant/non-compliant), p.9 If a bidder's approach is fully compliant with all mandatory requirements, but proposes an alternative method for a non-	From a legal perspective, as mentioned in paragraph 17.c. of the RFP, HQ SACT reserves the right to negotiate minor deviations to the RFP or Terms and Conditions. Bidders must indicate any requested deviation, adjustment or consideration in Enclosure 2 From a technical standpoint, alternative methods are authorised for non-

	mandatory element will this be treated as non-compliant or would this alternative be evaluated based on its merits?	mandatory elements, if compliant with the SOW, and will be assessed in accordance with the best value performance criteria.
12	HQ SACT General T&Cs – IP clause (external, per §1.e p.4); within RFP: §E.2 Proof of Concept – Data Sovereignty (NATO retains full ownership/control of data), p.30 IP - For Lot2 how do we define the boundary between IP that will belong to NATO upon delivery, pre-existing contractor IP used to deliver the services and third-party platform IP? Will bidders have an opportunity to document the pre-existing IP exclusions within the proposal?	NATO retains ownership of its data, all Foreground IP, and contract deliverables as defined in the RFP and the HQ SACT General Terms and Conditions. Pre-existing contractor IP and third-party IP remain the property of their respective owners. Bidders should clearly identify any pre-existing or third-party IP incorporated into their proposed solution, including any applicable licensing or usage restrictions. Bidders are invited to include a declaration of background IP in their technical offer if applicable.
13	Same as above: HQ SACT General T&Cs – IP clause (external); §E.2 Data Sovereignty, p.30 where a deliverable consists of the configuration, integration, or customisation of a licensed third-party cloud platform — as distinct from original source code authored by the contractor — could ACT clarify how the IP clause applies in that context? Specifically, does HQ SACT require full assignment/ownership transfer of those configuration artefacts, or would a perpetual, royalty-free licence to use and modify them be an acceptable alternative? This distinction is relevant because some configuration artefacts may be technically inseparable from the underlying platform IP, which remains with the platform provider under its own licensing terms.	NATO does not seek ownership of third-party platform intellectual property. Where deliverables include the configuration or integration, the underlying platform IP remains the property of the respective owner. All new Intellectual Property rights generated during the performance and for the purpose of the contract will vest in and be the sole and exclusive property of NATO/HQ SACT, in accordance with section 19 of the SOW. Bidders should identify any third-party IP or licensing constraints in their proposal. NATO requires sufficient rights to use, operate, maintain, and modify the Background IP delivered solution as required to allow NATO to use the deliverables for any objectives and business purpose related to or derived from the Contract. See answer #12

14	§1.d, p.4; §1.e General T&Cs, p.4; §17.a Award (FFP per Lot), p.9 Please expand the definition of the Firm Fixed Price according to the the RFP.	An FFP contract provides for a price that is not subject to any adjustment on the basis of the contractor's cost experience in performing the contract. Please note that FFP contract does not preclude use of surge capability clause.
15	HQ SACT General T&Cs – warranty clause (external, per §1.e p.4); within RFP: §E Security Audit & Required Documentation / Schedule of Milestones & Acceptance Criteria, p.30–33 The contract terms reference post-delivery warranty obligations. Could ACT clarify the following: (a) the intended duration of the warranty period and whether it runs from final acceptance of the full scope or from acceptance of individual deliverable milestones; (b) whether the warranty covers defects in the contractor's bespoke deliverables only, or also extends to the performance and availability of underlying licensed cloud platform services; and (c) whether the warranty obligation may be fulfilled through a certified third-party support partner engaged by the prime contractor, rather than directly by the prime contractor for the full warranty duration? (d) P30, E3. Security Validation: "Within 6 months of contract award" Could this be changed to "Within 6 months of delivery start date". Can we also assume that ACT security stakeholders will be reviewing the outputs of th engineering activity as an ongoing activity rather than at one fixed point upto 6 months after activity start date?	A) The warranty lasts for a period of twelve months (12) following the date of acceptance of deliverables B) The Contractor will be deemed not responsible for a Defect if (a) the use of the Software by the Purchaser was not in conformity with the Contract, and such use caused the Defect, or if (b) the Purchaser was explicitly not allowed to have certain development or maintenance services performed by its own personnel or by a third party, and if it will be sufficiently proven that any development or maintenance activity performed by such staff or third party has caused the Defect. However, this exception will not be applicable if the Contractor has failed to correct a Defect or to provide a reasonably requested modification to the Software within a reasonable period of time after receipt of the Purchaser's notice or request, and the Purchaser has therefore required its staff or a third party to perform the request. C) Yes, that is possible. In respect of HQ SACT's Prime Contractor Principle, the Prime Contractor is solely liable for the overall performance and management of the Contract.

		D) No. The requirement remains "within 6 months of contract award." Bidders should assume that ACT security stakeholders will engage throughout the engineering, implementation, and validation activities. Security reviews will be conducted as an ongoing process to support accreditation and risk management, rather than as a single review at the six-month point.
16	HQ SACT General T&Cs – data protection (external, per §1.e p.4); within RFP: Appendix A §1.1 Data Protection and Tagging, p.41; §A Security Accreditation (NATO security policies), p.22 The RFP references data protection requirements that will apply to the contract. Could ACT clarify how these requirements are intended to interact with a contractor's existing obligations under applicable national or regional data protection law? Specifically: (a) are bidders expected to comply with HQ SACT's data protection requirements in addition to their statutory obligations, or as a substitute for them; and (b) are there specific HQ SACT data protection policies that bidders should review and address in their proposals?	(a) Bidders are expected to comply with both the HQ SACT contractual requirements and any applicable national or regional data protection laws. The RFP requirements do not replace statutory legal obligations. (b) Bidders should address the data protection, security, data sovereignty, and accreditation requirements identified in the RFP and applicable NATO security policies. Any additional policy requirements relevant to contract performance will be communicated during contract execution as necessary.
17	Please can the Authority advise on the indicative timescale for the approval of funding, noting the comment on Pg 1: "This Procurement Opportunity is still pending validation of funding and approvals."	Secure Cloud Service requirement has now been validated as project to be funded by the relevant NATO Committee. Nonetheless any NATO Procurement Opportunity (including this one) is always subject to funds confirmation and hence HQ SACT reserves the right to cancel, withdraw, or suspend at any time, this RFP either partially or in its entirety. Contract award will not occur without confirmation of funds.

18	The contract term is now shown as 1+1+1 in the RFP which has increased from 1+1 in the NOPO Publication published 04/28/2026. Please can the Authority confirm that the budget remains as €5m per Lot per year, hence a total of €30m (total of 2 Lots). Originally in the NOPO, it was listed as €20m total.	The period of performance in the RFP has been updated since the publication of the NOPO. Please note that all options are non-committal and subject to being exercised solely at the discretion of HQ SACT based on satisfactory contractor performance, availability of funding, budgetary & operational requirements and Contracting Officer approval.
19	We note the proposed timescales for the phased delivery of capability and have significant concerns regarding the viability of a solution against the stated timeline (impacted by the procurement of equipment, cryptographic equipment). With our preferred approach or even using alternative solutions we do not believe the timescales are viable. Please can the Authority re-assess the viability of the required delivery timeline and the supporting advice provided and re-confirm the required timescales for delivery. *Additional Note, not as a clarification, but for context: based on the stated timescale we do not believe a compliant proposal can be made, and may result in our withdrawal.*	ACT acknowledges industry concerns regarding delivery timelines, including potential dependencies associated with equipment procurement, cryptographic devices, and security-related components. At this time, the delivery milestones and timelines stated in the RFP remain unchanged and reflect ACT's operational objectives for the programme. Bidders are encouraged to propose the most effective delivery approach to meet these timelines and to clearly identify any assumptions, dependencies, risks, or schedule constraints within their proposals. Should any changes to the schedule become necessary, they will be communicated through the formal procurement process.
20	In respect of the HQ SACT General Terms and Conditions incorporated into RFP-ACT-SACT-26-54, we would be grateful for clarification on the points below. The terms appear to be structurally misaligned with the Secure Cloud Platform requirements. The terms appear drafted around a goods/supply model, including title passing on acceptance after physical delivery and inspection, and key provisions covering intellectual property, licensing and security are in conflict with a cloud/SaaS platform provision. While some physical deliverables are expected (e.g. EUC devices and network infrastructure), these appear ancillary to the overall cloud platform. Some wider terms also appear imbalanced, including provisions that could give rise to	**1.** The HQ SACT General Terms and Conditions have been intentionally incorporated into the RFP and remain applicable to this procurement. No revised cloud-specific terms and conditions are planned. **2.** Bidders are expected to submit proposals that comply with the RFP requirements. Minor or non-substantial deviations may be identified in accordance with the RFP; however, ACT reserves the right to determine the materiality and acceptability of any proposed deviation during the evaluation process. **3.** Bidders should prepare their proposals based on the terms and conditions provided

	uncapped or unbounded liability, which will make compliance challenging or commercially unviable. The RFP Compliance Statement requires proposals to be fully compliant, with any deviations being minor or non-substantial. Can the Contracting Authority please confirm: 1) Whether the current terms have been incorporated in error, and whether revised cloud-aligned terms will be issued? 2) The extent to which bidders may propose deviations, given the stated minor/non-substantial limitation? 3) How bidders should proceed in light of the above? We would be grateful for clarification so that we can assess the compliance position appropriately.	in the RFP and clearly identify any proposed deviations in the Compliance Statement. Proposals will be evaluated in accordance with the requirements of the solicitation.
21	Proposals must be emailed, so must be of a limited size. Please can the Authority advise if there are any known gateway limitations on the attachment size constraint?	Bidders are invited to zip/compress their submission and send multiple emails if needed. Please refer to paragraph 12 of the RFP.
22	The scoring criteria for Lot 1 Serial 4 states a maximum score of 10; however the breakdown implies 20. Please can the Authority confirm the correct criteria	Thank you for identifying the discrepancy. The maximum score for Lot 1, Serial 4 is 10 points. The corrected scoring criteria are: • **0 pts:** No SLA or failover capability. • **2.5 pts:** Single-node deployment or no redundancy. • **5 pts:** At least one redundancy mechanism (compute or network). • **7.5 pts:** Multi-site failover with RTO ≤ 4 hours and RPO ≤ 1 hour. • **10 pts:** Full multi-site resilience with RTO ≤ 1 hour and RPO ≤ 15 minutes under a tested failure scenario. This corrected scoring supersedes the breakdown currently shown in the RFP. See amended RFP (Amdt 1)
23	Please can the Authority confirm the User Headquarters two locations? (required for network connection)	For planning purposes, bidders should assume two NATO user locations within the NATO enterprise environment. One will be located in North America, the other one in Europe. The specific locations will be provided to the successful contractor at the start of contract execution and solution design activities.

		Bidders should therefore propose a solution capable of supporting secure connectivity to two geographically separated NATO sites and clearly identify any assumptions made regarding distance, bandwidth, latency, or connectivity requirements.
24	Where there is an option to add more locations "Additional connection to user locations", can the Authority confirm whether is will be new countries or locations within an existing country or both?	Bidders should assume that additional user locations may include sites within existing countries, sites in new countries, or a combination of both. As specific future locations have not yet been determined, proposals should demonstrate sufficient flexibility and scalability to accommodate additional NATO user locations across the Alliance. Any location-specific requirements will be defined at the time the option is exercised.
25	ACT definition of Air-Gapped is: *"A security measure that physically or logically isolates a secure network from unsecured networks such as the public internet."* NIAG SG310 definition: "*A sovereign, fully disconnected and self-contained private cloud platform with no connection to public networks."* Is logical isolation sufficient for NS-level accreditation?, if so, could the Authority confirm that, for the Lot 1 base-period prototype, a non-public-internet-connected cloud environment accessed only through dedicated private connectivity may be used to validate the user experience, COI onboarding, migration sandbox, security controls, operational procedures, and accreditation evidence, provided physical-airgap-specific controls are evidenced through existing deployed airgapped or isolated cloud implementations and mapped to the target production architecture?	Yes. Under the updated NATO SECRET guidance, logical isolation may be acceptable for accreditation provided the solution meets all applicable security, accreditation, and data sovereignty requirements. For the Lot 1 prototype, bidders may use a cloud environment that is not connected to the public internet and is accessible only through dedicated private connectivity to demonstrate the required capabilities. Accreditation will be based on overall compliance with NATO security requirements, not solely on the use of physical air-gapping.

26	**Confidential CQ submitted regarding preferred approach to delivering requirements CANNOT BE ANSWERED in order to respect fair and equal treatment.**	
27	Noting the Authority will provide no hosting infrastructure as GFX, therefore all physical components will need to be procured by the supplier from Contract Award, including a significant BOM for the physical Air-Gapped solution for LOT1. It is our belief that the lead time for infrastructure and in particular Crypto could run into months and therefore the current milestones in particular for LOT1 are unachievable - would the Authority consider component lead times in reassessing the milestone timelines?	ACT acknowledges that infrastructure, cryptographic equipment, and other hardware components may have varying procurement lead times. However, the milestones defined in the RFP reflect the operational objectives of the programme and remain unchanged at this time. Bidders should propose an approach that can achieve the required outcomes within the stated timelines and clearly identify any assumptions, dependencies, risks, or procurement constraints in their proposal. Any future adjustments to the schedule will be communicated through the formal procurement process.
28	Will the Authority accept sanitized evidence from existing government, defence, national-security, air gapped, disconnected, or isolated cloud deployments to demonstrate airgap operating procedures, including offline patching, secure update import, support model, key management, monitoring, administrative access, and controlled data transfer?	Yes, ACT will consider sanitized evidence from relevant government, defence, national security, or similar secure cloud environments as supporting evidence of a bidder's experience and approach. Such evidence may be used to demonstrate operating procedures, security controls, and implementation practices, including offline patching, secure update import, support model, key management, monitoring, administrative access, and controlled data transfer. However, bidders must also demonstrate how those procedures and controls will be applied to the proposed solution and satisfy the specific requirements, security objectives, and accreditation needs of this RFP.

29	The company and its personnel must hold NS-level clearance. However, in Annex E, item 7.1 (page 75), it only refers to a "background check of all cloud providers who have access to service infrastructure (both physical or remote)." A CTS clearance is also required for privileged users (personnel performing administrative or privileged access functions). There is a inconsistency between Paragraph 4f and Annex E item 7.1 could the Authority clarify?	The Authority confirms there is no intended relaxation of the clearance requirements. Paragraph 4f establishes the baseline contractual requirement: the company/prime, relevant subcontractors/partners/consortium members must hold NATO SECRET FSC, and personnel requiring access must hold at least NATO SECRET PSC at start of performance. Annex E item 7.1 is an additional cloud-security control requiring background checks for cloud-provider personnel with physical or remote infrastructure access. It does not replace FSC/PSC requirements where personnel or facilities may access, handle, generate, or support NATO classified information. For privileged users, the specified CTS PSC requirement is a higher, role-specific requirement and therefore applies in addition to the baseline NS requirement. Accordingly, the applicable position is: NS FSC/PSC as the baseline; CTS PSC for privileged users where required; background checks are supplementary and not a substitute for NATO clearances.
30	The document states: *"Formal accreditation (e.g., IL6 or equivalent) will be evaluated and achieved if possible."* Given deployment across three countries, IL6 requirements are unlikely to be met. Could the Authority confirm that mandatory Accreditation should instead follow NATO regulations.	Yes. Accreditation for this effort will be conducted in accordance with applicable NATO security policies, directives, and accreditation processes. References to IL6 or equivalent should be understood as examples of comparable national security accreditation standards that may provide supporting evidence of security maturity. They do not replace the requirement to achieve accreditation under NATO regulations.

31	The Authority has requested 10GPbps through-put, requiring 8 dedicated lines per lot between 2 ACT sites and 4 industrial sites Total: 16 lines if two seperate hosting arrangements between the LOTs, has the Authority including this cost in their budget calculations	The Authority has considered connectivity costs in its budget planning. However, bidders should not assume a fixed requirement for 16 dedicated circuits. The Authority's requirement is to achieve the specified performance, security, and resilience outcomes, while bidders are expected to propose an optimised connectivity architecture that minimises cost and complexity.
32	Network Termination Equipment: ACT recommends “industrial-grade routers.” Are these Type C encryption devices?, Should they not be Type A certified for handling NS information?	No. The reference to “industrial-grade routers” should not be interpreted as specifying a particular cryptographic classification or approval level. Bidders are responsible for proposing network and cryptographic components that satisfy the NATO SECRET security requirements, including any applicable NATO-approved cryptographic requirements. The specific type of encryption device and associated architecture should be consistent with the bidder's proposed solution and accreditation approach. Any final cryptographic requirements will be subject to NATO security and accreditation authorities.
33	Page 38 – Applicable Security Policies: NATO NS cloud directive only applies to Lot 1 (air-gapped) No current framework exists for public cloud use with NS data. Only NIAG SG310 addresses this - Missing references: ADatP-4778 & ADatP-4774 - please can the Authority confirm the position with regards to applicable policies and standards	-The applicable security policies and standards are those identified in the RFP, together with any NATO security directives, accreditation requirements, and data protection standards applicable to the proposed solution. -The NATO SECRET cloud directive applies where relevant to the handling, processing, storage, or transmission of NATO SECRET data, regardless of lot. NIAG SG310, ADatP-4778, and ADatP-4774 may be referenced by bidders as supporting standards where applicable, but they do not replace NATO security accreditation requirements. -Final applicability will be determined through the NATO security and accreditation process based on the proposed architecture, data flows, classification level, and operating model.

34	Page 43 – Network Isolation / Furnished Materials: There is a contradiction: Table mentions “transferred & deployed NATO-owned HSM/appliances” Paragraph states “NATO supplied: none” Can the Authority confirm that for LOT1 they will provide the HSM and the supplier will need a on-premise KMS and for Lot2 the Authority will use the NATO HSM to generate keys to be uploaded to the Public Cloud Providers KMS Service in a BYOK model?	No. Bidders should assume that no HSMs, KMS components, or other cryptographic appliances will be provided by NATO unless explicitly stated elsewhere in the RFP. It is the bidder's responsibility to propose the cryptographic architecture, including any HSM, KMS, BYOK, or HYOK capabilities required to meet the security, key management, and accreditation requirements of the solution. Any NATO-managed cryptographic services or key management arrangements will be addressed during the security design and accreditation process, if applicable.
35	**Implementation Schedule** Several milestones defined in Section 6 "Schedule of Milestones and Acceptance Criteria" appear to require the completion of activities that are dependent on post-award procurement and infrastructure deployment activities. For example: • Secure Connectivity Established (T0 + 2 months) requires encrypted connectivity to be established, tested and accepted, and 100 users onboarded. • Initial Cloud Deployment (T0 + 2 months) requires operational infrastructure to be deployed and accepted across multiple sites and implementation of baseline security controls. • COI Deployment (T0 + 3 months) requires four operational COIs supporting representative workflows and 100 concurrent users. Achievement of these acceptance criteria may depend on activities such	The implementation milestones defined in the RFP remains the baseline schedule for this procurement. Bidders may propose an alternative implementation approach or phasing to support delivery; however, proposals will be evaluated against the milestones and acceptance criteria specified in the RFP. Any proposed schedule deviations should be clearly identified and justified in the proposal.

	as procurement and deployment of specialised cryptographic equipment and associated approval, delivery and acceptance processes, procurement of dedicated server hardware & data center infrastructure (LAN, WAN, ...), delivery and customs clearance, installation, configuration, testing and formal acceptance, which can only commence following Contract Award. Would the Contracting Authority confirm whether bidders may propose an alternative implementation schedule as part of their solution and that such a schedule will be considered during evaluation, provided that the overall scope, objectives and required capabilities of the programme remain unchanged?	
36	**Payment Milestones** The payment schedule in Section 7 "Payment Milestones" allocates 20% of the contract value to each major milestone following Contract Award. Based on the milestone definitions and associated acceptance criteria, a significant proportion of project effort, expenditure, procurement commitments and delivery risk is expected to occur during the early phases of the programme. This includes activities such as procurement and deployment of specialised cryptographic equipment and associated approval, delivery and acceptance processes, procurement of dedicated server infrastructure, delivery and customs clearance, secure connectivity implementation, cloud infrastructure deployment, security	See Amendment 1 RFP. Payment plan % are to be proposed by Bidder as far as it respects the minimum % indicated in the table IN section 7 of the SOW.

	hardening, integration and testing activities. While bidders understand and support the principle that payments are linked to the successful acceptance of contractual deliverables, the proposed payment allocation may not fully reflect the distribution of effort, expenditure, procurement commitments and delivery risk across the different project phases. Would the Contracting Authority consider proposals for an alternative allocation of payment percentages across the defined milestones and associated acceptance events, provided that the overall contract value, milestone structure and acceptance-based payment mechanism remain unchanged?	
37	From the RFP: Bidders (including subcontractors, partners, and/or consortium members) shall hold a NATO SECRET Facility Security Clearance (FSC). The Proposed individual team members shall hold NATO Personnel Security Clearance (PSC) at a minimum of NATO SECRET, at the time of the start of performance of the Contract. 16. Physical Security - Personnel providing the services shall hold a valid NATO SECRET clearance, or national equivalent, at the time of bidding. Personnel performing administrative or privileged access functions may be required to hold COSMIC TOP SECRET (CTS) clearance in accordance with NATO security policy on the aggregation of NATO SECRET information.	**i.** No. The security requirements defined in the RFP remain applicable. Bidders must meet the specified NATO security requirements. Equivalent national clearances do not replace the required NATO Facility Security Clearance (FSC) where applicable. **ii.** No. This procurement will not be assigned a U.S. Defense Priorities and Allocations System (DPAS) rating. **iii.** Bidders may include support services within their proposed solution, provided they are consistent with the RFP requirements and the proposed pricing. **iv.** The RFP does not require Trade Agreements Act (TAA) compliance. Bidders are responsible for ensuring that all proposed equipment complies with the applicable NATO security, procurement, and contractual requirements.

	Clarification Questions i. Would NATO consider amending the RFP to allow for a US Department of War equivalent facility and US Clearances for this effort since the work will be performed on a US installation in Norfolk Virgina whilst we establish NATO FSC status for our US delivery team ii. Will this contract have or can a DPAS Rating ? - DPAS (Defense Priorities and Allocations System) ratings are U.S. government designations (DX or DO) placed on contracts to ensure timely delivery of resources for national defense and emergency preparedness. DX-rated orders have the highest priority, followed by DO-rated, which take precedence over unrated commercial orders. Due to the Silicon shortages the industry is experiencing prices and lead times for compute and store have dramatically increased to the point Dell, HPE, Cisco, etc. are only giving us quotes that are valid for 7 days, so it's that volatile right now iii. We will include 2 years of support to cover any gap from procurement to deployment. iv. Does the equipment need to be TAA compliant?	

38	Clarification regarding the Facility Security Clearance (FSC) requirements. However, our corporate entity does not currently hold a NATO SECRET FSC. Under the national regulations, a defense contractor cannot apply for an FSC independently; the application process must be officially initiated („sponsored“) by a public sector entity or procurement agency in connection with a specific requirement. Is it permissible to participate in the tender under the condition that the FSC application process is initiated upon contract award or during the evaluation phase?	Subject to the specific terms of RFP-ACT-SACT-26-54, NATO policy does not automatically exclude a bidder that does not yet hold the required FSC, provided no NATO CONFIDENTIAL/SECRET or above information must be held/generated at the bidder's facility during tendering. However, an appropriate NATO SECRET FSC must be confirmed before classified contract performance/award requirements are met and before any NC/NS information is released. Where no FSC exists, the Contracting Authority is responsible for initiating/supporting the FSC action with the competent NSA/DSA using the FSCIS process; the clearance decision remains with National Authority. HQ SACT may therefore initiate the required request/notification if bidder is selected and the RFP permits this timing, but cannot guarantee the granting or timeline of the FSC. Personnel PSCs alone do not replace the corporate FSC requirement.
39	Can the Authority confirm how our FSC locations will connect to the corporate NATO-S network, to enable us to support the SCS programme programme remotely and in particular how will NATO-S design documents be shared from CA until an assured network link between the Authority and our support location/s is implemented. What is the timeline to enable this connectivity to be put in-place and for the Authority to assure our FSC Locations/s to NATO-S?	The Authority cannot release NATO SECRET design information to, or permit remote support from, a contractor location until the relevant facility has the required FSC and any CIS used for storage/processing/transmission is appropriately security accredited. Any connection of contractor FSC locations to NATO SECRET/NATO CIS would require joint accreditation by the relevant national and NATO Security Accreditation Authorities; the contractor's capability to handle NATO classified information in CIS must be reflected in the FSCIS. Until such accredited connectivity exists, NATO-S design documents may only be shared through Authority-approved classified channels/procedures identified in the

		SAL/PSI, not over unaccredited corporate networks. The policy does not set a fixed timeline for establishing NATO-S connectivity or assuring FSC locations. The FSCIS reply may confirm existing FSC/CIS status or that the process has been initiated, but completion depends on the responsible NSA/DSA/SAA processes and successful accreditation.
40	For COI 3 & 4 AFSC and Maritime respectively the SOW describes that the suppliers responsibility is to support stakeholders to migrate these COI's to the two Cloud configurations. Can the Authority confirm that advice and support is the full extent of the obligations or will the supplier be expected to establish a relationship with the COI enabling technology venders to receive training as to how the technology works to provide an expert level of support services once the COI has been migrated, i.e. to enable changes, upgrades, configuration and patch maintenance.	The Contractor is responsible for providing the migration support and technical assistance necessary to achieve the objectives of the prototype. The RFP does not require the Contractor to become the long-term application support authority or to obtain expert-level knowledge of the COI applications beyond what is necessary to support migration, integration, testing, and validation. Any ongoing application maintenance, upgrades, configuration management, or vendor-specific support responsibilities will remain with the respective COI Application Owner or technology provider unless otherwise specified in the contract.
41	The HQ SACT General Terms and Conditions are structurally misaligned with the requirement for a cloud-based platform and appear more suited to the supply of physical deliverables. Several provisions are also commercially onerous from a liability perspective, including broad indemnification obligations, the absence of a stated limitation of liability, and one-sided or disproportionate dispute resolution and termination rights. While we anticipate being able to submit a largely compliant technical solution, we consider there to be a material challenge in confirming compliance with the proposed contract	1) HQ SACT reserves the right to negotiate minor deviations to the listed General Terms. If requested deviations are unacceptable by HQ SACT and they are not withdrawn by a bidder, then the bid will be considered non-compliant. 2) Bidders are expected to submit proposals that comply with the RFP requirements. Minor or non-substantial deviations may be identified in accordance with the RFP; however, ACT reserves the right to determine the materiality and

	terms without substantive amendments. Given that the Enclosure 2 Compliance Statement permits only minor or non-substantial deviations, please could you clarify the following: 1) If a bidder's Compliance Statement identifies material or substantial deviations from the proposed contract terms, would this result in automatic disqualification from the RFP, evaluation and bidding process? 2) Recognising that substantive amendments may be required to enable compliance, please confirm the extent to which the proposed terms are negotiable, particularly where amendments are necessary to align the contractual position with the RFP requirement and to address key commercial provisions that would otherwise impose unworkable liability on the supplier for delivery of the services.	acceptability of any proposed deviation during the evaluation process. Bidders should prepare their proposals based on the terms and conditions provided in the RFP and clearly identify any proposed deviations in the Compliance Statement. Proposals will be evaluated in accordance with the requirements of the solicitation.
42	"Could the Authority confirm that an NS-cleared prime contractor may submit a proposal relying on technology providers (originating from a NATO country) **not currently** in possession of an FSC @ NS, as long as all personnel taking part in the project are NS cleared?"	The Authority allows submission of a proposal with NATO-country technology providers that do not currently hold an NS FSC, provided that no NATO CONFIDENTIAL/SECRET information is released to, held at, or generated by those providers until the required FSC is confirmed. However, if those providers will act as sub-contractors requiring access to or generation of NATO SECRET information, personnel NS PSCs alone are not sufficient. Each relevant facility must hold, or be able to obtain, the appropriate FSC at the required level before classified performance/access is permitted. The Contracting Authority must verify the FSC with the responsible NSA/DSA through the FSCIS process, and where no FSC exists the FSC/upgrade

		action must be initiated in accordance with national procedures. Therefore: yes, proposal submission is not automatically precluded, but classified work by those providers would be conditional on obtaining the Contracting Authority approval and required NS FSC and any applicable CIS/safeguarding accreditation.
43	Enclosure 2: Compliance Statement We note that the Compliance Statement permits bidders to identify minor or non-substantial deviations; however, substantial changes shall be considered non-responsive. Please could the Contracting Officer clarify the following: 1) What is meant by "non-responsive" in this context? a. For example, if the Contracting Officer determines that a proposed deviation is substantial, would the bid be rejected in its entirety? b. Alternatively, would the deviation request itself be rejected, with the bidder then expected to comply with the original term or requirement? 2) Please could the Contracting Authority provide specific guidance and examples of deviations that would be considered minor, non-substantial or substantial in relation to the HQ SACT General Terms?	1) HQ SACT reserves the right to negotiate minor deviations to the listed General Terms. If deviations requested by bidders are unacceptable for HQ SACT and they are not, if subsequently asked by HQ SACT, withdrawn by a bidder, then the bid will be considered non-compliant. 2) Bidders are expected to submit proposals that comply with the RFP requirements, The Contracting Authority assesses any proposed deviations on a case-by-case basis, considering the specific parameters of the contract, its objectives, risk allocation, and impact on successful contract delivery. Therefore, no exhaustive or advance classification of minor, non-substantial, or substantial deviations can be provided.

44	Please confirm whether bidders may identify, within Enclosure 2, any mandatory third-party supplier/licensor terms required for the provision of cloud, software, support or security components, and whether HQ SACT will consider incorporation of such terms in addition to HQ SACT General Terms and Conditions where they are necessary for the delivery of the proposed, including the flow up of such terms to the contracting authority.	Section 37 of the HQ SACT General Terms and Conditions determines the order of precedence of the contractual pieces, thus third-party supplier/licensor terms required are part of the contract framework.
45	Section 4, pag. 5 Can you confirm that the Declaration of Eligibility for NATO Competitive Procurement is required for both Prime Contractor and Subcontractors?	Yes. Except for as otherwise provided in this Q&A (Question 74), a Declaration of Eligibility (DOE) is required for the Prime Contractor and any subcontractors performing work under the contract.
46	Enclosure 3, pag. 14 Can you confirm that the Past Performance Information Form requires to be signed by the Bidder Authorized Company Official?	Yes. The Past Performance Information Form shall be signed by the Bidder's Authorized Company Official. Additional supporting documentation may be included where appropriate to substantiate the reference.
47	Enclosure 3, pag. 14 Can you confirm that past performances references required could also be expressed even if the contract is still ongoing but the relevant activities for the RFP are completed? For example, operation services are still ongoing.	Yes. Past performance references may include ongoing contracts, provided the relevant activities demonstrating experience applicable to this RFP have been successfully completed. Bidders should clearly identify the completed scope and its relevance to the requirements of this procurement.
48	Enclosure 3, pag. 14 The Bidder is required to submit a minimum of two (2) past performance references. Could you please confirm that this corresponds to one reference per Lot? In case of partial bidding (1 Lot out of 2), can you confirm that the limit is one reference?	The requirement is to provide a minimum of two (2) past performance references per Lot. See amended RFP.

49	Section 11, pag. 7 Section 11 (Content of Proposal), point a), outlines the required contents of the Technical Proposal. However, it does not specify any requirement for bidders to describe how they intend to meet the technical requirements. Could you please confirm whether bidders are free to structure and present the documentation using their preferred format and table of contents?	Bidders are free to structure their technical offers as they see fit as far as it contains the minimum list of documents stated in section 11. Bidders shall indeed describe how they intend to meet the technical requirements For financial offer, the mandatory price structure (enclosure 4) shall be respected to ensure fair price comparison between bidders.
50	SoW, Section 2, pag. 19 Statement of Work, Section 2 (Background and Scope of Work), point c), outlines the primary objectives of Lot 1, which include the following: 'Demonstrate and validate a federated, distributed, zero-trust-aligned cloud architecture grounded in NIST SP 800-207 and NATO Security Policy, and hosted in data centres distributed across at least four sites in three different NATO countries'. Meanwhile, Table 1 (Compliance Evaluation Criteria) awards points to solutions that include fewer sites than the minimum specified, with the sole exclusion criterion being a single site, which results in 0 points. Could you please confirm that the SoW expresses the ideal requirement, but that the other options that earn points also constitute compliance?	The minimum technical requirements are those defined in the Statement of Work. The Best Value scoring criteria are intended to differentiate between compliant proposals based on the degree to which they satisfy or exceed the evaluation criteria. To be considered compliant, proposals must meet the mandatory requirements of the RFP. The evaluation matrix does not modify or relax those mandatory requirements. Please refer as well to Appendix G – Compliance Matrix and Evaluation Criteria
51	Best Value Criteria Matrix Lot 1, pag. 91 In the Best Value Criteria Matrix for Lot 1, row no. 4 (“Performance and Resilience in Isolated Environment: Ability to meet performance and availability targets under failure scenarios”), the maximum score assigned to the criterion is indicated as 10 points; however, in the range classification, the maximum score stated is 20 points.	The maximum score for Lot 1, Serial 4 is 10 points. The corrected scoring criteria are as follows: • 0 pts: No SLA or failover capability. • 2.5 pts: Single-node deployment or no redundancy. • 5 pts: At least one redundancy mechanism, compute or network. • 7.5 pts: Multi-site failover with RTO ≤ 4 hours and RPO ≤ 1 hour. • 10 pts: Full multi-site resilience with RTO ≤ 1 hour and RPO ≤ 15 minutes under a tested failure scenario.

	Could you kindly clarify which is the correct maximum score?	This correction supersedes the scoring breakdown currently reflected in the RFP. All Proposals will be evaluated using the revised 10-point scale above. See amended RFP (amendment 1)
52	SOW Introduction, pag. 18 Given that the SCS prototypes are described as pre-accreditation validation and sandbox environments, could HQ SACT confirm whether the use of representative or synthetic datasets mirroring realistic NATO SECRET data structures and workflows but not containing actual classified information is acceptable, provided all security controls, processes, and accreditation requirements for handling NATO SECRET data are fully implemented?	Yes. Bidders may use representative or synthetic datasets for the prototype, provided they adequately demonstrate the required functionality, security controls, operational processes, and accreditation evidence. The use of synthetic data does not remove the requirement for the proposed solution to meet the NATO SECRET security and accreditation requirements defined in the RFP.
53	SOW, pag. 19 Could HQ SACT clarify how the evaluation will discriminate between solutions with an existing high-assurance, pre-accredited (e.g., NSA-aligned) design and those developed specifically for this prototype? In particular, will the maturity and readiness of the accreditation approach (including prior validation, documentation, and evidence frameworks) be explicitly assessed? Additionally, is it expected that bidders describe in detail their planned accreditation process and supporting artefacts within the proposal?	The evaluation will be based solely on the criteria defined in the RFP. Existing accreditation or prior validation may be included as supporting evidence of solution maturity but will not be evaluated as a separate criterion. Bidders should describe their proposed approach to supporting the NATO security accreditation process, including the generation of accreditation evidence and key supporting artefacts, as part of their technical proposal.
54	Best Value Criteria Matrix Lot 1 & Lot 2, from pag. 89 Considering that one of the primary objectives of the SCS prototypes is to support NATO security accreditation through evidence generation and validation activities, could HQ SACT clarify whether,	The Best Value evaluation will be conducted using the criteria defined in the RFP. A bidder's approach to supporting security accreditation will be assessed where it is reflected in the applicable evaluation criteria, such as security, architecture, compliance, and the quality of the proposed technical solution.

	and to what extent, the proposed approach to accreditation (e.g., ease of accreditation, maturity of accreditation artefacts, and alignment with accreditation processes) will be explicitly evaluated as part of the technical assessment, or if it is only indirectly assessed through existing criteria such as security controls, architecture, and compliance?	No separate evaluation criterion will be applied specifically for accreditation unless explicitly identified in the RFP.
55	The RFP states that prices shall be on a Firm Fixed Price Basis. Can the Authority confirm which elements of the pricing are Firm and which are Fixed? Can the Authority confirm that the Fixed elements will be subject to Indexation? Or whether all pricing needs to be at outturn economic conditions and provision for cost inflation within pricing?	The RFP requires bidders to submit a Firm Fixed Price proposal for all contract deliverables. Unless otherwise specified in the contract, prices shall remain fixed for the contract period and should include all anticipated costs, including inflation and other economic factors. No separate indexation or price adjustment mechanism is provided under the RFP.
56	We note that any requested deviations, adjustments or considerations regarding the HQ SACT General Terms and Conditions must be identified in the Enclosure 2 Compliance Certificate. While this is understood, please can you confirm whether bidders are also permitted to submit a separate tracked-change redline/mark-up of the HQ SACT General Terms and Conditions to clearly identify the requested deviations to the terms?	Bidders shall identify any requested deviations in the Enclosure 2 Compliance Certificate as required by the RFP. .
57	The RFP states that all proposed individual team members shall hold a minimum NATO SECRET Personnel Security Clearance. Does this requirement apply to all named personnel included in the proposal, or only to personnel requiring privileged administrative access, physical access, or on-site support?	The NATO SECRET Personnel Security Clearance requirement applies to all personnel requiring access to NATO classified information, systems, facilities, or any contract activities performed either at the Contractor facility or/and ACT. Bidders should ensure that all personnel requiring such access hold the appropriate clearance by the start of contract performance. Uncleared Personnel who do not require access to NATO classified

		information shall not be granted access to such information.
58	The RFP requires Lot 1 to be operational across four different sites in three NATO member nations by T0+4 months. Are all four sites expected to be fully established and available at contract award, or is a phased deployment approach acceptable provided that the T0+4 milestone is achieved?	A phased deployment approach is acceptable, provided the required milestone is achieved by T0+2 months for 2 sites and T0+4 months for 4 sites. Bidders should clearly describe their deployment approach, including key assumptions, dependencies, and how the required capability will be operational across the four sites by the specified milestone.
59	The RFP specifies that all cloud services shall be hosted and operated within NATO member nations. Does this requirement also apply to backup data, disaster recovery replicas, telemetry, support logs, monitoring data, and vendor support metadata?	Yes. Unless otherwise authorized by the Contracting Officer, all data associated with the service including backup data, disaster recovery replicas, telemetry, support logs, monitoring data, and other operational data shall be hosted and managed within NATO member nations in accordance with the RFP's data sovereignty and security requirements. Bidders should clearly identify any assumptions or exceptions in their proposal.
60	Is the Cross Domain Solution expected to be fully contractor-supplied, or may NATO-furnished or government-approved CDS components be integrated into the proposed solution?	The RFP does not prescribe a specific Cross Domain Solution (CDS) implementation. Bidders may propose either a fully contractor-supplied CDS or the integration of NATO-furnished or government-approved CDS components, where available. The proposed solution must meet the RFP's security, interoperability, and accreditation requirements.
61	The RFP references NATO cryptographic hardware and Hardware Security Modules. Are these expected to be supplied by the contractor, provided by NATO, or would functionally equivalent commercial HSM solutions be acceptable for the prototype?	Unless explicitly stated otherwise in the RFP, bidders should assume that all cryptographic hardware, including Hardware Security Modules (HSMs), is to be provided as part of the proposed solution. Functionally equivalent commercial HSM solutions are acceptable for the prototype, provided they meet the RFP's security, key management, and accreditation requirements. Any final cryptographic solution will be subject to NATO security and accreditation approval.

62	For the Secure Digital Workspace COI, are bidders expected to provide a commercial off-the-shelf solution, an open-source secure collaboration platform, or would a contractor-developed integrated workspace solution also be considered compliant?	Bidders may preferably propose a commercial off-the-shelf, contractor developed integrated workspace or open-source solution, similar to what is generally used in NATO or similar public/international organizations and provided it meets the functional, security, performance, and interoperability requirements of the RFP and supports the stated objectives of the COI.
63	The RFP refers to a commercial air-gapped multimodal AI capability. Is the AI model licence expected to be provided by the contractor, and does NATO maintain a list of approved AI models that bidders should use?	The RFP requires the Contractor to deliver an operational turnkey Secure Generative AI COI. Bidders should therefore include any AI model licences, tools, hosting platform, support, and dependencies required for their proposed solution, including any commercial air-gapped multimodal AI capability. The RFP does not identify a NATO-approved list of AI models for bidders to use. Proposed AI models and platforms must meet the RFP requirements, including isolation, no connection to external AI services or public endpoints, NATO operational control, security controls, auditability, data protection, and accreditation requirements.
64	The RFP specifies a response time of less than two seconds for 100 concurrent users. Could NATO clarify the assumptions used for this performance requirement, including expected prompt length, context window size, RAG corpus size, and approximate model parameter range?	The RFP specifies the performance requirement but does not define the detailed benchmark assumptions requested, including prompt length, context window size, RAG corpus size, or model parameter range. Bidders should therefore state the assumptions used in their proposal for demonstrating the response-time requirement, including workload profile, user concurrency, model configuration, retrieval approach, dataset/corpus size, prompt and context assumptions, and test methodology. Final validation will be based on the bidder's ability to meet the RFP performance, security, isolation, and operational requirements under the agreed test conditions.

65	The RFP refers to 100 end-user devices across both lots. If a bidder submits a proposal for only one lot, should the proposal include 100 end-user devices or only the proportion applicable to that lot?	A bidder proposing only one lot should include the end-user devices applicable to that lot. The RFP states that the contractor shall procure and deliver 100 total end-user devices across both lots, i.e. 50 per lot. Therefore, a bidder submitting a proposal for one lot should include 50 end-user devices for that lot, unless otherwise specified in the RFP. Bidders should clearly identify the quantity, configuration, delivery location assumptions, and any associated authentication devices included in their proposal.
66	The RFP refers to 100 pilot users across both lots. How should this requirement be interpreted for bidders proposing only a single lot?	A bidder proposing only one lot should interpret the pilot-user requirement as applicable to that lot. The RFP states that the User locations must be prepared to receive and distribute secure cloud services to 100 total pilot users across both lots, i.e. 50 per lot. Therefore, a bidder submitting a proposal for one lot should plan for 50 concurrent pilot users for that lot. Number of accounts can be greater than the number of concurrent connection. Bidders should clearly identify any assumptions regarding user onboarding, device allocation, authentication devices, access management, and support for the proposed lot.
67	The RFP requires dedicated secure connectivity between the contractor environment and two User Headquarters locations. Could NATO identify the relevant countries and/or locations, or provide the network demarcation points required for accurate connectivity pricing?	For planning purposes, bidders should assume two NATO user locations within the NATO enterprise environment, one in North America and one in Europe. The specific countries, locations, and demarcation points will be provided to the successful contractor during contract execution and solution design activities. Bidders should propose a solution capable of supporting secure connectivity to two geographically separated NATO sites and clearly identify pricing assumptions regarding

		geography, bandwidth, latency, circuit type, demarcation, and connectivity dependencies.
68	As dedicated leased-line and cross-border connectivity costs are location dependent, would NATO accept pricing based on clearly documented assumptions where final connectivity locations have not yet been disclosed?	Yes. Where final connectivity locations have not been disclosed, bidders may price on the basis of clearly documented assumptions. Assumption should at least include one site in North America (Norfolk, VA, USA) and one in Europe. Bidders should identify the assumptions used, including geography, bandwidth, latency, circuit type, demarcation, cross-border connectivity, lead times, dependencies, and any exclusions or pricing sensitivities. Bidders remain responsible for proposing a solution that satisfies the secure connectivity requirements of the RFP.
69	Could NATO clarify how reusable platform components, pre-existing software modules, orchestration code, automation assets, templates, and existing AI platform capabilities will be distinguished from Foreground Intellectual Property developed specifically under this contract?	Pre-existing intellectual property (background IP), including reusable platform components, software modules, orchestration code, automation assets, templates, and existing AI capabilities, will remain the property of the bidder or the applicable third party. Only intellectual property developed specifically under this contract will be owned by HQ SACT, according to Section 19 of the SOW of the RFP . Bidders should clearly identify any pre-existing intellectual property incorporated into their proposed solution. Please see answer # 12 and 13
70	Compliance matrix- Migration Sandbox in Air-Gapped Context: Ability to onboard and validate applications in an isolated environment. Tab1 #6 and Tab 2 #5 Could you please clarify acceptable means to demonstrate Migration Sandbox capability?	Bidders should demonstrate how their proposed Migration Sandbox supports the secure onboarding, migration, testing, and validation of applications in an isolated environment. A description of the proposed architecture, workflow, security controls, and migration process is sufficient to demonstrate compliance with this requirement.

71	Compliance matrix- Community of Interest workflows - Secure Digital Workspace, Secure Generative AI, Allied Federated Surveillance and Control (AFSC), and Centre for Maritime Research and Experimentation (CMRE). Tab1 #7 and Tab 2 #6 Given offerrors' lack of access to the listed COIs pre-award, could you please clarify acceptable means to demonstrate capability? Would description of the workflow for deployment and transition to operations, on the proposed architecture, suffice to demonstrate capability?	Yes. As bidders will not have pre-award access to the identified COIs, ACT will accept a description of the proposed workflow, deployment approach, and transition to operations as evidence of capability. The response should demonstrate how the proposed solution supports the onboarding, migration, integration, and operation of the representative COIs in accordance with the RFP requirements.
72	Price Proposal The pricing tabs are lot specific. Could you please clarify how discounts resulting from a single vendor providing both lots, when applicable, should be documented? One possible way to handle this is adding a third tab for Combined Lot #1 and Lot #2 pricing.	Bidders shall complete the price proposal separately for each lot using the provided pricing templates. If a bidder wishes to offer a discount contingent upon the award of both lots, this may be submitted as a separate pricing attachment or accompanying narrative.
73	4. Eligibility, Subparagraph f “ The Proposed individual team members shall hold NATO Personnel Security Clearance (PSC) at a minimum of NATO SECRET, at the time of the start of performance of the Contract.” Is Contractor access to NATO SECRET or above data required upon contract award? If so, how will the access be provided (e.g. networks, accounts, etc.)?	Access to NATO SECRET information, systems, or facilities will be provided only where required to perform the contract and in accordance with applicable NATO security policies. Any required accounts, network access, or other access mechanisms will be coordinated with the successful contractor during contract execution and will be granted only to appropriately cleared personnel on a need-to-know basis.
74	4.Eligibility, Subparagraph c “ A Declaration of Eligibility (DOE, as per enclosure 5) issued by the appropriate national authority of the Bidders nation of origin is required for prime and subcontractors.”	The Declaration of Eligibility (DOE) requirement applies to the Prime Contractor and any subcontractors performing work under the contract (where the Prime delegates a portion of the contract deliverables to a third party).

	Could you please clarify if this requirement also applies to suppliers of HW/SW or leased services (e.g. telco)?	Suppliers of laptops, tablets, security/smart cards are not required to provide a DOE for this RFP. Except for the case mentioned above, suppliers of raw material, commercial hardware, software, or leased services (e.g., telecommunications providers) are not crequired and are not required to provide a DOE
75	11.Content of Proposal, Subparagraph a Could you please clarify where in the Technical Volume the offerors should describe target architecture and delivery approach for the prototypes?	The target architecture and delivery approach should be described within the Technical Volume as part of the bidder's response to the Statement of Work and technical requirements. Bidders may organize the Technical Volume as they consider appropriate, provided the proposal clearly addresses all RFP requirements and enables the evaluation team to assess compliance.
76	Enclosure 4 – Mandatory Price Proposal Excel Spreadsheet Could you please clarify if price assumptions (e.g., FTE hours, escalation rate, currency conversion rate, BOEs, etc.) are to be submitted in the price proposal ?	Yes. Bidders may include pricing assumptions as , such as FTE hours, escalation rates, currency exchange rates, and the basis of estimate (BOE), to support their price proposal. Any assumptions should be clearly identified, consistent with the RFP requirements, and must not alter the Firm Fixed Price nature of the proposal.
77	2. Background and Scope of Work “ Establish a direct, dedicated secure connection between the User Headquarters (two locations) and the contractor datacentres” Could you please identify the two User Headquarters locations to be connected? If the two locations are yet TBD, please provide locations to be used in pricing the network connections to contractor's datacentres.	The two User Headquarters locations have not yet been finalized. For proposal purposes, bidders should assume two NATO user headquarters within the NATO enterprise environment, one in North America, one in Europe. Bidders should base their pricing on reasonable planning assumptions and clearly identify those assumptions in their proposals. The specific locations will be provided to the successful bidder(s) during contract execution.

78	2. Background and Scope of Work “ (unedr part c) 'two User Headquarters locations'” Is the 'two User Headquarters locations' a total requirement across both lots, or does each lot require separate connections to the same two user HQ locations or two separate ones? Is the target throughput specified for each HQ location and for both lots, or is that the requirements for each HQ loaction and each lot?	For proposal purposes, bidders should assume that each lot requires connectivity to the same two designated NATO user headquarters locations. The stated throughput requirements apply independently to each lot. Any site-specific connectivity details will be provided to the successful contractor during implementation.
79	2. Background and Scope of Work “ (under 2 d) The primary objectives for LOT 2 (Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing)” Could you please clarify if for Lot #2 there is a requirements for the datacenters or cloud regions to be physically located in multiple NATO contries?	Yes, Lot 2 requires the datacenters or cloud regions to be physically located in multiple NATO countries following at least the similar criteria as for lot 1 (4 sites, 3 NATO countries). Bidders should propose a hosting architecture that meets the RFP's security, data sovereignty, resilience, and accreditation requirements. Any assumptions regarding cloud region selection should be clearly identified in the proposal.
80	2. Background and Scope of Work “ (under 2.c.8)Leverage Cross Domain Solution (CDS) to enable controlled, automated data transfer and secure delivery of updates and patches into air-gapped environments.” Could you please clarify the types of data to be transferred through the CDS, and associated target performance requirements?	The RFP does not prescribe specific data types or performance requirements for the Cross Domain Solution (CDS). Bidders should assume the CDS will support the secure transfer of approved data, software updates, patches, and other authorized content required to operate and maintain the solution. Any assumptions regarding throughput, latency, or transfer volumes should be clearly identified in the proposal.
81	2. Background and Scope of Work “ (unedr c) Test Confidentiality, Integrity, and Availability (CIA) cyber security measures within a well-architected cloud environment.” Could you please clarify what C-I-A levels are expected? Would Moderate be	The RFP does not prescribe specific Confidentiality, Integrity, and Availability (CIA) impact levels. Bidders should propose a security architecture appropriate for processing NATO SECRET information and aligned with the applicable NATO security policies and accreditation requirements.

	acceptable or is High required in any of the areas?	The selected CIA levels and associated security controls should be justified as part of the bidder's proposed solution and will be assessed during the NATO security accreditation process.
82	5. Tasking and Deliverables "A. [...] The contractor shall demonstrate modern security architecture based on Zero Trust principles, aligned with National Institute of Standards and Technology SP 800-207, and shall support iterative security testing, technical assessments, vulnerability remediation, and the generation of accreditation evidence required by NATO security authorities." Could you please clarify contractor support responsibilities for the areas listed? On one end of the espectrum, the Contractor could be responsible for the development and execution of tests, remediation of vulnerabilities, and generation of evidence. On the other end, the NATO personnel perform these activities and Contractor is available to answer questions and troubleshoot / reconfigure the prototype.	The Contractor is expected to provide active support for security accreditation and validation, not merely passive question-and-answer support. For the contractor-provided solution, this includes supporting security test planning and execution, technical assessments, vulnerability assessment activities, remediation or mitigation of findings within the Contractor's scope of control, and generation of accreditation evidence and audit-ready artefacts required by the RFP. NATO security authorities retain responsibility for accreditation decisions and may direct, witness, review, or conduct independent assessment activities. The Contractor shall support those activities by providing access, documentation, test results, risk assessments, remediation plans, technical explanations, troubleshooting, and configuration changes as required for the prototype. Where a finding relates to a third-party component, NATO dependency, or item outside the Contractor's direct control, the Contractor shall identify the dependency, assess the impact, and propose an appropriate remediation or mitigation approach.
83	5. Tasking and Deliverables " A.3. [...] The architecture must also ensure high availability and resilience, including distribution across multiple locations to maintain operations during failure scenarios." Could you please provide more context on the data flows that need to be maintained, the failure scenarios in which those data	The RFP defines the required operational outcomes but does not prescribe specific data flows, failure scenarios, or availability targets for the prototype. Bidders should propose an architecture that demonstrates resilience and continuity of operations under representative failure scenarios. Any assumptions regarding data flows, availability, and recovery objectives should be clearly described and justified in the proposal.

	flows need to be available and a quantitative value for the availability?	
84	5. Tasking and Deliverables “ a.5. The solution shall [...] Provide audit-ready evidence of compliance and security controls” Based on earlier information in the Statement of Work (page 18), the requirement is to enable generation of auditbable evidence aligned with NATO Security Policy and NIST SP 800-53r5. Understanding the CIA impact values that are required for the SCS drives the security controls selected for implementation. Is NATO maintaining a common set of security controls baselines for use by all memebers or is this a design choice open to the offerrors?	The RFP identifies applicable NATO security policies, accreditation requirements, and required audit-ready evidence, but does not provide a single common CIA impact categorisation or security-control baseline for bidders to apply. Bidders should propose and justify the security control baseline for their solution, appropriate to an environment intended to support information up to and including NATO SECRET, and map those controls to applicable NATO security policies, NIST SP 800-53 Rev. 5 where applicable, Zero Trust principles, and the RFP requirements. The proposed baseline, control implementation, evidence-generation approach, and any gaps or assumptions should be clearly described in the proposal. Final acceptability of the control baseline and evidence package will be determined through the NATO security and accreditation process.
85	E.2. Proof of Concept Demonstration “ The contractor shall demonstrate: • Secure Connectivity: Validated, end-to-end secure link between HQ and cloud environment • Data Sovereignty: NATO retains full ownership and control of data within the cloud • COI Migrations Validity: Migrated applications meet operational and performance requirements • Zero Trust and Data-Centric Security: Architecture enforces defined security principles” Is the COI Migrations Validity a Contractoror or a COI Application Owner function?	The Contractor is responsible for demonstrating that the migration process and hosting environment support the successful operation of the migrated COI applications. The COI Application Owner remains responsible for validating application functionality and operational suitability. Acceptance of the migrated application will be a collaborative activity between the Contractor, the COI Application Owner, and ACT.

86	F. User Location Infrastructure Requirements Could you please provide any constraints (e.g., space, power, grounding, etc.) at the designated NATO sites where the SCS contractor infrastructure will be delivered? Should specifics on NATO provided facility infrastructure / site prep services (e.g. cabling within facility) be addressed in Section 15 (Furnished Materials and Services)?	NATO does not intend to host major infrastructure for SCS, only secure line endpoint.
87	18. Applicable security policies Could you please clarify where official copies of the listed security policies (as well as any other standards referenced in the RFP) could be obtained by prospective offerrors? Could SACT create a bidders library with all the documents referenced from the RFP?	*Answer under finalization- Bidders will be communicated an email address to request the referenced documents*
88	Appendix A – Security Accreditation and Validation Requirements 1.4. The prototype shall test multiple Key Management System (KMS) deployment models, including: BYOE (Bring Your Own Encryption): o No contractor-hosted KMS o NATO retains full control of encryption keys, segregated from cloud infrastructure o Test scenarios shall assess data flow latency and operational impact Will Type I crypto be required to support this effort?	The RFP does not mandate the use of a specific cryptographic product or Type I encryption device. Bidders should propose a cryptographic solution that meets the NATO SECRET security, key management, and accreditation requirements of the RFP. Any specific cryptographic requirements, including the use of NATO-approved cryptographic devices, will be determined through the NATO security and accreditation process.
89	Section 1.8.3 Data In Use “ The Process: 1. The encrypted data enters the Enclave. 2. The Enclave proves its identity to the NATO On-Prem Hardware via Cryptographic Attestation.	The RFP does not prescribe a specific media sanitization method. Bidders should propose a data sanitization approach that complies with applicable NATO security policies and recognized industry standards, such as NIST SP 800-88, where appropriate.

	3. Once verified, the On-Prem Hardware provides the session key needed to decrypt the data only inside that protected memory space. 4. Data is decrypted, processed, and re-encrypted before leaving the CPU's secure boundary." How should encrypted/sensitive data be sanitized when: 1. No longer needed 2. Due to HW maintenance / retirement requirement What process is preferred to sanitize data at rest and Equipment that has processed data (NIST SP 800-88/Media Sanitization)?	The proposed solution should include procedures for securely sanitizing data that is no longer required and for handling equipment maintenance, replacement, or retirement to ensure that no recoverable NATO data remains.
90	Appendix A, Lot 2, 1.10.4.2 Data Ingestion and Handling " Controlled mechanisms to **ingest** application data into the sandbox environment" How often will this ingest need to occur? Does this ingest need to occur real-time, batch (automated/scheduled or manual), or both? What is the volume of the data to be ingested? Are any transformations of the data required as part of ingest?	The RFP does not prescribe a specific ingestion frequency, data volume, or ingestion method. Bidders should propose an approach that best supports the intended use of the Application Migration Sandbox. The solution should be capable of supporting both manual and automated data ingestion, as appropriate. Any data transformation required to enable migration, testing, or validation of applications within the sandbox should be included as part of the proposed solution.
91	Appendix B.1.5 Acceptance Criteria " AI Response Speed - Response time <2 seconds for standard queries with 100 concurrent users" Could you please verify corectness of this requirement for the Secure Generative AI COI only, considering that each lot has 50 users?	The requirement applies to the Secure Generative AI COI only. For the prototype, bidders should assume up to 50 concurrent users per lot.

92	Statement of Work 5 Tasking and Deliverables - A.6 Development Environment and B. Application Migration and Cloud Readiness "Enable a controlled development and testing environment supporting application onboarding and deployment within the Application Migration Sandbox" and "The Contractor shall provide and operate a secure Application Migration Sandbox" Should development and test environments (and Sandbox) be sized separately from the COI requirements specified, or are dev/test workloads included in the stated resource numbers? If separate, what percentage of production capacity should we allocate for dev/test?	The resource estimates provided in the RFP are intended for the operational prototype environment and do not include dedicated development, test, or sandbox capacity. Bidders should size the development, test, and Application Migration Sandbox environments as appropriate for their proposed solution. The RFP does not prescribe a specific percentage of production capacity for these environments.
93	Appendix D - Section 1.5 “ The architecture must also ensure high availability and resilience, including distribution across multiple locations to maintain operations during failure scenarios.” The RFP states 'high availability and resilience' is required (page 23), but also states 'High availability / failover needed: Not required at this stage' (page 67, Maritime COI). Please clarify requirements for availability and restotarion time for the prototype and, if different, for each COI?	The prototype is intended to demonstrate an architecture that supports high availability and resilience. It is not required to provide full operational failover for every COI during the prototype phase. Where a COI states that "high availability/failover is not required at this stage," this applies only to that prototype use case. Bidders should demonstrate that their proposed architecture can support high availability and resilience in a future operational deployment. No specific restoration time (RTO) is prescribed for the prototype unless explicitly stated for a particular requirement.
94	Appendix D - Section 1.5, and Appendix C - Section 1.9 “ (e.g., 264 vCPUs for AFSC + 264 vCPUs for Maritime = 528 total)” Could you please clarify the requirements for the Compute/Storage Resources? Specifically: (1) Are the vCPUs per COI or shared across the COIs?	The compute and storage figures provided in the RFP are planning estimates for the prototype environment. 1. The stated vCPU and storage requirements should be treated as cumulative across the proposed COIs unless otherwise specified. 2. Bidders should include reasonable infrastructure overhead and capacity margin to support stable operation of the proposed solution.

	(2) Are infrastructure overhead and margin included in the compute and storage requirements? (3) Are backup and disaster recovery storage needs included in the stated requirements? (4) What backup retention RPO / RTO targets should be used?	3. Backup and disaster recovery storage are not included in the stated capacity estimates and should be sized by the bidder based on the proposed architecture. 4. No specific backup retention, RPO, or RTO values are prescribed for the prototype. Bidders should propose appropriate values that align with their solution and meet the resilience and operational objectives of the RFP.
95	Section 1.5. Storage and Compute Requirements “ Preferred technology: Logical airgap (current architecture is cloud-hosted on Azure; physical airgap is not currently in use but can be evaluated if required). [...] The platform currently uses Azure Data Lake Storage Gen2 (ADLS Gen2) as the shared storage backend for all Databricks clusters and ingestion pipelines.” Current use of Azure is noted for the Maritime Operations COI. Do other COIs have preferred technology? Is the expectation that the current preferred technology is replicated in the SCS solution(s)?	The references to Azure and ADLS Gen2 describe the current environment for the Maritime Operations COI and should not be interpreted as a mandatory technology requirement. The other COIs do not have prescribed technology stacks. Bidders may propose equivalent technologies, provided they meet the functional, security, and performance requirements of the RFP and support the successful migration and operation of the applicable COI.
96	n/a - general Please clarify external SCS interfaces for data ingest into SCS from other NATO systems relevant to the initial COIs? Is data ingest/distribution into SCS from other NATO systems or from SCS to other NATO systems within SCS scope or handled separately by NATO end users?	The initial COIs are intended to demonstrate representative integration capabilities. Bidders should assume that any interfaces required to support the defined COIs are within the scope of the proposed solution. Broader integration with other NATO systems beyond the defined COIs is outside the scope of this procurement and will be addressed separately as part of future implementation activities.
97	Appendix B.1.5 Acceptance Criteria “ AI Response Speed - Response time <2 seconds for standard queries with 100 concurrent users”	The intent of this requirement is to measure the responsiveness of the Secure Generative AI capability during normal user interaction. A "standard query" should be interpreted as a typical user request using Retrieval-Augmented Generation (RAG), involving

	What is the definition of a standard query? What is the polling rate of the users?	retrieval of relevant information from the approved knowledge base and generation of a concise response. The RFP does not prescribe a specific prompt length, context size, output length, or user polling rate. Bidders should clearly define the assumptions used for performance testing, including the representative query profile, request frequency, concurrency model, and measurement methodology, and demonstrate that the proposed solution can achieve the required response time under those conditions.
98	The RFP states that Bidders (including subcontractors, partners and/or consortium members) shall hold a NATO SECRET Facility Security Clearance (FSC) and that Proposed individual team members shall hold NATO Personnel Security Clearance (PSC) at a minimum of NATO SECRET, at the time of the start of performance of the Contract. Where a NATO clearance is not currently held, can the Authority confirm whether a National SECRET clearance for either personnel or FSC can be accepted at the start of the contract while a NATO clearance is being processed.	A National clearance is not acceptable to start the performance of the contract, a NATO FSC must be hold prior to the beginning of any classified contract phase. Contractor's personnel requiring access to NATO Classified Information, NATO classified systems or NATO classified facilities must hold a NATO PSC at the required level of classification prior to the start of any classified activity and access to classified information. The Facility Security Clearance is as stated in the RFP: bidders, including subcontractors, partners and/or consortium members, shall hold a NATO SECRET FSC at the time of the start of performance of the Contract. The RFP does not provide for a national facility clearance to be accepted in lieu of NATO SECRET FSC while NATO FSC is being processed.
99	Can the Authority confirm that both lot 1 & lot 2 cloud configurations will integrate (via log collection / SIEM tool) into an existing NATO SOC Service and that the relevant SIEM skills will be provided by the Authority as GFX. The suppliers responsibility is to ensure the relevant audit logs are made available to the Authority SIEM team/tooling.	The Authority expects both Lot 1 and Lot 2 solutions to provide comprehensive audit logging and security monitoring capabilities. Bidders shall ensure that relevant logs, events, and security telemetry can be made available to NATO monitoring and security management services through standard integration mechanisms.

		However, bidders should not assume that all SIEM, SOC, tooling, integration services, or specialist skills will be provided as Government-Furnished Equipment/Services (GFE/GFS). Bidders remain responsible for delivering a complete and operational solution, including any components, integrations, and services necessary to meet the security, monitoring, and operational requirements defined in the RFP.
100	In the SOW in Appendix A 1.7, the table refers to a NATO Crypto Hardware, Transferred & Deployed: NATO-owned HSMs/appliances. However, in the Furnished Materials and Services section it states that there are NO NATO Furnished Assets. Can the Authority confirm the position please.	The Authority confirms that no NATO Furnished Assets (GFE/GFX) are planned to be provided under this contract. The reference in Appendix A 1.7 to "NATO Crypto Hardware, Transferred & Deployed" should not be interpreted as Government-Furnished Equipment. Bidders are responsible for providing all cryptographic hardware, HSMs, appliances, licences, and associated components required to deliver a fully compliant solution. Any references suggesting the provision of NATO-owned cryptographic assets should be considered informational only and do not constitute a commitment by the Authority to furnish such equipment.
101	The Authority has requested 10Gbps through-put, requiring 8 dedicated lines per lot between 2 ACT sites and 4 industrial sites Total: 16 lines if two separate hosting arrangements between the LOTs. Please can the Authority advise if this has been included in its budget calculations?	***See response to Question 31.*** Bidders are responsible for proposing a connectivity architecture that meets the RFP performance, security, resilience, and accreditation requirements and for including associated connectivity costs in their proposal. Bidders should not assume a fixed number of dedicated circuits unless required by their proposed architecture. Any assumptions regarding circuit count, bandwidth, routing, resilience, carrier lead times, pricing, and delivery dependencies shall be clearly identified in the proposal. ***This response also addresses Question 790.***

102	Given the complexity, multi-lot scope of the requirement, and the upcoming vacation period, does HQ SACT foresee the possibility of an extension to the bid submission deadline (currently stated as 27 July 2026, 0900 hours EST)? A two to three week extension would allow us to submit a better-quality bid given key personnel will be on vacation at differing times during the response period.	Please refer to Amendment 1 RFP for revised submission deadline. This response also addresses Question 674.
	Due to volume of questions received, an incremental release of Q&A will be done on HQ SACT Contracting page for this RFP	