HQ Supreme Allied Commander Transformation
Purchasing and Contracting Section
Office of Budget and Finance

Request for Proposal

RFP-ACT-SACT-26-54

Secure Cloud Service

The publication of this RFP does not constitute a commitment to award a contract. This Procurement Opportunity is still pending validation of funding and approvals.

HQ SACT reserves the right to cancel, withdraw, or suspend at any time, this RFP either partially or in its entirety. No legal liability on the part of HQ SACT shall be considered for recovery of costs in connection to bid preparation. All efforts undertaken by any bidder shall be done considering and accepting, that no costs shall be recovered from HQ SACT.

BIDDING INSTRUCTIONS

1. General

a. Headquarters Supreme Allied Commander Transformation (HQ SACT) intends to utilize NATO Competitive Procurement to award contract(s) for Secure Cloud Services (SCS) requirements.

b. The SCS aims to prototype a secure off-premises cloud capability up to and including NATO SECRET to support NATO's transition toward modern, data-driven operations, AI-enabled decision-making, and multi-domain mission integration.

c. To award the contract(s), HQ SACT will apply a Sealed Bidding Procedure in accordance with the Procurement Policy for NATO Common Funding. The RFP (Request for Proposal) contains two (2) lots, one lot per type of cloud architecture:

- Lot 1: a Distributed Off-premises Physical Air-Gap Cloud (fully isolated infrastructure, maximum assurance)
- Lot 2: a Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing)

d. HQ SACT intends to award Firm Fixed Price Deliverables contract(s) in accordance with the HQ SACT General Terms and Conditions.

e. HQ SACT General Terms and Conditions Dated 15 January 2026 are applicable to this procurement and can be located on the ACT Website at https://www.act.nato.int/wp-content/uploads/2026/01/HQ-SACT-General-Terms-and-Conditions-20260115.pdf under Contractor Information.

f. Contract Award is contingent upon funding availability; Partial bidding is allowed. (E.g. Bidders may bid on and be awarded Lot 1 and/or Lot 2)

2. Classification

This Request for Proposal (RFP) is a NATO UNCLASSIFIED document.

3. Definitions

a. The "Prospective Bidder" shall refer to the entity that has indicated its intention without commitment, to participate in this RFP.

b. The term "Bidder" shall refer to the bidding entity that has completed a bid in response to this RFP.

c. The term "Contractor" shall refer to the bidding entity to which the contract(s) is awarded.

d. The term "Contracting Officer" designates the official who executes this RFP on behalf of HQ SACT.

e. "Contracting Officer`s Technical Representative" or "COTR" is the official who is appointed for the purpose of determining compliance of the successful bid(s), per the technical specifications.

f. The term "HQ SACT" shall refer to Headquarters Supreme Allied Commander Transformation.

g. The term “ACT” shall refer to Allied Command Transformation.

h. The term “NATO” shall refer to the North Atlantic Treaty Organization.

i. The term “days” as used in this RFP shall, unless otherwise stated, be interpreted as meaning calendar days.

j. The term “month” as used in this RFP shall, unless otherwise stated, be interpreted as 30 calendar days.

k. The term “shall” as used in this RFP means an obligation, not a merely directory instruction.

l. The term “Lot” shall refer to subdivisions of the Statement of Work that HQ SACT intends to award separately under the present RFP.

4. Eligibility

a. This RFP is open to governmental or commercial entities;

b. Bidders shall be established in a North Atlantic Treaty Organization Alliance member nation;

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. Proposals will be deemed non-compliant if the DOE for any participating partner has not been received by the bidding deadline. Bidders are encouraged to apply for this declaration immediately if not already previously submitted;

d. All Bidders’ personnel working on this RFP must be citizens of a NATO member nation;

e. Bidders shall be working in the required field (Service Cloud Service) and legally authorised to operate in the country and countries in which this contract is to be performed, at the time of contract. Bidders shall demonstrate the financial, technical, and professional capacity to deliver a secure cloud service at NATO Secret level, including demonstrable experience with Zero Trust architectures, Confidential Computing, Cross-Domain Solutions, and operation of dedicated private cloud connectivity;

f. 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.

5. Duration of Contract

a. The awarded contract(s) shall be effective upon signature (estimated 4 September 2026).

b. Estimated Period of Performance per Lot:

Base period: 12 months after contract signature

Option Period 1: additional 12 months

Option Period 2: additional 12 months

Option periods may be exercised solely at the discretion of HQ SACT based on satisfactory contractor performance, availability of funding, budgetary & operational requirements and Contracting Officer approval.

6. Exemption of Taxes

In accordance with Article VIII of the Paris Protocol, dated 28 August 1952, goods and services under this contract are exempt from taxes, duties, and similar charges.

7. Amendment or Cancellation

a. HQ SACT reserves the right to amend or delete any one or more of the terms, conditions or provisions of the RFP prior to the date set for bid closing. A solicitation amendment or amendments shall announce such action.

b. HQ SACT reserves the right to cancel, withdraw, or suspend at any time, this RFP either partially or in its entirety. No legal liability on the part of HQ SACT shall be considered for recovery of costs in connection to bid preparation. All efforts undertaken by any bidder shall be done considering and accepting, that no costs shall be recovered from HQ SACT.

8. Bidder Clarifications

a. Prospective Bidders should seek clarification at their earliest convenience. Any explanation regarding the meaning or interpretation of this RFP, terms, clause, provision or specifications, shall be requested in writing, to the contracting e-mail address hqsact.contracting@nato.int. Any clarification must be received via email **no later than 1 July 2026.**

b. In lieu of a bidder's conference, HQ SACT invites bidders to submit technical and contractual questions **no later than 1 July 2026**.

c. Information in response to all inquiries / requests for clarification to a prospective bidder shall be furnished to all prospective bidders at the following link: http://www.act.nato.int/contracting as a Question-and-Answer addendum. All such addendums and any necessary solicitation amendments shall be incorporated into this RFP. Verbal Interpretations shall not be binding.

9. Bid Closing Date

Bids shall be received at HQ SACT, Purchasing and Contracting Office, no later than **27 July 2026, 0900 hours, Eastern Time, Norfolk, Virginia, USA.** No bids shall be accepted after this date and time. **No hard copy proposals will be accepted.** Please see Proposal Submission (paragraph 12) for more details.

10. Bid Validity

a. Bids shall remain valid for a period of one hundred and twenty days (120) from the applicable closing date set forth within this RFP. HQ SACT reserves the right to request an extension of validity. Bidder shall be entitled to either grant or deny this extension of validity. HQ SACT shall automatically consider a denial to extend the validity as a

withdrawal of the bid.

b. HQ SACT will not accept supplier proposals prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-Trained Transformer (Chat GPT), or other language generating tools. HQ SACT reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at HQ SACT's sole discretion, and HQ SACT reserves the right to take further steps in such cases as appropriate.

11. Content of Proposal

The proposal shall consist of two (2) separate documents (Technical / Price) sent via e-mail as per the instructions. No hard copy proposals will be accepted. The E-mailed documents shall be received no later than **27 July 2026, 0900 hours, Eastern Time, Norfolk, Virginia, USA.**

a. Technical Proposal shall be a Signed PDF document and contain:

1) Company description;
2) A table of contents for the entire proposal (as per Enclosure #1);
3) The bidder's full name, address, Points of Contact, Telephone, e-mail address, Internet site;
4) Compliance statement (as per Enclosure#2);
5) Past performance (as per Enclosure #3);
6) If not already submitted, Signed Declaration of Eligibility (as per Enclosure #5)
7) List of key personnel to provide services;
8) Supplementary relevant information, if applicable; and
9) Compliance and Best Value Criteria Matrices (as per Annex B).

b. Price Proposal shall be

1) Submitted in U.S. Dollar Currency. Contractor may request payment post award in alternate currency based on agreed conversion rate.
2) Prices shall be on a Firm Fixed Price Basis, include any relevant discount schedule.
3) Price proposal (as per Enclosure #4).

12. Proposal Submission

a. Proposals shall be separate e-mail submissions to:

Technical proposal: **hqsact.techproposal@nato.int**
Price proposal: **hqsact.priceproposal@nato.int**

b. E-mail subjects shall include the solicitation information along with company name (for example: RFP -ACT-SACT-26-54_Tech_ABC Inc. / RFP -ACT- SACT-26-54_Price_ABC Inc.). Allow sufficient time in sending your submission in case you encounter e-mail size challenges.

c. No verbal bids or verbal modifications or telephonic bids shall be considered.

d. It is the ultimate responsibility of a prospective bidder prior to submission that the proposal is reviewed to ensure it meets the technical, contractual and administrative specifications, as well as the limitations and expressed conditions.

e. For the purpose of this RFP and in respect of HQ SACT's Prime Contractor Principle, the Prime Contractor is solely liable for the overall performance and management of the Contract, including delivering the agreed upon outcomes, managing the project's scope, budget, and schedule, and ensuring compliance with all contractual outcomes.

f. The Prime Contractor may, subject to the contracting officer's approval, subcontract certain tasks to other companies but retains the full liability for the requirements' success and for managing any issues.

g. Bidders are at liberty to constitute themselves into any form of contractual arrangements or legal entity they desire, bearing in mind that for purposes of this RFP a consortium is a joint venture or collaboration between two or more companies, having joint and several liability. When bids are submitted on behalf of a consortium, a designated company of the consortium shall represent the consortium with HQ SACT pursuant to a consortium agreement signed by all members. The lead of the consortium shall be vested with full power and authority to act on behalf of all members of the consortium within the powers prescribed either in the consortium agreement or by separate irrevocable Power of Attorney signed by all consortium members.

h. Evidence of authority on behalf of the consortium by the Contractor shall be enclosed and sent with any Bidder's response to this RFP. Failure to furnish proof of authority may be a reason for the RFP response be declared non-compliant.

13. Late Proposals

a. It is solely the bidder`s responsibility that every effort is made to ensure that the proposal reaches HQ SACT prior to the established closing date and time. No late bids shall be considered.

b. A delay in an e-mail exchange due to server or size restrictions does not constitute a delay by NATO.

14. Bid Withdrawal

A bidder may withdraw their bid up to the date and time specified for bid closing. Such a withdrawal must be completed in writing and emailed to the attention of the HQ SACT Contracting Officer.

15. Bid Evaluation

a. The evaluation of bids and determination as to the responsiveness and technical adequacy or technical compliance, of the products or services requested, shall be the responsibility of HQ SACT. Such determinations shall be consistent with the evaluation criteria specified in the RFP. HQ SACT is not responsible for any content that is not clearly identified in any proposal package.

b. Bidders must prepare and submit their proposals independently and not engage in any collusive, anti-competitive, or other improper conduct with any bidder or prospective bidder in relation to this RFP. Any indication of collusion, price-fixing, market allocation, or other conduct intended to distort competition may result in the exclusion of the bidder and may affect the bidder's eligibility in future procurements.

c. Proposals shall be evaluated and awarded taking into consideration the following factors:

1) Successful administrative submission of bid packages as requested in paragraph 11 and as listed in this RFP.
2) Successful determination of compliance on mandatory criteria (Compliant/non-compliant).
3) Technical factors / pricing factors rated as follows: Technical / Price = 70/30 (Best Value for Money)
4) Technical clarifications as determined may be conducted.
5) Acceptance of HQ SACT General Terms and Conditions.

16. Proposal Clarifications

During the entire evaluation process HQ SACT reserves the right to discuss any bid, clarify what is offered and interpret language within the bid to resolve any potential areas of concern.

17. Award

a. HQ SACT intends to award firm fixed price service contract per Lot (or one contract for both Lots) to the successful bidder(s) whose proposal represents the Best Value offer to NATO.

b. HQ SACT will collect information from references provided by Bidders on their past performances. Contractors must provide authorization to contact references or that past performance shall not be considered.

c. HQ SACT reserves the right to negotiate minor deviations to the listed General Terms

and Conditions to this RFP.

18. Surge Capability:

A surge capability requirement is included to have a contract vehicle in place should emerging circumstances require a quick and temporary increase in contractor services within the scope of the existing Statement of Work. The Contractor shall be prepared to provide additional services if needed to support this Statement of Work (SOW). The Contractor shall be prepared to evaluate requirements and submit a price proposal for any new in scope requirement for consideration by HQ SACT. Surge proposals will be evaluated by the Contracting Officer for fair and reasonable pricing and shall be developed based upon the same pricing structure as the original contract proposal. Surge requirements include, but are not limited to additional deliverables, not already accounted for and will be incorporated by formal contract modification. Requests for pricing are made on a non-committal basis and do not constitute a formal commitment by HQ SACT to contract for additional work; supplier will not be reimbursed costs for preparing price proposals or other related expenses in response to a surge request. HQ SACT surge efforts will not exceed 50% of the annual contract value or 50% of the cumulative contract value.

19. Disputes

Interested Parties should consult Appendix 1 of Procedure for NATO Competitive Procurement Policy to learn more about to applicable dispute resolution procedures: **https://www.nato.int/content/dam/nato/webready/documents/finance/procurement-procedure_en.pdf**

For this RFP, complaints shall be lodged by an interested party within 15 calendar days from the date when the interested party first knew, or ought to have known, about the circumstances giving rise to the grounds for the potential dispute, whichever is earlier. For complaints relating to the contract award decision, the deadline is 15 calendar days from the day following the date on which the contract award decision is communicated to the bidders.

20. Proposed personnel

If successful, contractor company must notify HQ SACT of any special accommodations or requirements of its personnel for on-site support.

21. Communications

All communication related to this RFP, between a prospective bidder and HQ SACT shall only be made through the nominated HQ SACT Contracting Officer. Designated contracting staff shall assist the HQ SACT Contracting Officer in the administrative process. There shall be no contact with other HQ SACT personnel regarding this RFP. Such adherence shall ensure Fair and Open Competition with equal consideration and competitive footing to all interested parties.

22. Points of Contact

Hqsact.contracting@nato.int

Enclosure 1: Proposal Content

PROPOSAL CONTENT / CHECKLIST

Table of Contents

- ☐ Bidder's name, address, POC, Contact numbers, email address.
- ☐ Compliance Statement (as per Enclosure 2).
- ☐ Past Performance (including References) (as per Enclosure 3).
- ☐ List of Key Personnel.
- ☐ Technical Proposal, including the Compliance matrix (as per Annex B).
- ☐ Price Proposal (Excel worksheet – as per Enclosure 4 - provides mandatory price proposal format).
- ☐ Declaration of eligibility (as per Enclosure 5).

Enclosure 2: Compliance Statement

COMPLIANCE STATEMENT TO SEALED BID RFP-ACT-SACT-26-54

It is hereby stated that our company has read and understands all documentation issued as part of this RFP. Our company proposal submitted in response to the referenced solicitation is fully compliant with the provisions of this RFP and the intended contract with the following exception(s); such exceptions are considered non-substantial to the HQ SACT solicitation provisions issued.

Note: Any requested deviations/adjustments or considerations regarding HQ SACT General Terms and Conditions **must be identified here - at the time of bidding - for consideration by the Contracting Officer.**

Clause	Description of Minor Deviation

(If applicable, add another page)

Company: _____

Signature: _____

Name &Title: _____ Date: _____

Company Bid Reference: _____

Bidder's proposal must be based on full compliance with the terms, conditions and requirements of the RFP and all future clarifications and/or amendments. The bidder may offer variations in specific implementation and operational details provided that the functional and performance requirements are fully satisfied. In case of conflict between the compliance statement and the detailed evidence or explanation furnished, the detailed evidence/comments shall take precedence/priority for the actual determination of compliance. Minor or non-substantial deviations may be accepted. Substantial changes shall be considered non-responsive.

Enclosure 3: Past Performance Information Form

Company is required to submit a minimum of two (2) past performances within the last five (5) years. Company must clearly state how the company met the requirements of past performance. Reference to a contract must include a detailed description of the work performed relevant to the requirements outlined in the SOW. Generic or Vague references to the contract awarded without clear connection to work performed will be disqualified

(a) Contracting Entity:

(b) Contract No:

(c) Type of Contract (Firm Fixed Price, IDIQ, Requirements):

(d) Title of Contract:

(e) Description of Work Performance and Relevance to Current Acquisition (Type of facility, capacity, estimated patronage, summary of staff used):

(f) Contract Dollar Amount:

(g) Period of Performance:

(h) Name, Address, Fax and Telephone No. of Reference:

(i) Indicate Whether Reference Acted as Prime or Sub-contractor:

(j) Comments regarding compliance with contract terms and conditions:

(k) Complete Contact Information for client:

(l) Permission to contact client for reference: Yes / No

Name of Authorized Company Official: _____

Signature of Authorized Company Official: _____

This Enclosure is designed to assist the respective company provide HQ SACT with all necessary documents/information required. For clarification, please refer to bidding instructions in part 1 of subject solicitation.

Enclosure 4 – Mandatory Price Proposal Excel Spreadsheet

Pricing shall be submitted as signed PDF and Excel; Workbook, using the excel workbook provided.

Proposals not submitted in the proper format will not be considered.

Formulas have been added for convenience; however, it is the company's responsibility to ensure that the formulas are correctly reflecting your expected bid proposal value.

Enclosure 5 – Declaration of Eligibility for NATO Competitive Procurement

Date:

Declaration of Eligibility for NATO Competitive Procurement

To: HQ SACT

Subject: Declaration of Eligibility for NATO Competitive Procurement

Reference: IFIB-ACT-SACT-26-54 Service Cloud Service (SCS)

1. With reference to the above-mentioned NATO Competitive Procurement (NCP) opportunity, the following *[insert Country of Origin]* bidder has expressed an interest in receiving the solicitation document:

a. Bidder Name: _____

b. Address: _____

c. Point of Contact/Title: Mr./Ms.: _____

d. Email Address: _____

e. Phone #: _____

2. I certify that this bidder has the necessary financial, technical and professional competence to be admitted by the Government of *[insert Country of Origin]* as a bidder were it responsible for awarding a contract of this nature. The bidder listed above is security cleared to the level of this procurement opportunity.

3. Extension to Other NCP Opportunities[1]. In addition to the referenced project, this Declaration of Eligibility may be used for other ACT NCP opportunities and is valid for the bidder in paragraph 1 for a period of three (3) years, unless rescinded in writing by the National Responsible Authority of *[insert Country of Origin].*

Check one box:

Yes ☐

No ☐

[1] Note to bidder: If "Yes" is checked, then present this Declaration of Eligibility for expressed interest in other ACT NCP Opportunities

Signature	
Name of National Responsible Authority	
Insert Country of Origin	

Statement of Work

1. Introduction

NATO is advancing toward data-centric operations, AI-enabled decision superiority, and multi-domain operational integration. The delivery of a secure, off-premises cloud infrastructure capable of handling information up to and including NATO Secret is a critical enabler of this transition and of the NATO Digital Transformation programme.

To de-risk and accelerate cloud deployment, Headquarters Supreme Allied Commander Transformation (HQ SACT) intends to contract for a Secure Cloud Service (SCS). SCS will:

- serve as a pre-accreditation validation environment,
- enable iterative security testing and architecture refinement,
- enable the generation of auditable evidence aligned with NATO Security Policy and NIST SP 800-53 Rev.5,
- provide an application migration sandbox and cloud readiness validation
- deliver a first level of operational cloud capability to priority Communities of Interest (COIs).

The deliverables for this solicitation are divided into two separate contract lots, each a prototype designed to evaluate and demonstrate a distinct technology approach to secure cloud for NATO. Lot 1 consists in the delivery of a Physical Air-Gap Off-premises Distributed Cloud (fully isolated infrastructure, maximum assurance). Lot 2 consists in the delivery of a Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing).

A secure off-premises cloud infrastructure capability accredited up to and including NATO Secret is a decisive enabler of NATO's transition to data-centric operations, AI-driven decision superiority, and integrated multi-domain operations.

2. Background and Scope of Work

The primary objectives of the SCS prototypes are to demonstrate and validate a federated, off-premise, distributed, zero-trust-aligned cloud architecture with datacenters distributed on at least four different sites in three different NATO countries.

The prototypes will deliver contractor-operated cloud services under NATO governance, security, and data sovereignty controls, supporting approximately 100 concurrent users, scalable to 150 during testing, across a four Community of Interest workflows - Secure Digital Workspace, Secure Generative AI, Allied Federated Surveillance and Control (AFSC), and Centre for Maritime Research and Experimentation (CMRE).

With datacentres deployed across government or commercially hosted sites, the prototypes will validate two complementary architectural configurations while assessing security, resilience, operational processes, interoperability, and accreditation readiness.

The focus of this effort is to support the modernization of NATO's security accreditation and application migration processes, enabling the adoption of emerging technologies while reducing technical and programmatic risk through representative capability validation.

This Statement of Work (SOW) defines the development of a high-security, cloud prototype capable of handling NATO Secret-level information.

Formal accreditation (e.g., IL6 or equivalent) will be evaluated and achieved if possible.

a. **The statement of work contains two lots, one lot per type of cloud architecture:**
   - Lot # 1: a Physical Air-Gap Off-premises Distributed Cloud (isolated infrastructure, maximum assurance)
   - Lot # 2: a Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing)

b. **The prototypes will:**
   - Establish a validated path to accreditation for off-premises distributed NATO Secret cloud services
   - Establish a sandbox to evaluate application migration and cloud readiness
   - Identify capability gaps across cloud services providers
   - Each lot will develop and demonstrate a distinct cloud architecture: a distributed physically off-prem air-gapped cloud, and a logically isolated hybrid secure cloud leveraging Confidential Computing

c. **The primary objectives for LOT 1 (Distributed Off-premises Physical Air-Gap Cloud (isolated infrastructure, maximum assurance)) are:**
   - Demonstrate, and validate a federated, distributed, zero-trust-aligned cloud architecture grounded in NIST SP 800-207 and NATO Security Policy and hosted on datacentres distributed across at least four different sites in three different NATO countries.
   - Establish a direct, dedicated secure connection between the User Headquarters (two locations) and the contractor datacentres, with target throughput of up to 10 Gbps (or equivalent performance supporting AI and multi-domain workloads) and network-layer encryption
   - Establish a greenfield environment to onboard up to four COI application workflows into the cloud and validate operational performance within each lot.

- Establish an application migration sandbox for Cloud Readiness Validation through the first base period year to allow additional Communities of Interest to de-risk their transition to the cloud.
- Validate security controls, operational processes, and multinational interoperability to reduce technical and accreditation risk
- Generate accreditation artefacts and audit-ready evidence to including System Security Plan, Zero Trust Maturity Report, Vulnerability Assessment Report, and Data Flow Diagrams to enable informed accreditation and implementation decisions. Accreditation artefact list provided in Appendices.
- Test Confidentiality, Integrity, and Availability (CIA) cyber security measures within a well-architected cloud environment.
- Enable secure integration between infrastructure and commercial cloud edge, including cross-domain solutions endpoints and Cross Transfer Services (CTS).
- Leverage Cross Domain Solution (CDS) to enable controlled, automated data transfer and secure delivery of updates and patches into air-gapped environments.

d. **The primary objectives for LOT 2 (Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing) are:**

- Demonstrate, and validate a cryptographically isolated commercial cloud leveraging Confidential Computing, grounded in NIST SP 800-207 and NATO Security Policy.
- Establish a direct, dedicated secure connection between the User Headquarters (two locations) and the contractor datacentres, with target throughput of up to 10 Gbps (or equivalent performance supporting AI and multi-domain workloads) and network-layer encryption
- Establish a greenfield environment to onboard up to four COI application workflows into the cloud and validate operational performance within each lot.
- Establish an Application Migration Sandbox for Cloud Readiness Validation through the first base period to allow additional Communities of Interest to de-risk their transition to the cloud.
- Validate security controls, operational processes, and multinational interoperability to reduce technical and accreditation risk
- Generate accreditation artefacts and audit-ready evidence, including System Security Plan, Zero Trust Maturity Report, Vulnerability Assessment Report, and Data Flow Diagrams to enable informed

accreditation and implementation decisions.

- Test CIA cyber security measures within a well-architected cloud environment.
- Enable secure integration between infrastructure and commercial cloud edge, including cross-domain solutions endpoints and CTS.
- Leverage CDS to enable controlled, automated data transfer and security delivery of updates and secure delivery of updates and patches into air-gapped environments.
- Encryption and decryption are handled through a multi-layered approach that separates the management of cryptographic keys from the environment where the data is processed. This ensures that even if the commercial cloud provider's infrastructure is compromised, the data remains protected.

3. Focus of performance and associated Lines of effort

The scope for both lots is focused on validating representative capabilities required for future operational scale, rather than delivering full enterprise deployment. It is a turnkey service, the contractor will deliver all the attributes necessary to operate the environment and deliver the requested services.

The technical expertise and services required to be performed by the Contractor consist of the following lines of effort:

- Security Architecture and Zero Trust Implementation.
- Data-Centric Security and Cryptographic Key Management.
- Direct, Secure Connection from Headquarters Infrastructure.
- Development of Two Cloud Architecture Configurations.
- Deployment of up to Four Priority Communities of Interest (COIs).
- Deliver an Application Migration Sandbox and Cloud Readiness Validation
- Security Audit, Documentation, and Accreditation Support.
- Continuous Monitoring, Operations, and Sustainment.

4. Period of Performance

The base contract, for both lots, covers a one year service period. The Bidder shall propose pricing for the following options:

- **Duration extension:** two options to extend the service by one year each
- **Additional COIs:** option to add further mission-specific environments beyond the initial four
- **Additional connection to user locations:** option to extend the secure

connection to additional locations

- **User growth:** options to expand in tranches of 100 or 500 additional users

5. Tasking and Deliverables

This section is comprised of the following subsections:

A. Security Accreditation and Validation Requirements

B. Application Migration and Cloud Readiness Verification

C. Secure (Direct) Connection Requirements

D. Mission-Specific Services (Communities of Interest)

E. Security Audit and Required Documentation

F. Network Termination Equipment

G. Cloud Architecture Configurations

A. Security Accreditation and Validation Requirements

A primary objective of this SOW is to support and inform NATO ’s security accreditation process for secure cloud capabilities up to and including NATO SECRET. The SCS prototype shall serve as an operational test environment to validate security controls, operational procedures, and compliance with applicable NATO security policies and standards.

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.

The contractor shall also consider emerging NATO security guidance and draft policy updates where these improve security, resilience, and operational speed, particularly in crisis or mission-driven environments.

Deliverables shall include auditable documentation, security test results, risk assessments, and lessons learned to support future accreditation decisions.

Successful execution of accreditation testing and evidence generation shall be considered the primary measure of success for the SCS prototype.

Further technical requirements are provided in the applicable Annexes.

A.1. Access Control and Identity Verification

All users must be authenticated and verified prior to accessing any resource. The solution shall:

- Enforce multi-factor authentication (MFA)

- Support onboarding and verification of approximately 100 total pilot users across both lots (i.e., 50 per lot).
- Ensure workload isolation, preventing lateral movement between applications

A.2. Data Centric Security

Data must remain protected at all times at rest, in transit, and in use. The solutions shall:

- Prevent unauthorized access through strong encryption and access controls
- Ensure all data is clearly classified and labelled
- Maintain NATO ownership and control over all data
- Continuously monitoring data usage to detect and respond to anomalies

A.3. Network Isolation

The prototype environment in Lot 1/Lot 2 shall be isolated from the public internet to prevent unauthorized access, using physical or logically equivalent controls.

The architecture must also ensure high availability and resilience, including distribution across multiple locations to maintain operations during failure scenarios.

A.4. Security Policy Management

The contractor shall demonstrate centralized and consistent enforcement of security policies, including:

- Definition of access rights and conditions
- Management of user access and dynamic access control
- Continuous monitoring and enforcement across all systems

A.5. Audit and Compliance

All services must align with NATO Secret security requirements. The solution shall:

- Enable secure, controlled transfer of updates, patches, and service into the environment.
- Provide audit-ready evidence of compliance and security controls

A.6.Development Environment

Enable a controlled development and testing environment supporting application onboarding and deployment within the Application Migration Sandbox and Cloud Readiness Validation. Full cross-domain CI/CD pipelines are not required.

B. Application Migration and Cloud Readiness Verification

A second primary objective of this SoW is to provide an Application Migration Sandbox and Cloud Readiness Validation: the Contractor shall provide and operate a secure Application Migration Sandbox and Cloud Readiness Validation environment to enable Communities of Interest (COIs) to prepare their applications for transition to the future Programme of Record (PoR).

The purpose of this sandbox is to allow COIs to assess, adapt, and validate their applications within a secure cloud environment ahead of NATO enterprise-level cloud adoption. By the completion of the prototype, applications onboarded into the sandbox shall achieve a level of cloud readiness such that transition to the enterprise cloud environment can be achieved with minimal modification, ideally through a rehosting approach.

The Contractor shall provide sandbox environments that are logically isolated per COI, accessible via the Direct Secure Connection, and compliant with Zero Trust and data-centric security principles. The environment shall support deployment of applications using virtual machines and, where applicable, container-based approaches, including the provisioning of required supporting services such as storage, databases, and middleware components.

The Contractor shall provide controlled and auditable mechanisms to ingest application artefacts and data into the sandbox environment, including secure data transfer procedures, integrity verification, and enforcement of classification and encryption requirements. All migration activities shall comply with NATO Secret security requirements and shall ensure full protection of data at rest, in transit, and in use.

Deployment of application components into the sandbox shall be supported through repeatable and controlled mechanisms. Full-scale cross-domain DevSecOps pipelines are not required; however, the Contractor shall enable reproducible deployment and configuration of application environments to support iterative testing.

Migration testing shall support two representative approaches:

- - Rehosting (lift-and-shift), validating that applications can operate in the cloud environment with minimal change;
- - Limited refactoring to resolve compatibility constraints and enable operation in a cloud-hosted environment.

The Contractor shall ensure that all applications remain isolated from one another and from other COIs, preventing any cross-application or cross-domain access in accordance with Zero Trust principles.

Application Migration Sandbox and Cloud Readiness Validation activities shall be conducted collaboratively: the Contractor will provide infrastructure, platform services, and technical support; and COIs will be responsible for application configuration, adaptation, and validation of functionality.

The Contractor shall support validation demonstrating that applications:

- can be deployed and executed within the secure cloud environment;
- maintain functional behaviour consistent with their intended use;
- do not rely on unavailable on-premises dependencies;
- comply with security, isolation, and access control requirements.

Migration activities shall contribute to the overall security accreditation effort by generating evidence on application behaviour, data handling, and enforcement of security controls within the cloud environment.

The Contractor shall deliver documentation including a Migration and Cloud Readiness Assessment Report, identifying applications onboarded, migration approaches applied, constraints encountered, and assessed readiness level, including whether applications are suitable for rehosting in the future enterprise cloud environment.

This activity is limited to validation and preparation and does not constitute full operational migration or production deployment.

C. Secure (Direct) Connection Requirements

Dedicated, private network links must be established between the User Headquarters and the Contractor's data centre. The connectivity effort includes redesigning the on-premises network at the pilot facilities to securely enable access to the commercial cloud, including preparation of the local area network. Additionally, the effort requires the installation of cross-domain hardware, such as data diodes and guards, to provide the physical security layer, supported by a software layer that manages, inspects, and controls cross-domain data transfers.

C.1. Connection Specifications

- **Technology:** Private Network Interconnects (PNIs) or specialized Dedicated Leased Lines. Dedicated, private network connection from NATO's on-premises site or co-location facility directly to the cloud provider's network infrastructure.
- **Bandwidth:** 10 Gbps dedicated throughput to support high-demand operations including AI and multi-domain applications

- **Encryption:** all traffic on the direct link must be encrypted at the network layer

C.2. End-User Devices

To support the 100 pilot users, the contractor must procure and configure end-user devices including laptops, smart cards, and updated access credentials. Contractor shall procure and deliver 100 total end-user devices across both lots (i.e., 50 per lot), half quantities in USA and half quantities in Europe.

Device management must be centralized and cloud-based, enforcing security settings such as encrypted storage and software compliance.

D. Mission-Specific Services (Communities of Interest)

The contractor shall deliver up to four mission specific cloud environments, each supporting a distinct operational use case, referred to as Communities of Interest (COIs). Technical information for each COI is listed in the appendices. **All COIs will be used in test environment as use cases. Contractor will deliver solutions for the Secure Digital Workspace and the Secure Generative AI but no expectation of Contractor to mature or deliver product for the other two (AFSC and Maritime operations).**

The below Section D.1 relates to the Secure Digital Workspace COI; Section D.2 to the Secure Generative AI (GenAI) COI; Section D.3 to the AFSC Digital Engineering (DE) / Mission Engineering (ME) COI; and Section D.4 to the D.4. Maritime Operations (CMRE/TFX Arctic).

D.1. Secure Digital Workspace

The Contractor will deliver an operational turnkey solution for this COI (the Contractor will deliver all the attributes necessary to immediately operate the environment and deliver the requested services).

A secure digital workspace supporting approximately 100 total users across both lots (i.e., 50 per lot), enabling classified collaboration and operational coordination. The environment shall provide:

- Collaborative document editing and shared workspaces
- Encrypted email, including migration of a subset of existing mailboxes
- Secure instant messaging and group communication channels

- High-definition voice and video conferencing optimised for secure connectivity

All data processing shall occur within the secure cloud environment; no local data storage is permitted on user devices. Data shall be automatically classified, labelled, and protected throughout its lifecycle. Users' action (e.g., copy, download, print) shall be restricted based on authorisation level.

D.2. Secure Generative AI (GenAI) COI

The contractor will deliver an operational turnkey solution for this COI.

This prototype adds secure, local Generative AI to the air-gapped NATO cloud. It allows personnel to use AI-driven analysis on classified data without ever connecting to the outside internet or external AI providers.

D.2.1. Core Functions

- Localized AI Hosting: All models live entirely on the NATO SCS prototype infrastructure/hardware. NATO is provided with an extension of a commercial air-gapped multimodal generative AI model. Alternatively, NATO is provided with the tools and environment to train its own generative AI model.
- Secure Classified Analysis: The AI only uses approved, internal data to generate answers. It is hardened against "prompt injection" or malicious attempts to trick the system into leaking secrets.
- Traceable Outputs: Every response provided by the AI includes clear references to the original source data, ensuring users can verify the information rather than trusting it blindly.

D.2.2. Security & Accountability

- Automatic Classification: The system automatically labels its own AI-generated content with the correct security level so users know exactly how to handle the information.
- Role-Based Access: Usage is strictly tied to a user's specific clearance and mission, you only see what you are authorized to see.
- Continuous Monitoring: Every interaction is logged and monitored for abnormal behaviour to prevent data leakage and maintain a complete audit trail.

This capability provides NATO with high-speed, AI-assisted decision-making while keeping sensitive data locked inside a fully controlled and auditable "digital fortress."

*See Appendix B for additional information

D.3. AFSC Digital Engineering (DE) / Mission Engineering (ME) COI

This COI requires a green-field, secure, air-gapped digital engineering environment to enable distributed AFSC stakeholders across ACT and NSPA AFSC System Integration Office (SIO) to collaboratively develop and govern executable architecture artefacts (e.g., SoSA-EU and SoS-TA linkages), conduct repeatable mission-thread analyses, and generate auditable evidence packages to support trade-space assessments and Analysis of Alternatives (AoA) decision-making.

The AFSC DE/ME COI establishes an environment that aligns programme efforts around interoperable and reusable capabilities, delivering the interfaces, services, and security required to sustain collaboration across the NS environment. It introduces a pilot Digital Engineering Environment and Integrated Development Environment (IDE), enabling distributed teams to collaborate at the NS level in support of AFSC, other ACT programmes, and broader NATO Enterprise initiatives.

D.3.1. Core Functions

- **Authoritative Architecture Repository Service:**

  A multi-user authoritative model repository supporting controlled collaboration, role-based access control, audit logging, backup and restore, and configuration-management concepts such as baselines, branches, tags, and approved releases for architecture artifacts.

- **Source Control and Configuration Management Service:**

  A Git-based service, or equivalent, for scripts, plugins, profiles, templates, configuration files, and integration code used to customize tools, automate workflows, and manage digital engineering environment configurations, including branching, merging, tagging, and traceability to approved architecture baselines.

- **Scripting and Tool Integration Environment:**

  An execution environment for supported scripting and automation languages, APIs, and SDKs required for architecture tool customization, model query and extraction, validation, data exchange, and workflow automation, including languages such as Java, JavaScript, Groovy, and Python, together with associated dependency/package management and developer tooling or IDE support as required.

- **Shared Artifact Storage:**

  Secure storage for model exports, generated documents, interchange files, scripts, configuration packages, and related collaboration artifacts, including retention, backup, restore, and access-control procedures.

D.3.2. Security & Accountability

- **Isolation:** Environment is isolated from other environments on the network so that members of other COIs cannot access AFSC DE/ME repositories.

- **Identity and Access Management**: Centralized authentication and authorization services supporting distributed team collaboration across repository, source control, and artifact services, including role-based access control, account management, and auditability.

- **Full Traceability:** Every action, model change, and automated process is logged for high-level auditing and trust.

  *See Appendix C for additional information.

D.4. Maritime Operations (CMRE/TFX Arctic)

This COI requires a green-field, secure, air-gapped digital engineering environment to enable maritime operations, including undersea and Arctic mission sets. The COI owner intends to migrate application data and workflows to the new environment at a later date, also funded separately.

Upon migration of application, the COI shall:

- Store and process large volumes of acoustic and sonar data
- Identify vessels through acoustic signatures analysis, including non-cooperative targets (no active transponders)
- Support disconnected operations, enable local data caching and synchronizing once connectivity is restored
- Generate alerts when vessels enter protected or sensitive maritime areas

These COI implementations will demonstrate operational relevance and validate that secure cloud services can effectively support mission-critical use cases across multiple domains.

*See Appendix D for additional information.

E. Security Audit and Required Documentation

Successful completion of the prototype is contingent upon passing a NATO security audit. conducted by a designated NATO security team within six months of contract award. Failure of the prototype to pass the security audit does not constitute contract non-performance, if the Contractor complies with the requirements of this Statement of Work.

E.1. Required Documentation:

The contractor shall provide full system access and deliver the following artefacts (See milestones and deliverable list and relevant appendix for full list of artefacts/requirements):

- System Security Plan (SSP): Defines the security boundary, implements controls and compliance with requirements
- Zero Trust Maturity Report: Assesses implementation across the five pillars of zero trust: identity, devices, network, applications, and data
- Vulnerability Assessment Report: results from automated and manual testing conducted within the isolated environment
- Data Flow Diagrams: Illustrate movement of NATO Secret data between HQ and each COI

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

E.3. Security Validation Requirements:

- Within six months of contract award, the contractor shall demonstrate that the solution meets NATO Secret-level security requirements.
- Completion of the audit and delivery of artefacts will establish the accreditation baseline and evidence package, enabling senior leadership to advise on evidence-based policy recommendations.

F. User Location Infrastructure Requirements

The User locations must be prepared to receive and distribute secure cloud services to the 100 total pilot users across both lots (i.e., 50 per lot). SCS is a turnkey service. The contractor is responsible for providing all required on-site equipment.

F.1. Network Termination Equipment

- Secure gateway hardware: industrial-grade routers capable of terminating the encrypted 10 Gbps circuit
- Encryption key management hardware: on-premises hardware security modules to manage the keys used for the air gap and data encryption
- Physical security: all termination equipment must be housed in a secure facility meeting NATO Secret physical protection standards

F.2. End-User Devices

- Thin-client access: users access all COIs through a secure virtual desktop. No classified data is stored on individual devices
- Hardware-based authentication: each of the 100 users across both lots (i.e., 50 per lot) must use a physical security key (FIDO2-compliant) or smart card for every login
- Single access portal: one secure application provides access to all four COIs

G. Cloud Architecture Configurations

Two configurations will be tested:

- **Distributed Off-premises Physical air-gapped**: Air-gapped cloud that is a

fully isolated, self-contained cloud environment and distributed on different sites and different countries

- **Hybrid Secure Cloud**: A cryptographically isolated architecture leveraging a private, dedicated network to bridge on-premises NATO crypto hardware with hardware-enforced, secure execution environments in a commercial cloud

As a turnkey service, both configurations must demonstrate consistent identity management, data security, network connectivity, governance, and workload management.

6. Schedule of Milestones and Acceptance Criteria

Base Period Milestone	Key Deliverables	Acceptance Criteria	Required Evidence
Upon Contract Award (Lot 1 / Lot 2) **T0**	Project Management Plan and Security Architecture	Approved PMP, Security Architecture, Accreditation Strategy, and Risk Register delivered and accepted.	Approved documents and review comments closed.
Secure Connectivity Established (Lot 1 / Lot 2) **T0 + 2 months**	Secure site-to-site connectivity	Encrypted connectivity established; 100 users onboarded;	Network test report, throughput results, user provisioning report.
Initial Cloud Deployment (Lot 1 / Lot 2) **T0 + 2 months**	Air-Gapped and Hybrid Cloud Prototypes	Lot 2 operational. Lot 1 datacenters distributed on 2 different sites. Baseline security controls implemented.	Deployment report and architecture validation.
COI Deployment (Lot 1 / Lot 2) **T0 + 3 months**	Four COIs operational	Secure Digital Workspace, Secure GenAI, AFSC DE/ME, and CMRE/TFX	UAT results, demonstration report,

Base Period Milestone	Key Deliverables	Acceptance Criteria	Required Evidence
		operational; representative workflows executed; 100 concurrent users supported.	performance report.
Four-Site Federation (Lot 1) **T0 + 4 months**	Distributed cloud architecture	Lot 1 datacentres operational across 4 different sites in 3 different NATO nations; workload distribution and synchronization validated.	Federation test report and topology diagrams.
Migration sandbox available (Lot 1 / Lot 2) **T0 + 4 months**	Application migration environment	At least one representative application successfully deployed and validated.	Migration report and application test results.
Security Audit Execution (Lot 1 / Lot 2) **From T0 to T0 + 6 months**	Security assessment	Security testing completed; findings documented and remediation plan delivered.	Audit report and vulnerability assessment.
AfT/IATO Readiness (Lot 1 / Lot 2) **T0 + 5 months**	Accreditation package	SSP, architecture diagrams, risk assessment and evidence package delivered.	Accreditation evidence package.
ATO Readiness (Lot 1 / Lot 2) **T0 + 7 months**	Accreditation package	SSP, architecture diagrams, risk assessment and evidence package delivered.	Accreditation evidence package.
Test phase in progress (Lot 1 / Lot 2)	Test phase interim report: Application migration status,	Performance compliance	Interim Report

Base Period Milestone	Key Deliverables	Acceptance Criteria	Required Evidence
T0 + 9 months	compute, storage and network performance		
Test phase finalized (Lot 1 / Lot 2) **T0 + 12 months**	Test phase final report: Application migration status, compute, storage and network performance	Performance compliance	Final Report

7. Payment Milestones

Base Period Milestone	Key Deliverables	Payment percentage
Secure Connectivity Established (Lot 1 / Lot 2) **T0 + 2 months**	Secure site-to-site connectivity	**20%**
Initial Cloud Deployment (Lot 1 / Lot 2) **T0 + 2 months**	Air-Gapped and Hybrid Cloud Prototypes	
Four-Site Federation (Lot 1) **T0 + 4 months**	Distributed cloud architecture	**20%**
Migration sandbox available (Lot 1 / Lot 2)	Application migration environment	

Base Period Milestone	Key Deliverables	Payment percentage
T0 + 4 months		
ATO Readiness (Lot 1 / Lot 2) **T0 + 7 months**	Accreditation package	**20%**
Test phase in progress (Lot 1 / Lot 2) **T0 + 9 months**	Test phase interim report: Application migration status, compute, storage and network performance	**20%**
Test phase finalized (Lot 1 / Lot 2) **T0 + 12 months**	Test phase final report: Application migration status, compute, storage and network performance	**20%**

8. Optional years

Option Period(s) Milestones	Key Deliverables	Acceptance Criteria	Payment percentage
Operations and Maintenance of Secure Cloud Environment Quarterly, end of each quarter	Ongoing maintenance of environment for continued test and usage by ACT and relevant COIs	Test phase report: Application migration status. Compute, storage and network compliance with the requirements	25% quarterly

9. Contractor Performance Requirements and Reporting

The Contractor(s) shall provide regular reports or updates on progress on the work being done and prior to deliverable being met.

Minimum of bi-weekly (once every two weeks) updates are required by the contractor to inform NATO of progress towards deliverables.

More frequent meetings or touch points are encouraged to ensure NATO is able to respond appropriately to requests for information, guidance or direction on project.

10. Personnel Required for Statement of Work

To be determined by Contractor. Contractor shall supply trained, qualified personnel to complete the work contained within this statement of work.

11. Time Requirements for Contractor Personnel

Firm fixed price contract.

12. Proof of Past Performance

Please see RFP Bidding Instructions.

13. Place of Performance

Work is primarily to be performed at contractor facilities.

14. Required Travel for Personnel Services Contracts

Contractor should anticipate travel for up to one on-site meeting per month of up to two days for requisite personnel over the first base period. Contractor should anticipate travel up to quarterly for on-site meetings of up to two days for additional option periods for requisite personnel. Contractor shall include estimated travel costs in the price proposal.

15. Furnished Materials and Services

a. **NATO Supplied:** None

b. **Contractor Supplied:** As a turnkey service, to support the 100 pilot users, the contractor must procure and configure end-user devices including laptops, smart cards, and updated access credentials. Contractor shall procure 100 total end-user devices across both lots (i.e., 50 per lot).

Device management must be centralised and cloud-based, enforcing security settings such as encrypted storage and software compliance. Devices will run standard NATO virtual machine images with pre-configured security settings. Only NATO-owned device enrolment will be supported in this prototype phase.

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.

17. Security Considerations (in line with NATO Security Policy and NIST SP 800-53 Rev.5)

a. The implementation of a private cloud environment for the storage, processing, and transmission of NATO classified information shall comply with all applicable NATO security policies, regulatory requirements, and industry best practices for information security and data protection. The solution must provide robust safeguards to ensure the confidentiality, integrity, and availability of sensitive data, including but not limited to strong access controls, multi-factor authentication, encryption of data at rest and in transit, continuous monitoring, logging, vulnerability management, and incident response capabilities. The provider shall demonstrate compliance with relevant security frameworks and accreditation requirements and ensure that all data remains within approved jurisdictions and controlled environments. Appropriate segregation of duties, privileged access management, backup and recovery mechanisms, and audit capabilities shall be implemented to minimise operational, insider, and cyber security risks. The contractor must also ensure that personnel with administrative or privileged access are appropriately vetted and that security responsibilities, reporting obligations, and breach notification procedures are clearly defined within the contractual arrangement

b. The contractor shall follow applicable policies for development of this prototype and implement relevant polices as closely as possible. Gaps in relevant security policies and industry standard security practices shall be identified and included in a report as part of the deliverable for the base portion of this contract.

c. The Contractor shall ensure that all cloud services, hosting environments and any other information technology resources used in the performance of this Contract are physically hosted and operated exclusively within the territory of NATO member nations.

The Contractor shall ensure that any subcontractors and third parties engaged in the performance of this Contract comply with this requirement.

18. Applicable security policies include:

- AC/35-d/2004-REV4 PRIMARY DIRECTIVE ON CIS SECURITY
- AC/322-D/0048-REV3 (INV), TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR CIS SECURITY
- ACC/322-D/(2004)0030 INFOSEC TECHNICAL AND IMPLEMENTATION DIRECTIVE ON THE REQUIREMENT FOR, AND THE SELECTION, APPROVAL AND IMPLEMENTATION OF, SECURITY TOOLS (ST)
- ACC/322-D/0030-REV6 (INV) TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR THE INTERCONNECTION OF COMMUNICATION AND INFORMATION SYSTEMS (CIS)
- AC/322-D(2007)0024 INFOSEC TECHNICAL AND IMPLEMENTATION SUPPORTING DOCUMENTATION ON SECURITY ASPECTS OF INTERNET PROTOCOL TELEPHONY
- AC/322-D(2004)0019 INFOSEC TECHNICAL AND IMPLEMENTATION GUIDANCE FOR THE PROTECTION OF CIS FROM MALICIOUS SOFTWARE
- AC/322-D(2004)0021 INFOSEC TECHNICAL AND IMPLEMENTATION GUIDANCE FOR ELECTRONIC LABELLING OF NATO INFORMATION
- AC/35-D/2004-REV4 PRIMARY DIRECTIVE ON CIS SECURITY
- AC/322-D(2019)0038 CIS SECURITY TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR THE SECURITY OF WEB APPLICATIONS
- AC/322-D(2021)0032-REV1 TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR THE PROTECTION OF NATO INFROMATION WITHIN PUBLIC CLOUD-BASED COMMUNICATION AND INFORMATION SYSTEMS
- AC/322-D(2026)0024 NS CLOUD DIRECTIVE
- AC/322-D(2017)0016 TECHNICAL AND IMPLEMENTATION DIRECTIVE ON SUPPLY CHAIN SECURITY FOR COTS CIS SECURITY ENFORCING PRODUCTS
- AC/322-D(2010)0055 INFORMATION ASSURANCE TECHNICAL AND IMPLEMENTATION DIRECTIVE ON SECURITY MANAGEMENT INFRASTRUCTURE (SMI)

- AC/322-D(2006)0041-REV2 DIRECTIVE ON THE SELECTION AND PROCUREMENT OF NATO COMMON-FUNDED CRYPTOGRPHIC SYSTEMS, PRODUCTS AND MECHANISMS
- AC/35-D/1032-REV1 SUPPORTING DOCUMENT ON THE SECURITY OF NATO CLASSIFIED INFORMATION

19. Intellectual Property

HQ SACT Background Intellectual Property (IP). Pre-existing IP will remain the property of the Party owning the IP. HQ SACT hereby grants to Contractor a royalty-free, non-exclusive, non-transferable license to use HQ SACT Background IP as required to allow the Contractor to perform its obligations under the Contract.

Contractor's Background IP. Upon contract award, the Contractor will identify in writing all its Background IPR prior to the start of the Contract. Upon completion of the Contract and on receipt of payment in full by Contractor, the Contractor grants to NATO, a perpetual royalty-free, nonexclusive, non-transferable license to use Contractor's Background IP as required to allow NATO to use the deliverables produced by the Contractor for any objectives and business purpose related to or derived from the Contract.

Foreground IP. Foreground IP means all intellectual property rights in the work , generated during the performance of the Contract. All rights in the results of the work undertaken related to this Contract will vest in and be the sole and exclusive property of NATO, as represented by HQ SACT/ACT, unless the Contractor advises HQ SACT before the conclusion of contracting process on existing third parties or Contractor's rights arising otherwise than by virtue of the Contract, and with due regard to national security regulations, This includes, but is not limited to any developed cloud prototypes, sandbox(es), technical data specifications, reports, the security audit report(s), manuals, drawings, computer software data, computer programmes, computer databases, computer software including any buyer-specific configurations, source code, documentation including software documentation, design data, specifications, instructions, test procedures, training material produced or acquired in the course of such work, inventions, derivative works, and, in particular, all rights, including copyright therein. Accordingly, HQ SACT may modify, protect, publish, incorporate into other documents share with others, or otherwise use without restriction all aspects of the results of the work undertaken as HQ SACT deems fit at its sole discretion. The Contractor will not in any way use, license, or allow third parties to use the results of the work procured or any portion thereof without the express prior written consent of HQ SACT's contracting authority. Any costs related to intellectual property rights outlined above are included into the fees under the Contract. Intellectual Property generated during the performance of the

Contract will be presumed to constitute Foreground IP where such results are reasonably connected to, informed by, or derive from the deliverables or preparation thereof.

TASKING AND DELIVERABLES APPENDICES

A. Appendix A – Security Accreditation and Validation Requirements

The solution shall implement a data-centric security model where protection is applied directly to the data itself, ensuring persistent security regardless of where the data resides or how it is accessed.

1.1. Data Protection and Tagging

- Security must be embedded at the object and field level, including field-level encryption and robust metadata tagging
- All data objects shall be tagged using machine-readable security metadata aligned to NATO data classification schemas
- Metadata tagging must enable automated enforcement of access control policies

1.2. Encryption Standards

- Data at rest and data in transit must be encrypted using NATO Encryption AES-256 or equivalent (for demonstration)
- Data in transit must be encrypted using TLS 1.3 or higher
- Encryption mechanisms must align with Zero Trust (ZT) maturity principles

1.3. Cryptography, Encryption, and Key Management

The solution must support secure and flexible cryptographic key management, ensuring NATO retains sovereignty over its data.

- Support cryptographic key lifecycle management, including key generation, storage, rotation, and revocation
- Key management must be backed by Hardware Security Modules (HSMs)
- The solution must support BYOK (Bring Your Own Key) and HYOK (Hold Your Own Key) models

1.4. The prototype shall test multiple Key Management System (KMS) deployment models, including:

- BYOE (Bring Your Own Encryption):
  - No contractor-hosted KMS
  - NATO retains full control of encryption keys, segregated from cloud infrastructure
  - Test scenarios shall assess data flow latency and operational impact
- Cloud HSM (Cloud-hosted Hardware Security Module):
  - Demonstrates HSM core functions including key generation, storage, rotation, and API-based orchestration
  - Test scenarios shall validate performance and compliance with NATO NS cloud security measures
- Cloud Managed KMS:
  - Native integration with cloud services (compute, storage, databases, development tools)
  - Test scenarios shall validate security compliance and performance improvements (e.g., latency reduction)
- Dedicated NATO-controlled KMS hosted in cloud (NATO Owned–NATO Operated (NO–NO) KMS):
  - NATO-operated KMS hosted within the commercial cloud environment
  - Test scenarios shall validate key sovereignty, lifecycle management, API orchestration, and no violation of NATO NS security requirements

1.5. Cryptographic Validation and Testing:

- Dedicated cryptographic testing shall be conducted to:
  - Validate data confidentiality and sovereignty
  - Identify and mitigate potential data leakage risks
  - Assess compatibility of cryptographic approaches with NATO commercial cloud extensions
  - Evaluate the potential to evolve or replace existing NATO Secret cryptographic implementations, where appropriate

1.6. Continuous Monitoring and Threat Detection

- The system must implement continuous monitoring with real-time behavioural analytics
- Capabilities must include detection of anomalous or unauthorized data access patterns
- Monitoring outputs must support rapid response and incident handling

1.7. Network Isolation (Technical Requirements)

- The environment must implement one of the following:
  - Lot 1: Physical isolation using dedicated infrastructure (Air-gapped). Lot 1 must demonstrate deployment of the following components:

Component	Location	Role	Connectivity
Workload	Service Provider Data Center	Sensitive processing on dedicated physical hardware.	**Air-Gapped**
Compute & Storage	Service Provider	Dedicated "Bare Metal" or Private Cloud stack.	Local internal network only.
NATO Crypto Hardware	Service Provider	Transferred & Deployed: NATO-owned HSMs/appliances.	Physically cabled to the dedicated compute.
Management Console	Service Provider	Local terminal for administration.	**No Remote Access:** Must be managed on-site or via a highly secured, encrypted terminal.

  - Lot 2: Logical isolation using cryptographic segmentation and software-defined controls with no public internet routing (Hybrid Secure Cloud). Lot 2 must demonstrate deployment of the following components:

- Hardware: NATO crypto appliance (with the NATO crypto algorithm) sits in pilot node's (ACT) rack.

- Connection: Connection to the commercial cloud will be done by dedicated network connection of commercially managed private, direct cloud connectivity service (secure connection) to create a private network path to the pilot virtual private cloud in the commercial/public cloud Region(s) (for redundancy 2 regions).
- The Workload: Next-generation virtualization hardware providing secure enclave hardware-isolated, highly-constrained compute environment that provides cryptographic attestation runs on a parent Virtual Machine instance in the commercial/public cloud Region(s).
- Communication: The Enclave sends a request through the “proxy (managed by the commercial cloud)” to the parent Virtual machine instance. The parent instance then sends that request over a secure connection (Dedicated, private network links must be established between the User Headquarters and the Contractor's data centre. This link must bypass the public internet entirely.) link to NATO on-prem crypto hardware.

Lot 2: Summary of Deployment

Component	Location	Role
Secure Enclave	Commercial Cloud Regions	Runs prototypes isolated, sensitive processing.
Hardware Crypto	NATO On-Prem, ACT	Stores master keys and perform physical crypto.
Connectivity	Direct, Secure Connection	Dedicated, private network links must be established between the User Headquarters and the Contractor's data centre. This link must bypass the public internet entirely.

- **In Lot 2 (Hybrid Secure Cloud):** architecture, encryption and decryption must be handled through a multi-layered approach that separates the management of cryptographic keys from the environment where the data is processed. This ensures that even if the commercial cloud provider's infrastructure is compromised, the data remains protected. Lot 2 must demonstrate the following encryption/decryption

capabilities:

- Key Management (The Root of Trust)
- The actual encryption/decryption keys never reside in the public cloud in an unencrypted state.

1.8. Lot 2 Encryption/Decryption: NATO On-Prem, U.S. Facility (Pilot Node)

Lot 2 must demonstrate the following encryption/decryption capabilities:

1.8..1. Key Management (The Root of Trust)

The actual encryption/decryption keys never reside in the public cloud in an unencrypted state.

- Location: NATO On-Prem, HQ SACT (Pilot Node).
- Mechanism: The NATO Crypto Hardware (HSM) generates and stores the Master Keys.
- Decryption Request: When the workload in the cloud needs to decrypt data, it does not "get" the master key. Instead, it sends the encrypted data (or a wrapped key) back to the on-prem hardware via the Direct Connect link. The hardware performs the cryptographic operation and sends the result back.

1.8..2. Data in Transit (The Secure Pipe)

As data moves between NATO pilot site and the Cloud Region, it is protected at the network layer.

- Mechanism: While the Direct Connect provides a private physical path, a VPN tunnel is typically established over that link.
- Result: This ensures that the data is encrypted before it even leaves the NATO perimeter and is only decrypted once it reaches the private interface of the Virtual Private Cloud (VPC) that will be hosted on public cloud.

1.8..3. Data in Use (The Secure Enclave)

To prevent the cloud provider from seeing data while it is being processed in RAM, Confidential Computing is used.

- Mechanism: The Secure Enclave creates a hardware-isolated memory partition.

- The Process:
    1. The encrypted data enters the Enclave.
    2. The Enclave proves its identity to the NATO On-Prem Hardware via Cryptographic Attestation.
    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.
- Mechanism: The NATO Crypto Hardware (HSM) generates and stores the Master Keys.

1.9. Security Policy Management (Technical Requirements)

The framework must ensure consistent, auditable, and centrally managed policy enforcement across the environment and the solution must implement a policy-based access control framework consisting of:

- Policy Decision Point (PDP): evaluates and determines access decisions
- Policy Administration Point (PAP): manages and defines access policies and credentials
- Policy Enforcement Point (PEP): enforces access decisions and monitors compliance

1.10. Application Migration Sandbox and Cloud Readiness Validation (Technical Requirements)

1.10.1 Objective

The purpose of application migration within the SCS prototype is to deliver a secure sandbox environment enabling Communities of Interest (COIs) to prepare their applications for transition to a future Programme of Record (PoR).

This sandbox will allow COIs to:

- Assess and adapt their applications to operate within a secure cloud environment,
- Identify architectural, security, and operational constraints early,
- Progressively achieve cloud readiness.

By the completion of the prototype, applications onboarded into the sandbox shall be:

- Technically validated within a cloud environment, and
- At a maturity level where, at worst, a rehosting (lift-and-shift) approach is sufficient to transition into the future enterprise cloud environment.

This activity is strictly focused on preparation and validation, not full production migration.

1.10.2 Scope of Application Migration Sandbox and Cloud Readiness Validation

The Contractor shall provide a controlled, secure Application Migration Sandbox and Cloud Readiness Validation environment enabling COIs to:

- Deploy and test representative applications,
- Evaluate different migration approaches,
- Validate cloud readiness against defined criteria.

The sandbox shall:

- Be isolated from production environments,
- Support multiple COIs concurrently with strict segregation,
- Allow iterative onboarding and testing throughout the prototype duration.

Migration activities shall remain limited in scale and scope, focusing on representative applications and use cases.

1.10.3 Migration Approaches to be Supported

The sandbox shall enable the following migration approaches:

a. Rehosting (Lift-and-Shift)

- Migration of applications with minimal change,
- Validation that existing applications can run securely in the cloud environment,
- Identification of dependencies and constraints.

b. Refactoring / Cloud Adaptation (Limited Scope)

- Targeted modifications to improve compatibility with cloud hosting (e.g., containerisation, externalisation of configuration),
- Focus on removing blocking issues, not full redesign.

The objective is to ensure applications reach a “cloud-compatible state”, not full cloud-native transformation.

1.10.4 Technical Requirements for the Application Migration Sandbox and Cloud Readiness Validation

To achieve the objective, the contractor shall provide the following technical capabilities:

1.10.4.1 Environment Provisioning

- Dedicated sandbox environments per COI, logically isolated using Zero Trust principles,
- Ability to deploy applications using:
  - Virtual Machines (VMs),
  - Containers (if applicable),
- Support for multiple application tiers (application, database, storage).

1.10.4.2 Data Ingestion and Handling

- Controlled mechanisms to ingest application data into the sandbox environment, including:
  - Secure transfer procedures (manual or automated),
  - Malware scanning and integrity verification,
  - Traceability of imported datasets,
- Enforcement of:
  - Data classification and labelling,
  - Encryption at rest and in transit.

1.10.4.3 Identity and Access Management

- Integration with secure identity services,
- Enforcement of:

  - Multi-Factor Authentication (MFA),
  - Role-Based or Attribute-Based Access Control (RBAC/ABAC),
- Segregation of users across COIs and applications.

1.10.4.4 Network and Connectivity

- Access to sandbox environments via the Direct Secure Connection,
- Isolated network environments ensuring:
  - No lateral movement between applications or COIs,
  - No exposure to the public internet.

1.10.4.5 Application Dependency Support

- Capability to host and configure common application dependencies, including:
  - Databases,
  - Middleware,
  - File storage solutions,
- Ability to replicate key aspects of legacy environments where required.

1.10.4.6 Observability and Monitoring

- Provision of monitoring capabilities allowing COIs to assess:
  - Application availability,
  - Basic performance characteristics,
  - Security events (logs, access attempts),
- Centralised logging to support audit and troubleshooting.

1.10.4.7 Configuration and Deployment Support

- Mechanisms to deploy application artefacts into the sandbox (manual or scripted),
- Version control of deployed configurations where applicable,

- Capability to support repeatable deployment--no requirement for full CI/CD pipelines.

1.10.5 Security Requirements

All Application Migration Sandbox and Cloud Readiness Validation activities shall comply with NATO Secret security requirements and shall:

- Ensure full data protection (at rest, in transit, and in use),
- Enforce strict isolation between:
  - COIs,
  - Applications,
  - Data sets,
- Maintain complete auditability of:
  - Data transfers,
  - Application deployments,
  - User activities,
- Prevent any unauthorised data exfiltration during migration and testing.

1.10.6 Roles and Responsibilities

- contractor Responsibilities:
  - Provide and operate the sandbox infrastructure,
  - Enable secure onboarding and hosting of applications,
  - Provide technical support and monitoring capabilities,
  - Document environment constraints and performance observations.
- COI Responsibilities:
  - Provide applications, datasets, and migration scenarios,
  - Perform application configuration and validation,
  - Identify required modifications for cloud readiness.

Migration shall be conducted as a collaborative effort, with contractor enabling and COIs validating.

1.10.7 Validation and Cloud Readiness Criteria

The contractor shall support validation demonstrating that applications:

- Can be deployed and executed within the sandbox environment,
- Maintain functional behaviour consistent with their intended use,
- Do not require fundamental architectural redesign to operate in the cloud,
- Can be isolated and secured in accordance with Zero Trust principles,
- Can operate without reliance on unavailable on-premise dependencies.

Cloud Readiness Outcome

An application shall be considered “cloud ready” within the scope of this prototype if:

- It can be successfully deployed in the sandbox environment,
- Any required modifications are limited and clearly identified,
- A rehosting approach is sufficient for transition to the future enterprise cloud.

1.10.8 Deliverables

The contractor shall produce:

Migration and Sandbox Report

- Description of sandbox architecture and setup,
- Applications onboarded and tested,
- Migration approaches applied,
- Identified technical constraints.

Application Cloud Readiness Assessment

- Per-application summary including:
    - Migration approach used,
    - Required adaptations,
    - Residual risks,
    - Readiness level (e.g., rehost-ready, requires adaptation).

Lessons Learned and Recommendations

- Key challenges encountered,

- Recommendations to accelerate migration in the Programme of Record,
- Identified systemic blockers (e.g., dependencies, security constraints).

1.10.9 Constraints

- Migration is limited to validation and preparation activities,
- No requirement exists to:
    - migrate full operational systems,
    - establish production DevSecOps pipelines,

The sandbox is not a production environment.

B. Appendix B- Secure Generative AI COI: Technical Specifications

1.1. Infrastructure and Deployment

- The AI environment shall be fully isolated and hosted within a secure, air-gapped cloud (physical or logical depending on the lot)
- No connections to external AI services or public endpoints shall be permitted
- High-performance compute (GPU clusters) shall be provisioned and isolated using Zero Trust enforcement mechanisms to prevent cross-COI access
- Secure data ingestion mechanisms (e.g., data diode or equivalent) shall be used to transfer classified data into the environment without exposing the system

1.2. Core AI Capabilities

Provide Artificial Intelligence as a service that enables orchestration of development of AI applications without building infrastructure or models from scratch.

- The system shall support AI-assisted analysis using classified internal data only
- Ability to implement a Retrieval-Augmented Generation (RAG) using a private vector database to enable context-aware responses
- A secure prompt management interface shall provide prompt templating, version control, and encrypted storage
- The system shall support model adaptation using mission-specific data through parameter-efficient fine-tuning techniques
- NATO shall retain full operational control over AI models, including configuration, usage, and auditing

1.3. Security Controls for AI

- An AI firewall shall be implemented to detect and prevent prompt injection and malicious input attempts
- The system shall prevent data leakage, including protection against prompt-based extraction techniques
- AI outputs shall be automatically scanned and sanitized to remove

unauthorized sensitive or personal data

- Controls shall be in place to prevent unauthorized modification, access, or extraction of AI model data

1.4. Data Controls

- All AI-generated outputs shall be automatically tagged with the appropriate classification level
- Role-Based Access: Usage is strictly tied to a user's specific clearance and mission; you only see what you are authorized to see.
- Access decisions shall be dynamically enforced and logged for audit purposes
- Data lineage shall be maintained to ensure traceability of all AI outputs

1.5. Acceptance Criteria

Criterion	Success Measure
Data Leakage Prevention	No evidence of classified data escaping the secure environment during high-volume AI operations
Audit Log Fidelity	100% of AI queries and responses logged with timestamp and user identifier
AI Response Speed	Response time < 2 seconds for standard queries with 100 concurrent users
Model Integrity	AI models cannot be modified or accessed by unauthorized users
Source Attribution	All AI-generated outputs include traceable references to source documents

1.6. Deliverables

- AI-as-a-service platform with built-in security controls
- Model agnostic hosting platform

- Controlled federated data access across COI

C. Appendix C - AFSC Digital Engineering (DE) / Mission Engineering (ME) COI: Technical Specifications

1. Platform Requirements and Technical Specifications

1.1. Approach

NATO programs manage classified models, data, and simulations in isolated silos, slowing every decision and eroding trust across the Alliance. The proposed environment offers a single, NS-level ecosystem that links a shared Authoritative Source of Truth (ASoT) while enforcing zero-trust security.

The AFSC DE/ME COI creates a secure shared workspace where teams across NATO can work together, share information, and build solutions that can be reused across multiple programs. It starts with a pilot environment that allows teams in different locations to collaborate securely at the NATO SECRET level in support of AFSC, Allied Command Transformation, and other efforts across the NATO enterprise.

1.2. Core Services

AFSC requires secure, distributed NS workbench for AFSC architects, mission engineers, analysts to : (a) develop and govern executable architecture artefacts [linkages/interface of System-of-Systems (SoS) End User Architecture (EUA) and SoS Technical Architecture (TA), which are developed by different teams]; (b) run repeatable mission-thread analyses; and generate evidence packs to support concept development, capability development/refinement, and trade-space and Analysis of Alternatives (AoA) decisions. The outcomes are AFSC decision evidence, and the software tools listed below are the means to produce that evidence, not the end-product themselves.

The AFSC DE/ME COI will be delivered in two iterations: first, a secure collaborative environment for teams to develop and share engineering work; second, an expanded environment to support mission analysis, simulations, and decision-making.

Iteration 1 – Digital Engineering Collaborative Architecture Environment:

- **Authoritative Architecture Repository Service:** A multi-user authoritative model repository supporting controlled collaboration, role-based access control, audit logging, backup and restore, and configuration-management concepts such as baselines, branches, tags, and approved releases for architecture artifacts.

- **Source Control and Configuration Management Service:** A configuration management tooling-based service, for scripts, plugins, profiles, templates, configuration files, and integration code used to customize tools, automate workflows, and manage digital engineering environment configurations, including branching, merging, tagging, and traceability to approved architecture baselines.
- **Scripting and Tool Integration Environment:** An execution environment for supported scripting and automation languages, APIs, and SDKs required for architecture tool customization, model query and extraction, validation, data exchange, and workflow automation, including languages such as Java, JavaScript, Groovy, and Python, together with associated dependency/package management and developer tooling or IDE support as required.
- **Shared Artifact Storage:** Secure storage for model exports, generated documents, interchange files, scripts, configuration packages, and related collaboration artifacts, including retention, backup, restore, and access-control procedures.
- **Identity and Access Management:** Centralized authentication and authorization services supporting distributed team collaboration across repository, source control, and artifact services, including role-based access control, account management, and auditability.

Iteration 2 – Mission Engineering Simulation and Trade Space Analysis Environment:

- Analysis Source Control and Run Provenance: A configuration management tooling—based service, for scenario definitions, simulation scripts, automation code, configuration files, and analysis workflows, with the ability to tag releases and maintain traceability among software versions, input data baselines, execution parameters, and resulting analysis outputs or evidence packs.
- Execution Environment for Analysis Automation: The ability to execute scripted automation and workflow pipelines for batch simulation runs, post-processing, evidence-pack generation, and repeatable trade space analysis, with logging, scheduling, failure reporting, and reproducibility controls.
- Artifact / Evidence Pack Storage: Secure storage for scenario packages, model exports, run outputs, reports, plots, logs, and evidence packages, including retention, backup, restore, and controlled access procedures.
- Tool Runtime and Integration Services: An environment to host, configure, and integrate mission engineering and trade space analysis tools introduced in later increments, including tools such as AFSIM, STK Enterprise, MATLAB, Ansys ModelCenter, and other approved physics-based simulation tools, together with the interfaces required for automated workflow execution and data exchange.

- Note: AFSC will fund commercial per-seat or instance licenses for AFSC-specific modelling, simulation, and analysis tooling software as listed in the appendix for AFSC DE/ME COI.
- Shared Reference Data and Scenario Baseline Management: Controlled storage and version management for common input datasets, scenario baselines, model parameters, reference libraries, and other reusable analysis content used across simulation and trade space analysis activities.

1.3. Infrastructure & Deployment Model (Hybrid by Design)

The AFSC DE/ME COI toolchain includes multiple GUI applications, therefore the contractor shall provide a hybrid hosting model:

- Server-side services (container/Kubernetes where vendor-supported or VMs otherwise): collaborative repositories (architecture repository, version control, artifact storage), APIs, authentication integration, logging.
- VDI / Virtual Machines for GUI-heavy engineering tools (e.g., architecture authoring and simulation desktop tools).
- VDI shall be the primary end-user access method for AFSC COI power users (no Secret data stored on local endpoints).
- GPU-enabled VDI capability when required for future 3D/visualization workloads (e.g., AFSIM, STK, MATLAB visualization).
- Air-gapped operations: No route to public internet; offline patching, data updates (e.g., geospatial, terrain, space related data, and model libraries) and software ingestion procedures must be defined and auditable.

1.4. Users, Roles, and Collaboration Model

- Pilot user scale: Initial capability for ~5 concurrent power users (architects/analysts), with a clear scaling path (e.g., 20+) if required.
- User roles:
  - Architects/Analysts: full tool access via Virtual Desktop Infrastructure (VDI) desktops. VDI access and performance requirements are specified in appendix for AFSC DE/ME COI.
  - Reviewers: web-based read/comment access where supported (e.g., model review portals), without installing full desktop authoring tools.
- Collaboration objective: Support distributed team working across sites with controlled sharing, versioning, and traceability (architecture models,

scripts/configuration, run outputs, evidence packs).

1.5. Digital Engineering Environment Tool Stack

The AFSC DE/ME COI shall be implemented initially as a proof-of-concept platform hosted on the Secure Cloud Service (SCS) Prototype. The platform shall host the software tools and supporting services required to enable timely, responsive, and information-rich distributed collaboration by geographically dispersed team members.

The contractor shall support both:

- client-side deployment of required desktop tools on VDI and/or virtual machines, and
- server-side hosting of required collaboration, repository, and web-access services.

Iteration 1 – Digital Engineering Collaborative Architecture Environment:

The contractor shall support installation, configuration, integration, and operation of the following tool stack currently used in HQ SACT, for the initial digital engineering collaborative environment:

- Architecture Modeling Clients:
  - Dassault Systèmes Cameo Enterprise Architecture with required Plugins for architecture development, analysis, and exchange.
  - Archi and Sparx Enterprise Architect, when required for coordination or exchange with stakeholders developing or maintaining models in that environment.
- Model Repository and Collaboration Services:
  - Dassault Systèmes Teamwork Cloud, serving as the controlled model repository and collaboration backbone for multi-user architecture development.
  - Cameo Collaborator for Teamwork Cloud, providing web-based model presentation, review, comment, and limited editing support for broader stakeholder participation.
- Scripting, API, and Automation Tooling:
  - Support for required scripting and automation languages, SDKs, and APIs used for tool customization, model query/extraction, validation, data exchange, and workflow automation, including Java, JavaScript, Groovy, and Python, as required.
  - Support for associated developer tooling, including integrated development environments and notebook-based environments, such as IntelliJ IDEA, Eclipse, Jupyter, or equivalent approved tools.
- Source Control Tooling:

- A configuration management tooling—version control environment for scripts, plugins, profiles, templates, configuration files, and integration/automation code associated with the digital engineering environment.

Note: AFSC will fund commercial per-seat or instance licenses for AFSC-specific modelling, simulation, and analysis tooling software as listed in the appendix for AFSC DE/ME COI.

Iteration 2 – Mission Engineering Simulation and Trade Space Analysis Environment:

The platform shall be capable of accommodating later addition of mission engineering simulation and trade space analysis tools, including:

- Ansys STK Enterprise, for physics-based mission modeling, visualization, and systems analysis.
- AFSIM, as a separate mission simulation framework, subject to its releasability by US Government.
- Ansys ModelCenter, for multi-tool workflow automation, trade studies, and optimization.
- MATLAB, for computational analysis, algorithm development, data reduction, and visualization.
- Additional approved tools, as required, such as:
  - Keysight EXata Network Modeling, for network digital twin / network modeling and emulation; and
  - HII TIREM, for terrain-aware RF propagation, electromagnetic environment analysis, and path-loss modeling.

Note: This SOW shall not assume that all tools operate as browser-based SaaS applications. The AFSC DE/ME COI requires support for a mixed deployment model consisting of desktop engineering tools hosted on VDI/Windows virtual machines, together with server-side collaboration, repository, and web-access services.

1.6. Performance and Responsiveness Requirements (VDI/GUI-based Engineering Tools)

Because the AFSC DE/ME COI relies on interactive, GUI-based engineering tools (e.g., architecture modeling and 3D visualization), the contractor shall provide a user experience suitable for day-to-day engineering work by geographically dispersed

users. Performance shall be verified during pilot operations and documented in a performance report.

1.6.1. VDI Interactivity and Network Performance Targets

The contractor shall provide VDI sessions that maintain acceptable interactive responsiveness for engineering tools under normal operating conditions for the pilot user load. As a baseline target for the pilot, the contractor shall demonstrate:

- VDI round-trip latency (RTT): target ≤150 ms between user endpoint and VDI session for normal conditions (measured during agreed test windows).
- Jitter: controlled such that interactive sessions remain usable (contractor to report measured jitter distribution during tests).
- Session stability: no unexpected session drops during agreed test periods for the pilot concurrency level.

Note: If some sites experience higher latency due to external constraints, the contractor shall document the limitation and propose mitigation options (e.g., regional access nodes, protocol tuning, bandwidth allocation).

1.6.2. Graphics/Visualization Performance (3D Tools)

Applicable to Iteration 2 or to any later phase in which 3D visualization tools are introduced. For tools requiring 3D visualization capabilities, the contractor shall provide an environment that supports usable interactive visualization for representative scenarios.

The contractor shall:

- Provide GPU-enabled VDI and/or virtual machine capability, where required, to support interactive 3D visualization performance.
- Demonstrate usable 3D interaction, including pan, zoom, and rotate functions, for an agreed representative scenario size and complexity.
- Configure the environment so that graphics performance is sufficient to support routine analysis, review, and stakeholder interaction for the applicable 3D tools.

1.6.3. Representative Workload Timing Targets

The contractor shall demonstrate that the environment supports at least ~5 concurrent power users for the pilot phase, with a clear scaling path (e.g., 20+) if required, executing normal engineering activities without unacceptable degradation in responsiveness. If additional scaling is requested during the prototype, the contractor shall provide indicative resource scaling options (compute/storage/VDI pool/GPU pool).

1.7. Data Handling for Mission Engineering Inputs

The AFSC DE/ME COI shall support controlled handling of curated datasets and model libraries required for digital engineering and, in later increments, mission engineering analysis. These datasets may include threat and environmental assumptions, system parameters, performance envelopes, model libraries, mission thread templates, geospatial data, and space-related reference data, as applicable to the approved implementation scope.

The contractor shall:

- Support fully disconnected on-premise operation of the software tools within the NATO Secret security boundary, with no dependency on public internet endpoints.
- Provide an auditable air-gap data ingestion process, including approved media transfer, malware scanning, provenance tagging, integrity verification as required, access control, and logging.
- Support data labeling and role-based access control within the COI.
- Support controlled export of approved results and products in accordance with applicable security policy.

Applicable to Iteration 2 or to any later phase in which STK, GCS, or comparable 3D mission visualization tools are introduced:

- Provide an internal geospatial content capability to supply terrain, imagery, and other 3D geospatial content to authorized clients operating in the on-premise environment.
- Where STK Enterprise is included in scope, provide this capability through STK Geospatial Content Server (GCS), or equivalent Government-approved capability, to host, process, and serve terrain, imagery, and related 3D geospatial content in an offline environment.
- Provide an auditable ingestion and update process for geospatial datasets, including

terrain, imagery, and tilesets, with integrity verification, malware scanning, provenance metadata, access control, and logging aligned to air-gap operations.

1.8. AFSC DE/ME COI Operational Workflow Support

The environment shall support repeatable analysis workflows:

- Create and manage architecture baselines (SoSA-EU/SoS-TA linkages), with controlled change management.
- Execute mission-thread analysis runs (single runs and run matrices) and capture run configuration + results in an auditable way.
- Generate and store decision-support evidence packs (assumptions, inputs, outputs, plots/tables, run provenance).

1.9. Storage and Compute Requirements

1/ Initial Pilot for 5 users:

Number of accounts:	5
Peak concurrent users:	5
CPU needed:	**73 vCPU cores minimum**
GPU needed:	**2 × GPU-accelerated nodes** – 1 × NVIDIA A30 + 1 × NVIDIA A40 (total ~ 2 × GPU-accelerated compute slots). *(only for the "Iteration 2" part of the stack)*
RAM needed:	**266 GB**
Storage needed:	**~5–6 TB active storage minimum** (repositories, scenario caches, geospatial content, outputs). **Backup/Archive: ~4–6 TB minimum,** depending on whether full GCS content is protected.
IOPS:	**>= 20,000 IOPS recommended floor**
High availability / failover needed?	Yes for all mission-critical services (Teamwork Cloud, Git, STK, GCS, AFSIM, ModelCenter, MATLAB). Recommend active-passive pairs in **two geographically-separate regions** (e.g., EU-West-1 & EU-Central-1). Non-critical tools (Archi, Sparx, EXata, TIREM) can remain single-instance.

(Note: The GPU count is expressed as nodes rather than "GPU cores", because modern server GPUs expose thousands of CUDA cores and are licensed per board. The A30 and A40 are the current NATO approved data center GPUs that balance FP32 performance for 3 D visualisation and double precision support for physics-based simulation.)

2/ If we eventually scale to ~20 users (long-term vision), the numbers look like this:

Number of accounts:	20
Peak concurrent users:	20
CPU needed:	**290 vCPU**
GPU needed:	**4 × GPU-accelerated nodes** (2 × A30, 2 × A40)
RAM needed:	**~1.0-1.1 TB**
Storage needed:	**~20-24 TB** active **+ ~12–16 TB backup/archive**
IOPS:	**≥ 70,000 IOPS** (provisioned SSD tier)
High availability / failover needed?	**Full active-active across two regions** for every service listed as "Yes".

1.10. Acceptance Criteria for AFSC DE/ME COI

The Security Audit and prototype evaluation shall verify the AFSC DE/ME COI can support the following minimum pilot outcomes:

Criterion	Success Measure
Collaboration	5 concurrent users can access VDI/VM desktops, check out/update architecture artefacts via the repository, and collaborate without data leakage across COIs.
Traceability & provenance	Each analysis run can be traced to a specific model baseline and script/config version (Git tags or equivalent), with stored evidence pack outputs.
Isolation	Demonstrate micro-segmentation and that compromise of another COI cannot access AFSC DE/ME COI repositories or VDI sessions.
Recoverability	Demonstrate backup/restore for the architecture repository and evidence store (Recovery Point Objective (RPO)/ Recovery Time Objective (RTO) targets defined for pilot).
Audit logging	Central logging captures user access, repository changes, and execution events sufficient for forensic reconstruction.

1.11. Deliverables

The contractor shall provide a Performance and Responsiveness Report for the AFSC DE/ME COI that includes:

- Measured RTT, jitter, and throughput observations during test events
- VDI session performance metrics (CPU/RAM/GPU utilization, display protocol settings)
- Timing results for the representative workload tests
- Identified bottlenecks and mitigation recommendations

D. Appendix D - Maritime Operations (CMRE/TFX Arctic) COI: Technical Specifications

1.2. Acoustic and sonar signal processing

- High-volume data storage: specialised storage optimised for raw acoustic and sonar data from hull-mounted and towed sensor arrays
- Automated vessel recognition: algorithms to identify vessel signatures through spectral analysis of acoustic signals
- Environmental modelling: processing of water column temperature and salinity data to model acoustic propagation and sensor performance

1.3. Disconnected operations

- Store-and-forward architecture: maritime assets must be able to cache data locally and synchronise with the cloud when a secure communications link is available
- Traffic prioritisation: critical alerts (e.g., torpedo detection) must be prioritised over routine traffic when bandwidth is limited

1.4. Maritime awareness

- Fused vessel tracking: a dashboard correlating unclassified vessel transponder data with classified intelligence imagery to identify vessels operating without active transponders
- Unmanned system control: secure, encrypted telemetry links for remote monitoring of unmanned surface and underwater vehicles

1.5. Storage and Compute Requirements

- This project requires the following specifications to operate:
  - Preferred technology: Logical airgap (current architecture is cloud-hosted on Azure; physical airgap is not currently in use but can be evaluated if required).
  - Number of accounts: ~100
  - Peak concurrent users: ~50

- CPU needed: ~264 vCPUs (logical cores) across all services.
- GPU needed: None required at this stage; GPU workloads are planned for the future.
- RAM needed: 1,592 GB (1.6 TB) total across all services.
- Storage needed: ~55–95 TB estimated total, based on a data flow of 150–260 GB/day across ingestion, processing, and fusion stages, with a 1-year retention period.
- IOPS: Peak ~35,000–40,000 requests/sec. The platform currently uses Azure Data Lake Storage Gen2 (ADLS Gen2) as the shared storage backend for all Databricks clusters and ingestion pipelines.
- High availability / failover needed: Not required at this stage; multi- region failover may be considered in the future.
- Growth planned over the next 12 months in any of the above: ~ +20% across users, data volume and computing.

Acceptance criteria / Expected level of performance

Criterion	Success Measure
Acoustic Data Integrity	No loss of signal quality when data transfers from the secure connection to cloud storage.
Dark Target Correlation	An unidentified radar contact automatically matched to a historical acoustic signature in under 10 seconds.
Geofencing Alerts	Automatic alerts triggered when tracked vessels enter protected maritime zones.
Offline Synchronisation	Full data consistency restored after a simulated 24-hour communications blackout.

1.6. Deliverables

- Maritime Signal Processing Framework: documentation of the technical approach to processing raw underwater sensor data
- Maritime Asset Identity Register: a Zero Trust registry of all authorised maritime platforms permitted to connect to the cloud service
- Acoustic Propagation Report: a simulation report demonstrating how environmental data is used to predict sensor performance

E. Appendix E – Overall Acceptance Criteria

Req Hierarchy ID	Requirement	SCS Acceptance Criteria
1	SCS shall provide infrastructure and core services	1 Infrastructure and Core services are cloud adopted, native, and operational across all entities of the SCS 2 Full spectrum of necessary infrastructure/core services fully configured to run globally, serving apps/services/COIs and office automation applications at NS level.
2	SCS shall establish identity directories	1 Single instance of SCS wide user identity directory hosted on the SCS prototypes that stores dummy NS user identities and their attributes
3	SCS shall provide end user devices and services	1)Centralized management and control of end user devices that will be used to access SCS. 2) Seamless end user experience with the SCS. 3) Enhanced device security, and small fraction of time needed to configure a device. 4) Application of conditional access policies to SCS resources based on the identity of the end user and the device that is being used

3.1	SCS shall provide cloud adapted end-user services and devices for seamless connectivity to the SCS	Purchase of laptops, tablets, security/smart cards as well as Enterprise level upgraded facility access/entrance cards done in accordance with the specified parameters of Quality of Service (QoS – to be defined) that are necessary to establish the connections
3.1.1	SCS shall establish Virtual Desktops by enabling VDI (Virtual Desktop Infrastructure) as connectivity option to specified COIs	1) COI users use a cloud-hosted version of operating systems 2) Modern browsers to access Virtual Desktop-hosted experiences
3.2	SCS shall provide cloud based Enterprise Mobility Management (EMM)	1 Centralized end-user device management capabilities as a service used to configure and protect user's devices and enrolment (registry). 2 Via integrated policy engine, Automated end-user device compatibility with respect to NATO SCS security policies and latest updates 3 NATO SCS Virtual Machine Image Repository 4 NATO-owned Device (NOD) enrolment
3.3	SCS shall provide asset management through inventory management system	1 Centrally managed device inventory system that stores and tracks owner, location, status, maintenance, and descriptive information for SCS end-user devices.
4	SCS shall produce physical design providing underlying on-premises	Optimized commercial cloud access for SCS's on-premises users.

	physical network layer re-design	
4.1	SCS shall re-design NS Campus LAN for the SCS access locations	CAMPUS Local Area Networks (LANs) to be ready for commercial cloud usage
4.2	SCS shall optimize network design to access commercial cloud for on premises users by implementing best practices	1 Establish connectivity between on-premises Enterprise WAN and commercial cloud's data centres by enabling direct connection to specific set of supported features and services that are offered by commercial cloud data centres - For each of SCS locations, leasing or purchase of dedicated fibre circuits that will cover from that locations WAN end-point to the nearest commercial cloud entry point. - If necessary, deployment and configuration of fibre circuits
4.3	SCS shall establish application performance and data synchronization in disconnected, enabling compute workloads with little or no connectivity to commercial cloud for select COIs	1 SCS provides offline client access to storage and compute power in a disconnected environment 2 Capability developed enabling working offline for the select SaaS COTS products including core services and office automation. 3 Offline application synchronization for critical Non-COTS Core Services has been established.
5	SCS shall establish cloud specific Service Management and	1 Command Line Interface CLI is being used to create and manage cloud resources from the command line or

	Control (SMC) platform in form of user/machine interfaces of the cloud platform for interacting, using, consuming, management and monitoring purposes	through scripts and other automation tools 2 GUI (Graphical User Interface) access for SCS resource management 3 SMC fulfils enhanced network capacity, storage and computing capabilities in achieving 4 individual cloud characteristics across SCS: On-demand self-service, Rapid elasticity, Broad Network Access, Resource pooling
5.1	SCS SMC shall provide proactive incident resolution to Level 1 and Level 2 service requests up to Infrastructure as a Service layer incidents	1 Identification of the reoccurrence of previously identified, recorded and orchestrated IaaS incidents 2 Generated SMC logs have been centrally stored and aggregated automatically for instance resolution and problem root level analysis automations providing trackable incidents
5.2	SCS SMC shall enable automated control and resource optimization by leveraging a metering capability at some level of abstraction appropriate to the type of service including storage, processing, and network bandwidths.	1. Determination of the log collection methods, sources, metrics attached, log aggregation, proactive incident resolution attachment to the monitoring capability in scope of SMC functionality. 2. Configuration, development of a platform to get real time insights of application, service container or serverless insights via dashboards.
5.3	SCS SMC shall provide IaaS Monitoring and capacity management	1 Global event log collection, aggregation, storage, correlation and reporting, as well as incident tracking and

		resolution both for reactive and proactive ways 2 Auto notification sub-capability in accordance with quantification levels set for identified operational needs 3 Creation of specific service usage and security reports such as annual/monthly/weekly outage reports for different services per site per command
5.4	SCS SMC shall provide customizable service KPI assignment, granular per site per command (Domain and Element Level)	1 Dynamic assignment of granular level KPIs for different services per site per command 2 Creation of workload utilization baselines for future comparison, and identify thresholds to automatically expand or decrease capacity KPIs depending on the usage pattern
5.5	SCS SMC shall automate platform and service provisioning by establishing Infrastructure as code (IaC) capability	1 SCS infrastructure service deployments will be automated, consistent and repeatable 2 Technical scripting of SCS cloud governance policies, enabling continuous auditing and compliancy checks of running SCS services 3 Deployment, update, deletion, and management of SCS resources in a single, coordinated operation
5.6	SCS SMC shall establish end user self-service catalogue	1 Centralized request portal integrated into the SCS SMC platform, giving end users access to SCS business services they will need and order,

		implementing domain SCS workflow of request fulfilment
6	SCS shall establish real time compliancy checks and continuous/autonomous audit / accreditation of its services	Flexible and dynamic SCS cloud environment with its ever changing and ephemeral workloads by providing services that enable NATO to formalize account design, automate security and cloud governance controls, and streamline auditing. This will ensure workload, resource accessibility and data processes are always compliant with current security policies.
6.1	SCS shall provide continuous/autonomous audits of SCS Services	1 SCS accreditation being done as a continuous and living process, relying on dynamic cyber security measures to be applied to the ever-changing commercial cloud environment and external threats 2 Accreditation/Auditing becoming a capability, done autonomously, and adaptable to changing configurations
6.2	SCS shall achieve continuous compliance checks, real-time auditing and issue real-time alerts about misconfigurations	1 SCS relying on (near) real-time auditing and compliancy checks concerning security policies providing continuous monitoring of deploying services to keep SCS up-to-date with current versions of services and to be aligned with ever-changing cyber security needs.

6.3	SCS shall be accredited with respect to static (on-paper) compliancy, auditing and certification standards	1 Completion of the Analysis and determination of compliancy, auditing and certification standards NATO provides 2 Preparation of contractual security compliancy standards (on-paper auditing) and cloud security alliance for cloud service provider's delivered services to the SCS
7	SCS shall implement defense in depth, a layered approach to cyber security following zero trust methodology	1 SCS's each IT layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data
7.1	SCS shall provide Physical/Personnel security	1 Provide background checks of all of the cloud provider personnel who have access to service infrastructure (both physical or remote) 2 Limiting access to SCS SMC and the equipment dedicated to NATO in commercial cloud environment to authorized personnel only (NS Accredited)
7.2	SCS shall provide security policy administration	1 Development of the following components (as part of EMM and SMC functions), providing generation, distribution, enforcement and update of SCS security policies: Policy Engine (PE), Policy Administrator (PA), Policy Enforcement Point (PEP)
7.3	SCS shall provide Identity and access security controls	1 Multifactor

		authentication or condition-based access, to control access to infrastructure and change control supporting different identities of users, services, or devices 2 Cybersecurity strategies and technologies in place for exerting control over the elevated (PAM "privileged") access and permissions for users, accounts, processes, and systems across an IT environment to restrict access rights and permissions for users to absolute minimum necessary to perform routine, authorized activities.
7.4	SCS shall establish perimeter security of network's IaaS endpoints	Monitoring and control of communications in place at the external boundary of the SCS to prevent and detect malicious and other unauthorized communications, with boundary protection devices and services.
7.5	SCS shall provide network layer security	1 Network segmentation and network access controls (network layer real-time threat protection, end-to-end encryption, monitoring, and analytics) in place of cloud hosted SCS, to limit communication between resources. 2 Outgoing/Incoming Internet Access is disallowed
7.6	SCS shall provide IaaS compute layer security	Enforcement of virtual server protection Policies and processes such as change management and software updates,

		providing consistent appliance of governance and compliance rules and templates when provisioning virtual servers, auditing for configuration deviations, and remediating automatically where possible.
7.7	SCS shall provide IaaS hosted application layer security	SCS IaaS hosted applications are secure and free of security vulnerabilities
7.8	SCS shall provide public key infrastructure (PKI) (Key Management Service)	SCS can generate, distribute, sign and store certificates issued by the enterprise to resources, subjects, services and applications
7.9	SCS shall provide data layer security	Controls have been developed and configured to manage access to commercial cloud hosted data and encryption to protect data
7.9.1	SCS shall provide Data residency	1 SCS data stored within a specific NATO geographic boundary preventing data flow and replication through a non-NATO region 2 SCS commercial cloud hosted global services configured to avoid replication of NATO data across non-NATO countries
7.9.2	SCS shall provide data sovereignty	SCS data security compliancy is established with respect to NATO data security directives and policies through administrative policies and technical controls that govern who can access data, how it is used

		and stored, and how long the user can retain it.
7.9.3	SCS shall provide Encryption for data at rest	SCS stored data is inaccessible without appropriate decryption by secure cryptographic keys via SCS service to create and control keys used to encrypt user data
7.9.4	SCS shall provide Encryption for data in transit	SCS encrypting the data at the application layer before sending it over a network
7.9.5	SCS shall provide encryption and privacy for data in use	1 SCS encrypting the data in end-user device RAM 2 Physical protection in place to restrict access to data in use for non owners
7.10	SCS shall implement initial steps towards NATO Alliance data centric security	1 Basic Labelling implemented limited to the application layer and office automation products 2 Labelling policy settings will be protected by Documents Right Management 3 Information Rights Management established by having Owners or publishers apply labels to limit access to specific users and groups or to data in specific geographies, mandate encryption or set mandatory retention or deletion periods of data 4 SCS providing data loss prevention by scanning documents in transit labelled as ‘NATO Secret’ and ‘NATO Restricted’ and block the

		content from being shared. 5 SCS providing Data Lifecycle Management by enforcement of data deletion and retention policies, and help meet record keeping requirements including disposition approval, event-based retention triggers, and immutability of files
8	SCS shall establish the infrastructure virtually	1 Virtual private clouds and their associated subnets have been created in which each site or node will have its own sub-virtual private cloud in the form of a separate, dedicated tenant, with capability to have its own security measures applied within a specified sandbox. 2 Subnets have been established representing either represent a different sub-site within the NATO entity or host services that have specific requirements for network routing or to limit access to commercial cloud services for specific subnets with a virtual network service endpoint including creation of network segments/tenants for COI applications
8.1	SCS shall provide and configure private connectivity between virtual networks by peering	1 Private network traffic between sites with no public internet gateway or encryption required has been established. 2 Each location will have a low latency, high-bandwidth connection to the others. supporting cross

		regional data replication enabling operation of distributed near real time COI applications
8.2	SCS shall prepare on-premises network environment by deploying and configuring VPN gateways	Virtual VPN gateways have been delivered providing encrypted traffic between cloud-hosted virtual networks and the remaining on-premises networks (virtual site-to- site VPN gateways) as well as enabling individual devices to virtual networks (Point-to-site) gateways
8.3	SCS shall deliver virtual WAN (Wide Area Network)	1 Integrated connectivity solutions in hub and spoke as well as intuitive troubleshooting enabling different types of users who will have different connection options of the following: Full access from on-premises without internet, Limited access outside network without internet connection 2 SCS DNS configuration in place, both for the on-premises LAN-WAN DNS settings, such as DNS routing policies etc, , and commercial cloud specific DNS settings
9	SCS shall provide IaaS	SCS IaaS is operational providing the following capabilities listed as sub requirements
9.1	SCS shall host Virtual Machines for the services that have migration option of deployment to SC IaaS	1 For the services that have migration option of deployment to SCS IaaS, Virtual Machine Analysis of the needed Instance types has been done 2 VM security groups, applying fundamental of network security, firewalls to the VMs have been attached 3 Development of the VM Instance Placement strategies based on the type

		of COI or application, and its capability requirements has been done 4 Attachment of different network drives with ability to keep persistent data to the VMs have been done 5 VM snapshot procedures, timelines, in scope of data portability solution provided
9.2	SCS shall develop auto customization scripts of the VMs	1 Configuration control of those under a common repository has been established 2 Scripts are attached to VMs, based on the needs of boot time or configuration purposes
9.3	SCS shall configure auto scalability of VMs	1 Auto scaling groups of specific applications have been established, both for vertical and horizontal in perspective/aligned with assigned/specific BCP plans and strategies, fulfilling assigned high availability rates/KPIs 2 IaaS Monitoring, automation of monitoring based on assigned metrics, such as CPU usage, automation of scale-out and scale-in policies will be provided
9.4	SCS shall configure VM load balancing	Depending on the identified COI, app/service use-cases, configuration of VM specific load balancing, choosing the right type
10	SCS development and deployment shall be verified and validated	SCS development and deployment has been verified and validated by providing the following capabilities listed below:
10.1	SCS shall prepare necessary test environments	1 Test Environments have been established as a separate tenant for the COI and office automation services/applications

		2 Engineering integration environment has been developed including the physical and virtual test environments that will be used to conduct required types of functional and non-functional tests covering the migration of services to the IaaS
10.2	SCS shall demonstrate full spectrum of real life test cases with real user types and authorizations	1 Test scenarios and inputs have been provided 2 Non-functional tests including cyber security, responsiveness, QoS parameter alignment have been done successfully 3 SCS connectivity options are reliable and secure per site per service, providing necessary QoS parameter enhancement, fulfilling expected benefits from cloud environment 4 Existing and future potential issues, all resolved in that test environment regarding data residency/sovereignty of commercial cloud's global services
11	SCS provide materiel life cycle management based on the business continuity strategies defined per service	1 NATO relying on 'managed services' provided by commercial cloud to be always in optimum in terms of capacity, performance and reliability agreed through SLAs between the NATO and the service provider 2 Life cycle management of SCS owned and operated solutions have been established
11.1	SCS shall provide business continuity strategies and disaster recovery plans	1 SCS reacting to service disruptions with respect to specific plans 2 SCS business continuity plans are incorporated

		in 2 key elements: Risks and potential business impact, planning an effective response 3 SCS (Business Continuity Plan) strategies and plans are prepared with respect to different needs and workflows of 3 areas: Strategic, business, operational/tactical
11.2	SCS shall provide service catalogue	SCS service catalogue prepared by following a bottom-up approach, starting from standalone cloud services, identifying composition of every SCS hosted service at component level that will be composed of those standalone services
12	SCS shall provide different authentication strategies including federation of identity services	1 Cloud only identities, no identities are being maintained on-premises 2 Hybrid entities: SCS performing continuous synchronization of user identities hosted on-premises, providing SSO (single sign on) and commercial cloud 3 Business-To-Customer (B2C) identity as a service: SCS enabling external users outside the network to use their own account identities getting SSO 4 Analysis, and determination of necessary identity claims for specific applications or services, fullfilling their roles of assigned use cases as well as in case the need of federated authentication
13	SCS shall provide Identity Management (IdM)	SCS has full suite of identity management that is hosted on commercial cloud providing multi-factor authentication,

		role-based access control, security monitoring, alerting and auditing, self-service password and group management
13.1	SCS shall create generic SCS users and their NS service access types	Generic user types created and their initial service accessibilities enabled with respect to their IERs (Information Exchange Requirements) that will differ for Core and Standard Entity users
13.2	SCS shall provide role based access control	1 Capability of creating and defining dynamic flexible roles attached to the identities, group creation and assignment, configurable resource accessibility/authorization through attributes attached to roles 2 Dynamic user types introduced on the flow by configurable resource accessibility
13.3	SCS shall provide appropriate level of authorization to its resources by implementing PAM (Privileged Access Management) principles	List of user types/groups per service with their associated authorization levels have been identified and associated authorization levels to groups have been associated
13.4	SCS shall develop its directory services	1. Creation of the root account, physical protection in a vault has been established 2. Creation of the users and groups, including the Organizational units (OU) - directory hierarchies, applying resource-based security policies to the OUs 3. Create IAM multi factor authentication and password policies

		4. Enable CLI and develop re-usable scripts to manage resources. Store them in a common repository. 5. Configure audit logging of IAM credential usage reports

F. Appendix E - Glossary of Technical Terms

The following terms appear in this document. Definitions are provided for readers unfamiliar with cloud security or NATO terminology.

Term	Plain-Language Definition
Air Gapped	A security measure that physically or logically isolates a secure network from unsecured networks such as the public internet.
ABAC (Attribute-Based Access Control)	A security model that grants access based on a combination of user attributes such as clearance level, role, and organisational membership.
AES-256	A widely used encryption standard that protects data stored in the system.
BYOK / HYOK (Bring/Hold Your Own Key)	An arrangement in which HQ SACT, not the cloud provider, controls the encryption keys used to protect their data.
CDS (Cross-Domain Solution)	Hardware and software that enables controlled, verified transfer of information between networks of different classification levels.
COI (Community of Interest)	A group of users sharing a specific mission or functional area, each operating within their own dedicated and isolated cloud environment.
Contractor	The legal entity, authorized to conduct business where the Contract is performed, engaged to convey deliverables, perform services, or deliver goods pursuant to this contract.
FIDO2	An international authentication standard that supports physical security keys for strong, passwordless login.

Term	Plain-Language Definition
GPU (Graphics Processing Unit)	High-performance computing hardware used to run AI and data-intensive applications.
HSM (Hardware Security Module)	A physical device that securely generates, stores, and manages encryption keys.
IAM (Identity and Access Management)	The system that controls who can access which resources and under what conditions.
LLM (Large Language Model)	An AI model trained on large text datasets, capable of generating human-like responses to queries.
MACsec / IPsec	Network encryption standards that protect data travelling across a physical or virtual network link.
MFA (Multi-Factor Authentication)	A login process that requires two or more forms of identity verification (e.g. password plus a physical security key).
Microsegmentation	Dividing a network into small, isolated zones so that a compromise in one area cannot spread to others.
NATO Secret (NS)	The second-highest NATO classification level, used for information whose unauthorised disclosure could seriously damage NATO interests.
RAG (Retrieval-Augmented Generation)	An AI technique that allows a language model to search and reference a specific set of documents when answering questions.
SAML / OIDC	Industry-standard protocols that allow different identity systems to verify users across organisational boundaries.
System of Systems Architecture - End User (SoSA-EU)	ACT's operational/requirements focused portion of the overall SoS architecture for AFSC

Term	Plain-Language Definition
System of Systems Architecture – Technical Architecture (SoSA-TA)	NSPA's technical/system focused portion of the overall SoS architecture for AFSC
TLS 1.3	The current standard for encrypting data as it travels across a network.
VDI (Virtual Desktop Infrastructure)	A system in which users access a desktop environment hosted in the cloud rather than on their local device, keeping all data in the secure environment.
Zero Trust Architecture	A security model based on the principle of never automatically trusting any user or device, regardless of where they are connecting from. Every access request is verified.
ZTA Pillars	The five areas that Zero Trust security must cover: Identity, Devices, Networks, Applications, and Data.

G. Appendix G – Compliance Matrix and Evaluation Criteria

Bidder's technical proposal will be assessed based on criteria mentioned in the following tables. HQ SACT reserves the right to conduct technical discussions with bidder.

The technical evaluation will be done in two steps.

Bidder technical proposal will be first evaluated against the Compliance Matrix to be assessed as Compliant/Non-Compliant, and second against the Best Value Criteria Matrix to assess the technical score that the bidder obtains used afterwards to establish Best Value score based on the Technical/Price 70/30% criterion.

Ultimately, bidders shall clearly demonstrate by providing unequivocal explanation to where and how it meets the criteria set forth in this solicitation. The bidder must demonstrate their experience and expertise in the subject matter, in which will be graded in accordance with the Compliance Matrix and Evaluation Criteria.

An assessment of " non-compliant" in any of the criteria of the Compliance Matrix or a score of " 0" (zero) in any of the criteria of the Best Value Matrix, will result in the bidder' s proposal as being " Technically Non-Compliant"

A minimum total technical score of 60/100 points is required to adequately meet the requirement for this solicitation. A proposal with a minimum total technical score of less than 60 points will be graded as " Technically Non-Compliant" .

Compliance Matrix for both Lots

#	ITEM	COMPLIANT / NON-COMPLIANT
1	Contractor is headquartered in a NATO nation and all personnel supporting this contract (including subcontractor's personnel and consortium member) must be a citizen of a NATO member nation. If individuals have dual citizenship that includes a non-NATO nation, their citizenship must be provided. Contractor shall be legally authorized to operate in NATO member nations at the time of the bidding.	
2	Contractor is to provide a minimum of two past performance citations (for work within the past five years) to show that it has successfully completed work that is similar to or directly traceable to the requirements outlined in this SOW.	
3	Key personnel are citizens of NATO member nation with valid passport with no travel restrictions relevant for Contract performance. (Nationality must be indicated to include other citizenships)	
4	The bidder shall demonstrate the capability to deliver a secure cloud service off-premises distributed among different sites, within NATO countries.	
5	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.	

Best Value Criteria Matrix Lot 1:

#	Item	Range	Max Score (100 pts)
1	**Air-Gap Architecture Maturity:** Ability to deliver a fully isolated environment with no dependency on external/public networks, verified through architecture and connectivity validation.	0 pts: Internet dependency identified or external service required. 5 pts: Logical isolation only; external dependencies remain. 10 pts: Physical isolation demonstrated at 1 site. 15 pts: Physical isolation demonstrated at ≥2 sites with no external dependency. 20 pts: Fully independent infrastructure (compute, storage, network, IAM) across all nodes, validated with no external dependency.	20
2	**Security Assurance and Sovereign Control: Degree of NATO control over infrastructure, security stack, and cryptographic elements.**	0 pts: CSP retains control of security and keys. 5 pts: Partial NATO control of IAM or monitoring only. 10 pts: NATO control over IAM and audit logs. 15 pts: NATO control over IAM + logging + key lifecycle (HSM or equivalent). 20 pts: Full NATO control of all security components (IAM, logging, encryption, HSM, policies) with independent administration.	20
3	**Off-premises Multi-Site and Multi-National Distribution: Ability to deploy across different sites in different NATO nations, with operational consistency.**	0 pts: 1 site. 5 pts: ≥2 sites, single country. 10 pts: ≥2 sites, 2 countries. 15 pts: ≥3 sites across ≥2 countries 20 pts: ≥4 sites across ≥3 NATO countries with validated federation (consistent identity, policy, and workload deployment).	20
4	**Performance and Resilience in Isolated Environment: Ability to meet performance and availability targets under failure scenarios.**	0 pts: No SLA or failover capability. 5 pts: Single-node or no redundancy. 10 pts: ≥1 redundancy mechanism (compute or network). 15 pts: Multi-site failover with RTO ≤ 4h and RPO ≤ 1h. 20 pts: Full multi-site resilience with RTO ≤ 1h and RPO ≤ 15 min under tested failure scenario.	10

#	Item	Range	Max Score (100 pts)
5	**Cross-Domain Integration Capability: Ability to securely ingest data through controlled transfer mechanisms (CDS/CTS).**	0 pts: No secure ingestion. 2.5 pts: Manual transfer without audit. 5 pts: Controlled ingestion with logging. 7.5 pts: Automated transfer with validation and traceability (logs + integrity checks). 10 pts: Fully automated CDS/CTS with policy enforcement, audit logging, and data validation (classification + integrity).	10
6	**Migration Sandbox in Air-Gapped Context: Ability to onboard and validate applications in an isolated environment.**	0: No sandbox capability demonstrated 2.5 pts: Demonstrated Deployment of test environment only. 5 pts: ≥1 Demonstrated application deployed successfully. 7.5 pts: ≥2 Demonstrated applications deployed and executed with rehosting approach identified. 10 pts: ≥4 Demonstrated application deployed, executed, and validated as rehost-ready (no blocking dependency).	10
7	**Community of Interest workflows - Secure Digital Workspace, Secure Generative AI, Allied Federated Surveillance and Control (AFSC), and Centre for Maritime Research and Experimentation (CMRE).**	0 pts: No COI workflow deployment capability demonstrated 2.5 pts: 1 Demonstrated COI workflow deployment capability and operational for testing. 5 pts: 2 Demonstrated COI workflow deployment capability and operational for testing. 7.5 pts: 3 Demonstrated COI workflow deployment capability and operational for testing. 10 pts: 4 Demonstrated COI workflow deployment capability and operational for testing.	10

Best Value Criteria Matrix Lot 2:

#	Item	Range	Max Score (100)
1.	**Confidential Computing and Data-in-Use Protection: Ability to protect data during processing using secure enclaves/TEEs.**	0 pts: No data-in-use protection. 5 pts: Encryption at rest/in transit only. 10 pts: TEE used for limited workload. 15 pts: TEE used for ≥1 COI workload with attestation. 20 pts: TEE used for ≥2 COIs with attestation and isolation of all sensitive processing workloads.	20
2.	**Cryptographic Sovereignty and Key Management: Degree of NATO control over encryption keys and lifecycle.**	0 pts: CSP holds keys. 5 pts: Partial control (BYOK only). 10 pts: External key storage managed by NATO. 15 pts: Dedicated HSM under NATO control. 20 pts: Full sovereign key management (HYOK), with external NATO-controlled HSM, zero key exposure to CSP.	20
3.	**Hybrid Architecture Integration: Ability to securely integrate NATO infrastructure and cloud environment.**	0 pts: No hybrid integration. 5 pts: Basic connectivity only. 10 pts: Secure connectivity (network + encryption). 15 pts: Unified IAM and policy enforcement across environments. 20 pts: Full hybrid integration with unified IAM, ZTA enforcement, and consistent policy control across all workloads.	20
4.	**Scalability and Cloud Service Capability: Ability to scale for AI, COIs, and data workloads.**	0 pts: No scaling capability. 5 pts: Fixed capacity. 10 pts: Manual scaling supported. 15 pts: Auto-scaling for ≥1 workload (e.g. AI or data processing). 20 pts: Auto-scaling across ≥2 COIs supporting concurrent workloads ≥100 users, with performance maintained.	20
5.	**Application Migration and Cloud Readiness Capability: Ability to onboard applications and prepare them for enterprise cloud transition.**	0 pts: No migration support demonstrated. 2.5 pts: Deployment capability mentioned but not demonstrated. 5 pts: ≥1 Demonstrated application deployed successfully.	10

		7.5 pts: ≥1 Demonstrated application rehosted and executed with identified constraints. 10 pts: ≥1 Demonstrated application per COI deployed, executed, and validated as rehost-ready (no blocking dependencies for transition).	
6.	**Community of Interest workflows - Secure Digital Workspace, Secure Generative AI, Allied Federated Surveillance and Control (AFSC), and Centre for Maritime Research and Experimentation (CMRE).**	0 pts: No COI workflow deployment capability demonstrated 2.5 pts: 1 Demonstrated COI workflow deployment capability and operational for testing. 5 pts: 2 Demonstrated COI workflow deployment capability and operational for testing. 7.5 pts: 3 Demonstrated COI workflow deployment capability and operational for testing. 10 pts 4 Demonstrated COI workflow deployment capability and operational for testing.	10