NATO OTAN

Allied Command Transformation

Norfolk, Virginia | USA

NOTIFICATION OF PROCUREMENT OPPORTUNITY (NOPO)
Pre-Solicitation Notice
NATO Competitive Procurement

Secure Cloud Service (SCS)

ACT Reference #: RFP-ACT-SACT-26-54

Date of NOPO Publication: 04/28/2026

Anticipated Solicitation Release Date: 05/18/2026
Anticipated Solicitation Closing Date: 06/22/2026
Anticipated Contract Award Date: 07/15/2026

Point of Contact:
Supreme Allied Commander Transformation
BUDFIN – Purchasing and Contracting Branch
Attn: ACT Contracting Officer
7857 Blandy Road, Suite 100,
Norfolk, Virginia, USA 23551-2490
e-mail: hqsact.contracting@nato.int

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 NATO Secret is a critical enabler of this transition and of the NATO Digital Transformation programme.

To de-risk and accelerate cloud deployment, NATO Allied Command Transformation (ACT) intends to contract for a Secure Cloud Service (SCS). SCS will serve as a pre-accreditation validation environment, enabling iterative security testing, architecture refinement, and the generation of auditable evidence aligned with NATO Security Policy and NIST SP 800-53 Rev.5, while delivering a first level of operational cloud capability to priority Communities of Interest (COIs). Two prototypes will be delivered to address two different technologies.

The ACT hereby notifies the following Procurement Opportunity in accordance with the Procedure for NATO Competitive Procurement. This notification is issued to foster open and fair competition among eligible vendors from participating nations.

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

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

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

The contract will be awarded to one or two vendor(s) as a fixed-price contract with the following estimated period of performance per Lot:

- a base period of performance from the award date (estimated 15 July 2026) through 15 July 2027,
- one (1) option period may be added: 15 July 2027 – 15 July 2028

The estimated total contract value, inclusive of options, is approximately EUR 20,000,000.00 for the two Lots (estimated EUR 5,000,000 per lot per year).
The cloud architecture (prototype) prioritize representative capability validation over full operational scale.

Vendors are invited to review the requirements described herein and to register for participation through the appropriate national authority of the prime vendor's nation of origin. Vendors may form partnerships or sub-contractor relationships; however, all vendors, whether prime, partner, or sub-contractor, shall meet all identified eligibility requirements for participation.

Declarations of Eligibility shall be sent to hqsact.contracting@nato.int by **18 May 2026, 0900 hours**, Eastern Standard Time, Norfolk, Virginia. E-mail subject shall include the Procurement

Opportunity information along with company name (for example: ***RFP-ACT-SACT-26-54 Company XYZ*).**

This opportunity reflects NATO's commitment to transparency, equal treatment of suppliers, and the efficient delivery of goods, works, and services in support of NATO missions and participating nations. All eligible and responsible sources may submit a proposal, if and once RFP is published, which shall be considered by the ACT.

1. Title of Procurement Opportunity

Secure Cloud Service (SCS).

2. Description of Requirement

2.1. Background

Secure cloud capability delivery is on the critical path to NATO Digital Transformation and to enabling advancements in Artificial Intelligence (AI) and Multi-Domain Operations (MDO). Following decision at NAC (North Alliance Council) level, the alliance is accelerating its programmatic schedule to deploy cloud capabilities.

These milestones remain vulnerable to delays driven by two principal risk areas: security accreditation timeliness for off-premises NATO Secret cloud services, and the complexity of migrating Community of Interest (COI) applications into a cloud environment. Several priority COIs also require a first level of cloud capability.

The SCS is designed to de-risk cloud deployment and accelerate the overall roadmap by producing a comprehensive security audit report and accreditation evidence package to inform a future NATO Secret accreditation decision by December 2026, together with a cloud migration sandbox available to COIs through July 2027, or up to July 2028 with options.

2.2. Project Context & Objective

The SCS prototypes are contractor-operated service under NATO governance and data sovereignty controls supporting approximately 100 concurrent (scalable to 150 for testing conditions) users across at least four Communities of Interest. The capability will be deployed as a distributed off-premises cloud architecture across at least four sites (government or privately owned) in three NATO countries, validating two complementary architectural configurations and delivering operational services to priority COIs. The prototype prioritizes representative capability validation over full operational scale The primary objectives are:

2.2.1. Develop and validate two types of cloud architecture: a Physical Air-Gap Cloud (fully isolated infrastructure, maximum assurance) and a Hybrid Secure Cloud (cryptographically isolated commercial cloud leveraging Confidential Computing), demonstrating NATO's balance of security and operational flexibility.

2.2.2. Demonstrate and validate a federated, distributed, zero-trust-aligned cloud architecture across at least four sites (government or privately owned) in three NATO countries, grounded in NIST SP 800-207 and NATO Security Policy.

2.2.3. 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.

2.2.4. Establish a direct, dedicated secure connection between the User Headquarters and the Cloud Service Provider (CSP), with minimum target throughput of up to 10 Gbps (or

equivalent performance supporting AI and multi-domain workloads) and network-layer encryption.

2.2.5. Migrate and validate up to four priority COI application workflows — Secure Digital Workspace, Secure Generative AI, Modeling & Simulation, and C2 Operations demonstrating both refactor/rebuild and lift-and-shift migration approaches.

2.2.6. Deliver a Confidentiality, Integrity, and Availability (CIA) cloud environment, leveraging Cross-Domain Solutions (CDS) and Cross-Transfer Services (CTS) to enable controlled, automated data transfer and the secure delivery of updates and patches into air-gapped environments.

2.2.7. Provide a migration sandbox through July 2027, or up to July 2028 with options, to allow additional Communities of Interest to de-risk their transition to the cloud.

3. **Scope of Work** *[subject to change, pending solicitation to be published]*

The scope is focused on validating representative capabilities required for future operational scale, rather than delivering full enterprise deployment. The technical expertise and services required to be performed by the Contractor consist of the following lines of effort:

- **3.1. Security Architecture and Zero Trust Implementation.**
- **3.2. Data-Centric Security and Cryptographic Key Management.**
- **3.3. Secure Direct Connection and Headquarters Infrastructure.**
- **3.4. Development of Two Cloud Architecture Configurations.**
- **3.5. Delivery of Four Priority Communities of Interest (COIs).**
- **3.6. Application Migration Testing.**
- **3.7. Security Audit, Documentation, and Accreditation Support.**
- **3.8. Continuous Monitoring, Operations, and Sustainment.**

The estimated key milestones for delivery are summarized in the following table:

Milestone	Key Deliverables
Contract Award	Finalised Project Management Plan; Initial Security Architecture Design.
Secure Connectivity Established	Direct secure connection setup and 100 user onboarding.
Secure Clouds Developed	Two types of prototype cloud architectures and configurations on two sites.
COI Deployment	Deployment of COI capabilities across two operational sites with consistent functionality and availability.
Additional Site Deployment	Expansion to a total of four fully functional operational sites across three NATO countries.
Security Audit Execution	Comprehensive security audit to assess system compliance, identify vulnerabilities, and validate implemented controls.

Milestone	Key Deliverables
Final Audit & Accreditation	Delivery of final security audit report and, if achieved, system accreditation.
COI Migration Sandbox	Sandbox environment for Communities of Interest to de-risk cloud migration.

4. Vendor Eligibility

4.1. Participation in this Procurement Opportunity is restricted to vendors from NATO member nations.

4.2. Vendors (partners and subcontractors) must hold a NATO or National Facility Security Clearance (FSC). The Proposed team must hold NATO or National SECRET clearance, at the time of proposal submission.

4.3. Vendors must 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.

5. Access to Solicitation Documentation

Interested vendors, officially registered by national authorities with a Declaration of Eligibility, may participate in and receive the link to the solicitation documentation for this Procurement Opportunity by email when the solicitation is released on https://www.act.nato.int/opportunities/contracting/

6. Language of Solicitation and Bid Submission

6.1. Solicitation Documentation and Proposal Submission Language: English.

For the Financial Controller:

[Original Signed By]

Catherine GIGLIO
HQ SACT Acting Head of Contracts

Annexes:

A: Declaration of Eligibility for NATO Competitive Procurement

B: Distribution List

End of Notification

Annex A – Declaration of Eligibility for NATO Competitive Procurement

Date:

Declaration of Eligibility for NATO Competitive Procurement

To: ACT Procurement Authority

Subject: Declaration of Eligibility for NATO Competitive Procurement

Reference: **RFP-ACT-SACT-26-54** Secure Cloud Service (SCS).

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

- Vendor Name:
- Address:
- Point of Contact / Title: Mr./Ms.:
- Email Address:
- Phone #:

I certify that this vendor 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 vendor listed above is security cleared to the level of this procurement opportunity.

Extension to Other NCP Opportunities. In addition to the referenced project, this Declaration of Eligibility may be used for other ACT NCP opportunities and is valid for the vendor 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:

☐ Yes

☐ No

Note to Vendor: 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]

Annex B – Distribution List

NATO Delegations:

Albania	Greece	Poland
Belgium	Hungary	Portugal
Bulgaria	Iceland	Romania
Canada	Italy	Slovakia
Croatia	Latvia	Slovenia
Czechia	Lithuania	Spain
Denmark	Luxembourg	Sweden
Estonia	Montenegro	The Republic of Türkiye
France	Netherlands	The United Kingdom
Finland	North Macedonia	The United States
Germany	Norway	

Embassies in Brussels (Attn: Commercial Attaché):

Albania	Greece	Poland
Belgium	Hungary	Portugal
Bulgaria	Iceland	Romania
Canada	Italy	Slovakia
Croatia	Latvia	Slovenia
Czechia	Lithuania	Spain
Denmark	Luxembourg	Sweden
Estonia	Montenegro	The Republic of Türkiye
France	Netherlands	The United Kingdom
Finland	North Macedonia	The United States
Germany	Norway	