SAVUNMA VE HAVACILIK SANAYİ İHRACATÇILARI BİRLİĞİ

Sayı: 58224147-TİM.OAİB.26.ARG4.2026/19-1952 Ankara, 26/02/2026
Konu: ACO Piyasa Anketi/RFI-SOFCOM - Tactical Mission Network

Sayın Üyemiz,

T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı tarafından iletilen bir yazıda, Müttefik Harekât Komutanlığının (ACO), "RFI-SH-26-01" referans numaralı **"SOFCOM - Tactical Mission Network"** konulu bilgi talebine ilişkin duyurusu iletilmektedir.

NATO Özel Harekat Komutanlığı (SOFCOM) için stratejik bir görev ağı oluşturulacağı; bu ağın farklı veri akışlarını alıp görüntüleyebilen sohbet, video telekonferans, veri/video/dosya paylaşımı, gerçek zamanlı ses çevirisi ve veri gölü (data lake) gibi özellikleri destekleyen ortak bir operasyonel tablo sağlayacağı; sürdürülebilir bir servis tabanlı teslim modelinin SOFCOM tarafından belirlenen yönetim ve güvenlik sorumluluklarına uygun şekilde işletileceği; sıfır güven (zero-trust) mimarisi ve mobil cihaz yönetimi uygulamalarını içereceği ve uzaktan cihaz silme (remote wipe) işlevlerini sağlayan bağlantı teknolojileriyle uyumlu olacağı ifade edilmektedir.

Konu ile ilgili **soruların 25 Şubat 2026**, talep edilen bilgilere yönelik **cevapların** ise **17 Mart 2026** tarihine kadar dokumanda bildirilen **iki e-posta adresine birden** iletilmesi gerekmektedir.

Bilgileri ve gereği rica olunur.

Musa DEMİR
Genel Sekreter

EK: RFI (27 sayfa)

Ayrıntılı bilgi için: İftar Hatice İrem Biga - Uzman Yardımcısı
Ceyhun Atuf Kansu Cad.
No: 120 06520
BALGAT ANKARA
Tel : (312) 447 27 40
Faks : (312) 446 09 11
info@ssi.gov.tr
www.turksavunmasanayi.gov.tr
www.ssi.gov.tr

SUPREME HEADQUARTERS ALLIED POWERS EUROPE

GRAND QUARTIER GÉNÉRAL DES PUISSANCES ALLIÉES EN EUROPE

Mons - Belgium

Finance and Acquisition Directorate
Acquisition Management Branch
Building 101
7010 SHAPE

Tel: +32 65 44.53.47

POC: Maggie Brothers
Email: margaret.brothers@nato.int

Date 10 February 2026

REQUEST FOR INFORMATION (RFI)

ALLIED SPECIAL OPERATIONS FORCES COMMAND (SOFCOM)

TACTICAL MISSION NETWORK

RFI-SH-26-01

This RFI is for informational and planning purposes only, and it does not constitute a Request for Proposal (RFP)/Request for Quote (RFQ) or a promise to issue an RFP/RFQ in the future. It is not to be construed as a commitment by NATO for any actual procurement of materials or services.

Respondents are advised that NATO will not pay for any information or administrative costs incurred in response to this RFI. All administrative costs associated with responding to this RFI are solely at the responding parties' expense. Responses shall be UNCLASSIFIED and shall not contain any proprietary information or trade secrets. Any responses containing restrictive markings will not be read by NATO.

Any response submitted by respondents to this RFI constitutes consent for that submission to be reviewed by NATO personnel and Contractor employees supporting NATO Allied Special Operations Forces Command (SOFCOM), unless the respondent clearly objects in writing to the release of this information to NATO SOFCOM Contractor employees supporting NATO SOFCOM Tactical Mission Network.

(Original signed)

Margaret Brothers
Senior Contracting Officer
Strategic Acquisition Management Section

General Information	
Request For Information No.	**RFI-SH-26-01**
Project Title	**SOFCOM – Tactical Mission Network**
Due date for submission of requested information	**17 March 2026 (1700 CET)**
Contracting Office Address	**Finance and Acquisition Directorate** Acquisition Management Branch Contract Management Section BP 18/A, Bld/bât 101 7010 SHAPE
Contracting Officer	**Ms. Margaret Brothers** Senior Contracting Officer Strategic Acquisition Management Section Tel: +32 65 44 53 47 E-mail: margaret.brothers@nato.int
Additional Point of Contact	**Mr. Giuseppe COL**, Head, Contract Management Section Tel: +32 65 44 22 40 E-mail: giuseppe.col@nato.int

1. GENERAL

1.1. PURPOSE

1.1.1. The main purpose of this Request for Information (RFI) is to validate the procurement requirements and strategy to create a Strategic Mission Network for Special Operations Forces Command (SOFCOM) by establishing a secure, sustainable, interoperable, service-based capability.

1.1.2. This RFI also serves to raise awareness among potential suppliers regarding critical contract requirements for which actions must be undertaken well in advance of the formal solicitation processes or the contracts effective dates due to the time required for the completion of such actions (e.g., establishment of subcontracts, obtaining the required NATO security clearances, etc.)

1.1.3. This document and its annexes provide instructions concerning the participation in the RFI and the submission of responses and includes information on the intended procurement strategy and the contract objectives, requirements, constraints and terms and conditions.

1.1.4. The same information will be gathered from different vendors and will be used to evaluate whether NATO's requirements are aligned with market capabilities and customary terms and conditions for the type of services to be procured. The response to the RFI will also be used to improve the clauses and provisions of the eventual solicitations of offers and to identify suppliers that may be interested in participating in this business opportunity.

1.1.5. Participation in this RFI is not mandatory. Any prospective participant that declines to respond to this RFI will remain eligible to take part in the solicitations of offers stated above.

1.1.6. This RFI is issued in accordance with the procedures established in the NATO procurement regulations. A copy of these regulations is available at: https://shape.nato.int/financeandacquisition

1.2. SCOPE

1.2.1. Annex 1 provides information about the Statement of Requirement (SoR) of this RFI action, and other useful information regarding the scope of services to be provided.

2. RFI PROCEDURE

2.1. GENERAL

2.1.1. In order to submit a response to this RFI, participants must fill out Annex 6 "RFI-SH-26-01 Response Form" that has been attached to this document.

2.1.2. The responses to this RFI will be reviewed by staff from different functional areas within ACO/SHAPE, including but not limited to duly authorized representatives from the ACO Finance and Acquisition Directorate, NATO SOFCOM, and security and procurement authorities of ACO/SHAPE and NATO SOFCOM.

2.1.3. In view of the information received, participating firms may be invited to take part in information exchanges prior to the launch of any solicitation of offers. This process will allow NATO to gather additional information, clarify certain aspects of the responses, and validate the intended procurement strategy.

2.1.4. Participation in these information exchanges is not mandatory. The practical details of the sessions and topics to be discussed will be agreed in consultation with the relevant suppliers.

2.2. CONFIDENTIALITY

2.2.1. ACO/SHAPE may incorporate industry comments and responses to this RFI, in part or in whole, into the future release of a solicitation of offers for related goods and services.

2.2.2. RFI participants that include data in their responses that they do not want disclosed to the public for any purpose, or used by NATO, except for internal evaluation purposes and development of the eventual RFP, must:

2.2.3. Mark the title page with the following legend:

"This document includes data that shall not be disclosed outside NATO and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than for NATO internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit NATO's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]"; and

Mark each sheet of data it wishes to restrict with the following legend:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document."

2.3. RESPONSE TO THE RFI

2.3.1. The participants to this RFI must complete and submit Annex 6 hereto. Responses **shall not exceed 25 single-sided pages** using 12-point font and shall be UNCLASSIFED.

2.3.2. Participants are free to provide comments in whatever depth they so choose or may decline to participate in this part of the solicitation process without prejudice.

2.4. HOW TO SUBMIT THE RESPONSE

2.4.1. Responses shall be written in English and submitted by **email** no later than **17 March 2026 (1700 CET)**. *Respondents are not permitted to provide more than one response*.

The Procurement and Contracting Officer responsible for this RFI is:

Ms. Margaret BROTHERS
Email: margaret.brothers@nato.int
Senior Contracting Officer
SHAPE, Strategic Acquisition Management Section
7010 – SHAPE, Belgium

Additional POINT OF CONTACT for this RFI:

Mr. Giuseppe COL
Email: giuseppe.col@nato.int
Head, SHAPE Contract Management Section
7010 – SHAPE, Belgium

2.5. REQUESTS FOR CLARIFICATION

2.5.1. All questions about the RFI shall be sent via email to margaret.brothers@nato.int and giuseppe.col@nato.int on or before 12:00 PM Central European Summer Time (CET), Wednesday, 25 February 2026. NATO responses will be emailed no later than 1700 (CET), Wednesday, 04 March 2026.

2.6. EXTENSION OF CLOSING DATE

2.6.1. Any participant may request directly to the SHAPE Acquisition Management (AQM) Branch an extension of the RFI closing date. However, requests are to be sent via email to margaret.brothers@nato.int and giuseppe.col@nato.int no later than ten (10) calendar days before the closing date. SHAPE AQM may, at its own discretion, grant an extension of the RFI closing date.

2.7. DISCLAIMERNON-REIMBURSEMENT OF COSTS

2.7.1. This is a request for information only and your response shall not be construed as an offer. As such, this request does not constitute a solicitation, and SHAPE will not consider unsolicited proposals provided as a response to this RFI. Rather, the intent is to gather industry feedback, and all responses shall be in the form of information. This request for information does not commit SHAPE to pay any costs incurred in the preparation of any submission or any kind of participation into this RFI, or to contract for goods or services.

ANNEX 1 to RFI-SH-26-01

STATEMENT OF REQUIREMENT (SOR)

SOFCOM Strategic Mission Network

1. General Information

1.1. This Statement of Requirement (SoR) defines the objectives, scope, deliverables, governance and quality measures for the adaptation of a current Special Operations Command Europe (SOCEUR) owned service, referred to as Shadow Net for Special Operations Forces (SNS), to a NATO Special Operations Command (SOFCOM) owned Enhanced (SNS) referred to throughout the document as eSNS.

1.2. The eSNS is a secure, cloud-hosted, Software-as-a-Service (SaaS) capability designed to provide resilient communications, situational awareness, and interoperability across NATO multinational SOF and other networks.

1.3. The Service will initially support 1,500 simultaneous users, with the ability to scale in capacity and federation reach in line with operational demand.

1.4. The eSNS will operate as a fully outsourced managed service under SOFCOM authority, with the ability to transition in part or in whole to SOFCOM control as internal capabilities and resources mature.

1.5.1. This firm fixed-price Contract consists of the following:

a. One 12-month Base Year period (SOFCOM): provide baseline eSNS licenses to 1,500 users.

b. Four 12-month Option Year periods: provide continued eSNS licenses to 1,500 users.

1.5.2.During the entire period of performance of this contract (to include option periods that are exercised) individual NATO nations shall have the right to procure directly with the Contractor for additional licenses, capacity, or services through separate, bilaterally negotiated contracts at the same “Terms & Conditions” as the prospective / SOFCOM awarded contract without fragmenting governance, security, technical architecture, or pricing.

1.5.3. The Contractor shall maintain a unified technical architecture while ensuring financial and administrative separation between the SOFCOM Contract and NATO Nation Contracts.

2. STATEMENT OF OBJECTIVES

2.1. Corporate Objectives

2.1.1. The overarching NATO corporate objective is to create a Strategic Mission Network for SOFCOM referred to as eSNS, as a secure, sustainable, interoperable, service-based capability.

2.1.2. eSNS shall serve as the digital backbone of multinational SOF collaboration, enabling real-time situational awareness, mission planning, operational coordination, and data sensor integration across domains and theatres.

2.1.3. Establish an efficient and repeatable process for NATO Nations to purchase additional eSNS capabilities as their operational need dictates, see 1.5.2.

2.2. Contract Objectives

2.2.1. The objectives of this Contract are to:

a. Create a Strategic Mission Network that provides a common operational picture able to ingest/display a wide range of data streams and features, chat, video teleconference, data/video/file sharing, real time voice translation, and data lake.

b. Establish a sustainable service-based delivery model with SOFCOM defined governance and security responsibilities.

c. Implement a zero-trust architecture, mobile device management, and comply to connect technology that enables remote wipe functionality.

d. Enable federation and interoperability with systems through SOFCOM-desired accredited interfaces and include accreditation package.

e. Deliver a scalable, monitored and continuously improving service aligned with ITIL latest version best practices.

f. Facilitate SOFCOM-approved, organization-managed, non-personal, Bring-Your-Own-Device (BYOD) capability via use of automation or a QR code enrolment/provision.

g. Migrate user devices from existing Strategic Mission Networks as needed.

h. Facilitate wide array of sensor integration (i.e. Full Motion Video, Wireless signals, etc.).

2.3. Management Objectives

2.3.1. The Contractor will have the flexibility to allocate resources, expertise and subcontractors to achieve Contract objectives in accordance with defined timelines and performance standards.

2.3.2. The Contractor shall employ an agile management approach consistent with ITIL latest version and NATO BI-SC 80-92 Automated Information Systems Security (AIS) directives, ensuring effective risk, incident and configuration management. In addition, employ suitable DevSecOps model to ensure Development, Test, and Production environments are separated, and managed appropriately with separation of roles/duties

2.3.3. SOFCOM Security Officer as Designated Accreditation Authority retains ultimate authority for policy, accreditation, and strategic direction of the Service. Contractor shall submit the initial accreditation package for review and approval by the designated authority.

3. PERSONNEL AND RESOURCES

3.1 General

3.1.1. Contractor personnel requiring access to NATO facilities, networks, or classified information shall require valid NATO security clearances up to NATO Secret level, valid throughout the duration of the Contract. Members should be prepared to travel as needed, across NATO facilities and participating nation SOF headquarters as operationally required

3.2. Project Team Composition

3.2.1. The Contractor shall assign sufficient personnel to cover a 40 hour/week support in the European Time Zone, with ability to surge when needed for operational requirements to ensure timely and effective service delivery (>99.9% uptime of services).

3.2.2. Key personnel shall include:

a. Team Leader –responsible for contract performance and liaison with the SOFCOM Project Manager. The Team Leader shall maintain on-site presence at SOFCOM Headquarters

(based on 5 days per week, with the ability to surge weekends, when required by the Contracting Officer Technical Representative (COTR)).

b. Cloud Service Engineers – responsible for service performance, resilience, and optimization.

c. Security Engineers – responsible for Security Information and Event Management (SIEM) operation, monitoring, and incident response.

d. Helpdesk Operators/System Admins – responsible for user support, with surge capability to 24/7 cover within agreed timescales.

e. Federation/Interoperability/Networking Specialist – responsible for (Tactical Assault Kit (TAK), Common Operating Picture/Common Data Picture integration, cross-domain federation, and secure data exchange. Should be knowledgeable of near-real time live-video/Full Motion Video integration.

f. Training and Change Management Specialist – responsible for technical training and supporting service adoption.

g. Android/Android Press Kit Application Developer – responsible for development of new android applications for future fielding.

h. Knowledge Manager (KM)/Lessons Learned – responsible for development of Wiki type collaboration platform to share relevant eSNS information.

3.2.3 Any change to the Team Leader role shall require prior approval from the COTR.

3.3 Personnel Qualifications and Experience

3.3.1 The Team Leader shall have not less than three years' experience whereby recent experience is within the last two years, and relevant experience in managing service transition or adaptation projects of comparable scope.

3.3.2 Engineers shall demonstrate recent and relevant expertise in cloud environments, cybersecurity, and tactical communications that are consistent with industry leading standards.

3.3.3 Helpdesk operators shall demonstrate proficiency in supporting end-users across multiple platforms and connectivity types

3.3.4 All personnel shall be proficient in English, both written and spoken.

4. FURNISHED PROPERTY AND SERVICES

4.1. General

4.1.1. The SOFCOM shall provide the Contractor with access to existing service documentation, user inventories, and operational requirements necessary for adaptation.

4.2. Contractor Responsibilities

4.2.1. Except for the items stated at Paragraph 4.1.1, the Contractor shall furnish everything required to perform this Contract.

5. CONTRACTOR DELIVERABLES

5.1. General

5.1.1. The Contractor shall be responsible for executing all deliverables defined in this SoR, ensuring service continuity, adaptation, and sustainment.

5.1.2. The Contractor shall meet the Initial Operating Capability (IOC), defined as: Service Operational, accredited by SOFCOM Security Officer, and available to minimum 500 users within the first three months from Contract Effective Date.

5.1.3. The Contractor shall meet Full operating Capability (FOC) defined as the establishment of eSNS across NATO SOF with all 1,500 licenses federated and operational six months from Contract Effective Date and three months from IOC.

5.2. Contract Management

5.2.1. The Contractor shall:

a. Designate a Team Leader as the primary Point of Contact (POC).

b. Provide an initial team list within **five working days** of the **Contract Award Date**.

c. Conduct weekly checkpoint and progress meetings with the SOFCOM Project Manager.

d. Maintain a Risk Register, Issue Log, Monthly Highlight Reports, and a Lessons Learned Log.

5.3. Phase 1 – Service Transition and Adaptation

5.3.1. The Contractor shall execute the following:

a. Establish secure processes and governance under SOFCOM Contracting Authority with no loss of continuity of service.

b. Adapt identity and access management (including integration with NATO where applicable) and federation configurations (including TAK server federation, cross-domain data exchange protocols, and secure gateway configurations) to align with SOFCOM security requirements.

c. Optimize applications, performance, and monitoring.

d. Deliver readiness certification.

5.3.2. Deliverable Products for Phase 1 shall include:

a. D-1: Transition Plan – Transition tasks, timeline and handover activities.

b. D-2: Inventory Report – Comprehensive system and user inventory.

c. D-3: Service Readiness Report – Validation of operational and security readiness.

d. D-4: Governance Framework – Policy and control model for SOFCOM ownership.

e. D-5 Service Management Plan - SLAs, KPIs, reporting and escalation structure.

5.3.3. Period of Performance Milestones:

a. Phase 1 Period of Performance: 30 – 90 days from Contract Effective Date to include IOC achievement at Day 60 from Contract Effective Date.

5.4. Phase 2 – Service Operations and Sustainment

5.4.1. The Contractor shall execute the following:

a. Deliver Enterprise-level services to 1,500 users. This initial baseline is to be scalable upwards. As an estimate in the first year there is a potential requirement for additional licenses roughly estimated up to 15,000 users, to be executed nationally (by each requesting NATO Nation) under the provision in Section 1.5.2.

b. Provide secure communications (encrypted AES-256), including instant messaging/Chat, video teleconferencing, file synchronization, VoIP/RoIP, and voice translation services.

c. Operate TAK for planning, mapping, and mission coordination.

d. Deliver helpdesk and technical support (as defined at Paragraph 3.2.2).

e. Manage SIEM, firewall, Intruder Detection Systems (IDS)/ and Intruder Prevention System (IPS), Virtual Private Networks (VPNs), and Cybersecurity threat (vulnerabilities)

f. Conduct training, semi-annually, for operators, planners, and administrators.

5.4.2 Deliverable Products on a recurring basis shall include:

a. D-6: Monthly Service Reports – Performance and availability

b. D-7: Monthly Security Monitoring Reports – Security audit and incident summaries

c. D-8: Training Records per training cycle – Course delivery and attendance log

d. D-9: Expansion Deployment Plans as required – Documentation for service scale-up

e. D-10: Quarterly Lessons Learned report – Continuous improvement recommendations

5.4.3 Period of Performance Milestones:

a. Phase 2 Period of Performance: 90 days post Contract Effective Date and post-IOC through duration of contract inclusive of option years.

6. Quality Control and Product Acceptance

6.1. General

6.1.1. High standards of quality are to be maintained throughout adaptation and sustainment of the eSNS.

6.1.2. Quality control and product acceptance criteria as below and aligned with ISO 9001 and ITIL latest version.

6.2. Quality Control

6.2.1. The Contractor shall implement automated monitoring of Key Performance Indicators (KPIs) as agreed with SOFCOM management team and documented in the Service Management Plan (D-5), which must be approved prior to commencement of Phase 2 operations.

6.2.2. The Contractor shall implement automated reporting tools and submit monthly Service Quality Dashboards (with daily reports upon request).

6.3. Product Acceptance

6.3.1. All deliverables, whether documents, reports, or service outputs, shall be reviewed by the SOFCOM Project Manager within five working days of submission.

6.3.2. Acceptance or rejection of deliverables are to be confirmed in writing, based on predefined acceptance criteria established in the Contract or agreed during the transition phase.

6.3.3. If a deliverable is rejected, the Contractor shall correct deficiencies and resubmit the deliverable within a mutually agreed timeframe at no additional cost to the Contracting Authority.

6.3.4. Service performance outputs (e.g., monthly reports, monitoring data, and security event summaries) shall be subject to ongoing acceptance based on compliance with the agreed service level indicators.

6.3.5. Inspections: Review of adapted governance, administrative processes, and updated documentation for compliance with requirements.

7. Quality Assurance - Surveillance

7.1.1. The Contractor shall apply appropriate quality assurance measures (ISO 27001), to ensure that the delivery of service remains compliant with contractual requirements and operational needs.

7.1.2. During the period of this SoR the COTR will be conducting surveillance of the Contractor efforts. The Services Summary table below lists the performance objectives and performance thresholds for critical tasks in the SoR.

7.1.2.1. **Critical Tasks** are those Contractor activities whose failure would materially impact the availability, security, integrity, or continuity of the eSNS service, or would prevent SOFCOM from exercising effective governance and operational control.

For the purposes of this Contract, Critical Tasks include, but are not limited to:

- Operation and sustainment of the SOFCOM-funded baseline service, including availability, performance, and capacity management;
- Cybersecurity operations, including monitoring, incident detection, response, and remediation;
- Identity, access management, and federation services required to enable authorised user access and interoperability;
- Execution of approved service changes, configuration management, and release management in accordance with the Service Management Plan;
- Delivery of defined support services, including helpdesk operations and incident resolution within agreed response times;
- Maintenance of governance, reporting, and assurance artefacts required to support service oversight, accreditation, and performance surveillance.

Critical Tasks are defined in Sections 5.3 (Phase 1 – Service Transition and Adaptation) and 5.4 (Phase 2 – Service Operations and Sustainment) and are subject to performance monitoring and surveillance as described in Section 7.

7.1.3 The performance threshold briefly describes the minimum acceptable levels of service required for each performance objective. These thresholds are critical to mission success. The Method of Surveillance defines how the COTR will capture and monitor performance of the services. The primary method of surveillance and basis for the performance threshold for this SoR is the valid Customer Complaint and periodic COTR inspection. Examples of customer complaints include, but not limited to, issues with (examples Reports, Performance Duties and Security Management Protocol). A valid complaint is one that is consequential to the successful performance of the SoR for an issue that was not corrected in a reasonable amount of time and adversely impacted performance, schedule, and/or cost. The COTR will coordinate with the SOFCOM Management Team on all uncorrected complaints.

Performance Objective	SoR Para.	Performance Threshold	Method of Surveillance
Specific Duties	3.2.1, 5.3.1, 5.4.1, 6.2	Not more than 2 COTR validated complaints per month	Customer Complaints
Contractor Reports	5.3.1, 5.4.1, 6.2	Not more than 2 COTR validated complaints per month	Customer Complaints
Governance Framework	5.3.1	Not more than 2 COTR validated complaints per month	Customer Complaints
Service Management Plan	5.3.1	Not more than 2 COTR validated complaints per month	Customer Complaints
Training	5.4.1	Not more than 2 COTR validated complaints per month	Customer Complaints
Operation of TAK	5.4.1	Not more than 2 COTR validated complaints per month	Customer Complaints
KPI's	5.3.2 & 6.2.1	Not more than 2 COTR validated complaints per month	Customer Complaints
Contractor Security Management Protocol	5.3.1 & 5.4.1	Not more than 2 COTR validated complaints per month	Customer Complaints

7.2. Ongoing Monitoring of Service Performance

7.2.1. The Contractor shall continuously monitor eSNS performance against defined **Key Performance Indicators (KPIs)**, including availability, latency, incident response times, and user capacity. Results reported in the Monthly Service Report (D-6).

7.3. Security Monitoring and Audits

7.3.1. The Contractor shall conduct regular audits of security monitoring tools, including SIEM, intrusion detection/prevention systems, and firewall configurations. Audit findings are to be documented in the Security Monitoring Report (D-7), with corrective actions tracked to closure.

7.4. Deliverable Reviews

7.4.1. Monthly checkpoints with the COTR to review submitted deliverables, including service reports, training delivery (D-8), and expansion deployment readiness (D-9). The Project Manager shall provide written acceptance or rejection in accordance with Section 6.2.

7.5. User Satisfaction and Continuous Improvement

7.5.1. The Contractor shall capture user feedback, specifically to measure satisfaction levels, capture lessons learned and propose then implement continuous improvement initiatives. Findings and recommendations are to be captured in Lessons Learned Logs and discussed during monthly review meetings.

ANNEX 2 to RFI-SH-26-01

eSNS POLICY AND GOVERNANCE FRAMEWORK.

1. POLICY AND GOVERNANCE FRAMEWORK

1.1. Purpose

This section defines the governance and policy structure that will ensure SOFCOM retains strategic control and data sovereignty over the Service while outsourcing day-to-day operations to the Contractor.

1.2. Governance Structure

a. **Strategic Governance (SOFCOM Authority):**

– Owns policies and standards

– Establishes and Chairs a Service Governance Board (SGB);

– Approves major changes and security postures.

b. **Operational Governance (Contractor):**

– Executes daily operations under SOFCOM direction;

– Implements approved security and performance policies;

– Reports KPIs and incidents through agreed channels.

– Responsible for initial and continued monitoring of the network

c. **Collaborative Governance:**

– Monthly Joint Service Review Boards (SRBs) consisting of key Contracting Authority and Contractor personnel;

– Annual Strategic Review to re-validate SLAs and in-sourcing readiness.

2. Policy Domains

Policy Area	**Objective**	**Governance Owner**
Data Ownership & Sovereignty	All data remains NATO/SOFCOM property	SOFCOM
Access & Identity Management	Zero-Trust authentication and Role Based Access Control	Joint
Change & Configuration Control	CAB-approved changes only	Joint
Security & Incident Response	Aligned to NATO Cyber Security Incident Response Team procedures	Joint
Compliance & Audit	Periodic audits and external assurance	SOFCOM
Business Continuity	Disaster Recovery and resilience testing	Contractor (executed) / SOFCOM (approved)

Policy Area	Objective	Governance Owner
Service Transition	Progressive transfer to SOFCOM as capability matures	SOFCOM
Data Hosting/Availability	Must reside within NATO country	SOFCOM

3. Progressive In Sourcing

3.1.1. The scope of the contract will be reviewed annually, and SOFCOM reserves the right to progressively assume operational responsibilities as its internal capability develops. A cost reduction model, when necessary, will be agreed as SOFCOM assumes areas of responsibility from the Contractor, prior to the annual extension of the contract.

3.1.2. The Contractor shall support this transition through knowledge transfer, documentation and training.

3.1.3. An In-Sourcing Readiness Plan will be reviewed annually by the Service Governance Board.

4. DELIVERABLES MATRIX

Deliverable	Phase	Purpose	Owner/Reviewer
Transition Plan	1	Define handover and transition tasks - Section 5 of the SoR	SOFCOM
Governance Framework	1	Establish policy and control model	SOFCOM
Service Management Plan	1	Define SLAs, KPIs and reporting	Joint
Monthly Service Report	2	Monitor performance and availability	SOFCOM

ANNEX 3 to RFI-SH-26-01

eSNS HIGH LEVEL ARCHICTECTURE

1. System Context

1.1. eSNS provides secure, resilient, and scalable communications in order to provide SOF users with situational awareness and digital force protection.

1.2. The Service is fully cloud-hosted, employs zero-trust principles, and integrates multi-layered security functions to ensure mission assurance.

2. Users

2.1. The Service will support 1,500 active users, across all NATO SOF nations as respective tenants, at Contract start, with the ability to scale based on SOF operational requirements.

2.2. Users shall access the Service using NATO approved devices enrolled within the Mobile Device Manager.

2.3. Remote and federated users shall connect through accredited secure gateways. No additional client software beyond approved applications shall be required.

3. Interoperability

3.1. The Service shall support federation with SOF national systems through approved interoperability mechanisms. To note this is out with NATO unclassified or classified systems.

3.2. All data exchanged between federated systems will be outside NATO classification and maintain best in class commercial encryption.

3.3. Interfaces shall include:

a. Secure web services and Application Programming Interface (APIs) with control of all calls retained in the higher classification domain;

c. TAK federation for tactical data sharing between authorized nodes.

d. Secure messaging notifications generated within the Service.

e. Incorporate AdTech, Commercial Telemetry Data, or alternative Commercially Available/Publicly available information.

f. Integration of Full Motion Video, Unmanned Systems (UxS) drone footage, near real-time video feed (i.e. Compass etc).

g. Integration with Common Operating Picture/Common Intel Picture Products (i.e. Clever Shepherd, etc.)

4. Hosting and Infrastructure

4.1. The Service will deploy within public cloud tenants hosted exclusively in NATO SOF nations. Each NATO Nation will be hosted within a SOFCOM Cloud and furnished with a baseline capability.

4.2. The following zones will provide:

a. **Production Zone** – Hosting the live operational service.

b. **Reference Zone** – Hosting a reference environment for training, validation, and acceptance activities.

c. **Development Zone** – Hosting controlled environments for testing, adaptation, and sustainment.

d. **Disaster Recovery Zone** – Providing continuity and redundancy in the event of primary site failure.

e. **Storage availability** – Hot, warm, or cold (deep storage) retrieval

5. Security Functions

5.1. SIEM with continuous monitoring and alerting.

5.2. IDS/IPS.

5.3. Distributed Denial of Service (DDoS) protection and traffic scrubbing.

5.4. Multi-factor authentication (MFA) and federated identity management.

5.5. RBAC with privileged access management.

5.6. Mobile Device Management/Comply to Connect.

5.6.1. Mobile Device Management will maintain the ability to perform remote wipe functions,

and policy enforcement for end user devices.

6. Accreditation

6.1. The Contractor shall be responsible for accrediting eSNS in accordance with SOFCOM standards and requirements.

ANNEX 4 to RFI-SH-26-01

LIST OF PROCESSES AND SERVICE VOLUMES

1. General

1.1. This Annex defines the principal processes and estimated service volumes associated with eSNS.

1.2. Figures are indicative and intended to establish baseline capacity. They are not limiting, and the Contractor shall ensure scalability to meet operational demand.

1.3. Volumes are expressed on a monthly basis unless otherwise specified.

2. Operational Processes

Ref.	Process / Sub-Process Name	Approximate Volumes	Notes
OPS-01	User onboarding and account management	1,500 accounts at Contract start; ability to nationally increase based on individual NATO Nation needs will require approval of the COTR, per Section 1.5.2.	Includes creation, modification, suspension, and deactivation of user accounts.
OPS-02	TAK mission planning sessions	~100 concurrent sessions/month	Includes overlays, target management, and real-time geospatial collaboration.
OPS-03	Secure messaging transactions	~50,000/month	Encompasses individual, group, and broadcast messages across multiple domains.
OPS-04	Video Teleconferencing (VTC) sessions	~300/month	Sessions averaging 30–60 mins; up to 20 concurrent users per session.
OPS-05	VoIP calls	~10,000/month	Includes peer-to-peer and multi-party calls.
OPS-06	File transfer and synchronization	~5 TB/month	Individual files up to 2 GB; includes replication across nodes.
OPS-07	Federation data exchanges	~20 partner nodes	Secure tactical exchanges with national and coalition systems.
OPS-08	Helpdesk support requests	~300 tickets/month	Includes Level 1 triage and Level 2 technical investigation.

Ref.	Process / Sub-Process Name	Approximate Volumes	Notes
OPS-09	Security incident alerts	~100/month	Generated by SIEM/IDS requiring triage, containment, and reporting.
OPS-10	Training sessions	~20 per year	Covering end-users, administrators, and mission planners.
OPS-11	Feed/COP/analytic tools	~10Tb/month	TBD

3. Scalability

3.1. All processes shall be capable of scaling upwards of the baseline volumes without degradation of performance.

3.2. The Contractor shall provide surge capability for operational deployments and exercises and should price on 30 days per annum for exercise support, subject to notice periods agreed in the Transition Plan.

ANNEX 5 to RFI-SH-26-01

CURRENT SNS STRUCTURE AND CAPABILITY

1. General:

1.1. Within this environment, a **Mission Landing Zone** is established. This landing zone provides the shared core SNS services that underpin all national and regional operations.

2. National Nodes

2.1. Each participating nation on the current SNS network is provisioned with a **dedicated cloud-based server**, referred to as a **National Node**.

2.2. National Nodes are:

a. Self-sufficient and capable of operating independently in the event of federation disruption;
b. Isolated in design, employing a zero-trust architecture that enforces strict access and security controls;
c. Equipped with core services, including:
d. Transport Layer Security (TLS) for data in transit;
e. Android Tactical Assault Kit (ATAK) server services for situational awareness and mission collaboration.

2.3. National Nodes provide sovereign control to each nation while maintaining technical interoperability with other nodes on the network.

3. Regional Hubs

3.1. National Nodes are federated into Regional Hubs. These hubs are aligned to support NATO SOF operations, exercises, and readiness activities.

3.2. Regional Hubs provide the following functions:

a. Data compartmentalization to maintain security boundaries between missions and national contributions;
b. Rapid data synchronization via TAK protocols to ensure timely situational awareness;
c. Bandwidth economy through regional optimization of traffic flows;
d. Centralized policy management to ensure consistent standards across federated nodes;
e. Simplified configuration for administrators and engineers.

4. Central Federation

4.1 Data and services from Regional Hubs are further federated to a **centralized Special Operations Command Europe (SOCEUR) hub**.

4.2. This central hub provides:

a. Authoritative policy enforcement and service governance;
b. Consolidated monitoring and situational awareness across all nodes and regions;
c. The capability to federate with external mission environments.

5. Device Policy

5.1. SNS supports a **Bring Your Own Device (BYOD) using Comply to Connect** approach to ensure agility and broad accessibility. Device must be within the Operating System Lifespan of the OS provider (current with patches and still supported by OS provider)

5.2. To mitigate risk, BYOD is **restricted to devices hardened under SOCEUR-managed Mobile Device Management (MDM)**. This ensures compliance with security policies while preserving device and transmission agnosticism (Wi-Fi, Satellite Communications (SATCOM), Internet Service Provider (ISP), cellular, or radio transport).

6. Implications for Contractors

6.1 The current SNS architecture places specific requirements on any Contractor selected to adapt, operate, and sustain the Service. Key implications include:

a. **Service Ownership and Federation:**

The Contractor must ensure that National Nodes remain sovereign and self-sufficient, while still federating seamlessly into Regional Hubs and the central SOFCOM hub. Adaptation work must preserve zero-trust design principles and strict compartmentalization.

b. **Cloud-Based Operations:**

SNS is fully cloud hosted. The Contractor **must demonstrate** proven ability to manage Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) environments, including multi-tenant configurations, high-availability design, and continuity/disaster recovery planning.

c. **TAK-Centric Services:**

As TAK is the operational backbone of SNS, the Contractor must demonstrate extensive experience with TAK, and be able to provide assured availability, scalability, and optimization of TAK services, including ATAK server configuration, geospatial synchronization, and real-time collaboration features.

d. **BYOD and Endpoint Security:**

While SNS supports a BYOD model, all devices must be hardened under SOFCOM Mobile Device Management (MDM). The Contractor is responsible for enforcing these controls and for maintaining endpoint compliance across multinational participants.

e. **Scalability and Responsiveness:**

The architecture is designed to scale rapidly. The Contractor must be capable of expanding user capacity, creating new National Nodes, or re-establishing environments at speed in support of operational needs.

f. **Security Monitoring and Incident Response:**

The Contractor must operate continuous security monitoring, including SIEM, IDS/IPS, and threat intelligence integration, ensuring timely detection and resolution of security events across all layers of the service.

g. **Interoperability with Mission Networks:**

eSNS must federate with SEME, UTN, TTN, MME, and other mission environments. The Contractor must demonstrate capability to manage federation across domains, including the use of secure gateways, controlled data exchanges, and accredited federation mechanism.

ANNEX 6 to RFI-SH-26-01
RFI RESPONSE FORM

Participants are encouraged to fill all the fields and answer all the questions stated in this form. Participants may use attachments to expand their answers.

Company Information and Contact Details	
Company name	
Company address	
DUNS	
Tax or registration number	
Company web page	
Main products/services	
Main market/customers	
Number of years in the market	
Company location(s)	
Number of company employees	
Point of Contacts for this RFI (Name, Telephone, email address)	

Eligibility, Responsibility and Past Performance

Ref.	Questions	Answers
1	Has your company created, fielded, maintained an operational tactical mission network in large scale combat operations? Provide details of when, where and metrics on what was provided within the past 24 months.	
2	Describe the technical applications your company would use to achieve the following: 2-way and conference voice/video, video streaming of multiple feeds/sensors, Common Operating Picture (COP), Common Information Picture (CIP), file storage, knowledge management, digital force protection/wardriving, and analytics in a zero-trust environment with associated costs? Please detail your breakdown.	

Technical

Ref.	Questions	Answers
3	Has your company created, fielded, maintained an operational tactical mission network in large scale combat operations? Provide details of when, where and metrics on what was provided within the past 24 months.	
4	Describe the technical applications your company would use to achieve the following: 2-way and conference voice/video, video streaming of multiple feeds/sensors, Common Operating Picture (COP), Common Information Picture (CIP), file storage, knowledge management, digital force protection/wardriving, and analytics in a zero-trust environment with associated costs? Please detail your breakdown.	

5	Is the tech stack you described in question 2 modular, scalable, and interoperable with Modular Open Systems Approach (MOSA). Describe an example, providing specific information of automation projects performed recently and the benefits achieved through those projects.	
6	Describe how your company would provide embedded operational support and engineering support services for the defined base period of 12 months with four option periods of 12 months each. (Additional support for exercise for up to 30 days per 12-month period. With the option to increase scale as operation need dictates.) providing specific information of automation projects performed recently and the benefits achieved through those projects.	
7	Describe your company's security tech stack approach to achieve mobile device management (mobile and laptop), automated security monitoring, (Security Information and Event Management (SIEM)/ Security Orchestration, Automation and Response (SOAR), managed portal, metrics reporting tool providing specific information of automation projects performed recently and the benefits achieved through those projects.	
8	Describe how your company would integrate Business to Business (B2B) connections in support of multiple Identity Provider (IDPs) providing specific information of automation projects performed recently and the benefits achieved through those projects.	
9	Describe how your company is able to build and deploy services that support Open ID Connect (OIDC) configurations providing specific information of automation projects performed recently and the benefits achieved through those projects.	

10	Describe how your company implements cross domain solutions with the sanitization of certain data fields and populate on a Common Operating Picture (COP) at the Common User Interface (CUI) level near real time.	
11	Provide a detailed analysis of how you scaled a user base over the course of 24 months. Please include metrics. For example, if you scaled from 1,000 to 10,000 users explain how you did that. providing specific information of automation projects performed recently and the benefits achieved through those projects.	
12	Provide your opinion regarding the eligibility and responsibility criteria specified in paragraph 5.2. of Annex 1. Are these criteria aligned with the contract objectives? Should we add other conditions or adjust the criteria to maximize value and minimize risk?	

NATO Background

Ref.	Questions	Answers
13	Is your company headquartered in a NATO allied nation, and is the division of the company that can perform this work located in a NATO allied nation?	
14	Have you performed NATO contracts? If yes, please describe the work.	
15	Does your company hold a NATO facilities clearance? If so, specify the date of validity.	

16	Do you have NATO security cleared personnel to be able to comply with the security requirements of the contract? If so, specify the number, level of security classification, and project roles.	
17	Describe your experience with NATO security accreditation activities and the adoption of NATO security accredited products.	

Performance Requirements and Project Approach

Ref.	Questions	Answers
18	Describe how your company would meet the requirements specified in Section 5. Contractor Tasks of the Statement of Requirement under each one of the sub-sections below. In your response, please, identify clearly those areas of work or tasks that you will not be able to perform and any limitations regarding functional scope (e.g., if you will focus on the optimisation of treasury management activities only). Also, identify specific subcontractors and software products that would be used for the performance of the relevant work area.	
19	Please provide a high-level timeline for the execution of all the phases of the project and express your opinion on whether the target period of performance (12-month base with four 12-month option periods) is realistic and sufficient for the performance of the contract and the achievement of the contract objectives. Suggest an alternative duration and project timeline if appropriate.	

Contract Type, Duration, Terms and Conditions

Ref.	Questions	Answers
20	Do you have any comments or suggestions regarding the proposed contract structure, type and duration that will help increasing best-value to ACO?	
21	Please provide the terms and conditions applicable to developing a Strategic Mission Network for SOFCOM that would be provided under the prospective contract and clarify whether this would be provided as a service or as a product with embedded services.	
22	Please identify any specific terms and conditions that you find unreasonable or that will be too onerous for the performance of the contract. Propose alternative wording in order to make contract terms and conditions less onerous and more conducive to a best-value contract outcome for both parties.	

Price and Cost Information

Ref.	Questions	Answers
23	Please provide a rough price estimate for the contract period of performance (60 months total): Base period - 12 months Option Year 1 - 12 months Option Year 2 - 12 months Option Year 3 - 12 months Option Year 4 - 12 months	

24	Can you offer firm fixed-priced contracts? Would you be able to offer a more advantageous price if some or all periods of performance were structured as a cost-plus-fixed-fee?	

Additional Information and Suggestions

Ref.	Questions	Answers
25	Specify any additional information that is not provided in the RFI and that you would need in the eventual RFP for you to be able to submit a best-value proposal.	
26	Please, make any other suggestions for improvement of the procurement action or to contribute more effectively to the objectives sought by SOFCOM. Provide sufficient details so the suggestion can be properly assessed and integrated into the formal procurement strategy.	
27	Propose any other changes and adjustments, not covered by the sections above, which could be incorporated into the RFP or the intended acquisition approach to obtain best-value for SOFCOM.	