NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Kalnciema Street 11B, Rīga, LV-1048, Phone: +371 67335467
e-mail: info@stratcomcoe.org

INVITATION TO TENDER

FOR PROCUREMENT OF MICROSOFT 365 AND COPILOT LICENSES WITH ASSOCIATED MIGRATION, IMPLEMENTATION AND TRAINING SERVICES

To be supplied to the NATO Strategic Communications Centre of Excellence (NATO StratCom COE)

Revision	Version 1
Release Date	**March 30, 2026**
Issuer	Mr Edgars Sulcs
Suppliers Response date	**May 7, 2026** submitted via e-mail tender@stratcomcoe.org by 23:59 hrs (Eastern European Time zone: UTC +02:00).

Invitation to Tender for the procurement of Microsoft 365 and Copilot licenses with associated Migration, Implementation and Training services

You are kindly invited to submit proposal to provide Microsoft 365 and Copilot licenses with associated Migration, Implementation and Training services.

By participating in this procurement, you are indicating your acceptance to be bound by the guidelines set out in this letter.

To simplify exchange of information regarding this Invitation to Tender (ITT) please nominate a Bid Manager and relevant contact details of phone and e-mail address.

Please direct any questions regarding the ITT content or process to Edgars Sulcs. You should not contact other NATO StratCom COE personnel unless asked to do so by the appointed NATO StratCom COE representative.

All questions should be submitted in writing to the e-mail: edgars.sulcs@stratcomcoe.org

The NATO StratCom COE makes no obligations in any way to:

1. pay any service provider for an ITT response;
2. award the contract with the lowest price proposal or any service provider; or
3. accept any ITT information received from service providers; or
4. include service providers responding to this ITT, in any future invitations; or
5. any other commitment to service providers whatsoever.

Looking forward to receiving your response.

Yours sincerely,

Edgars Sulcs
CIS Specialist
Framework Nation Support Branch
E-mail address: edgars.sulcs@stratcomcoe.org

Whilst due care and attention have been exercised in the preparation of this document, it remains subject to the conclusion of a contract. All warranties, whether express or implied by statute, law or otherwise, are hereby disclaimed and excluded.

These limitations are not intended to restrict continued discussions between NATO StratCom COE and potential suppliers.

Any proposal submitted to NATO StratCom COE shall be considered subject to the successful conclusion of a contract between NATO StratCom COE and the selected supplier.

Table of Contents

1. **Introduction**
2. **Background**
3. **Requirements**
4. **Tender Submission**
5. **Timetable**
6. **Respondent Instructions**
7. **Tender Assessments**
8. **Decision Announcement to Participants**
9. **Contract Details**

1. Introduction

1.1. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), based in Riga, Latvia, contributes to the improved strategic communications (StratCom) capabilities within the Alliance and Allied nations. The NATO StratCom COE designs programmes to advance StratCom doctrine development and harmonization, conducts research and experimentation to find practical solutions to existing challenges, identifies lessons from applied StratCom during operations, and enhances training and education efforts and interoperability.

1.2. The NATO StratCom COE is conducting a procurement for Microsoft 365 and Copilot licenses, together with associated migration, implementation and training services, to support and enhance its digital workplace environment. The solution shall enable secure collaboration, communication and information management across the organization, while ensuring proper deployment, configuration and user adoption of the Microsoft 365 ecosystem.

2. Background

NATO StratCom COE has been strengthening its digital workplace and AI capabilities to enhance productivity, collaboration and data-driven decision-making. As the use of modern digital tools and artificial intelligence solutions continues to grow, the NATO StratCom COE seeks to further develop its internal capabilities through the implementation of Microsoft 365 and Microsoft Copilot services.

3. Requirements

3.1. Overall requirement

The Service provider shall be responsible for the licensing, base configuration, identity consolidation, and data migration to the Microsoft 365 ecosystem. Please note that the implementation and migration phase is an upfront, standalone project that must be completed at the beginning of the engagement. Post-implementation managed services and ongoing support are explicitly out of scope. The Service Provider shall complete the implementation and migration within a maximum period of 6 months from contract signature.

3.2. Licensing Requirements

3.2.1. The contract resulting from this procurement shall be concluded for an initial period of **5 (five) years**, with the possibility to extend the contract for an additional period of up to **3 (three) years**, subject to the needs of NATO StratCom COE and the availability of budget.

3.2.2. Following the initial one-year term, NATO StratCom COE reserves the right to review license pricing prior to each annual renewal. Any price adjustments for subsequent renewals must be verified against and strictly align with the official pricing published on the Microsoft website.

3.2.3. Microsoft 365 E7 (which natively includes Copilot, Agent 365, and the full Entra Suite), required in conjunction with Microsoft Teams:

3.2.3.1. Estimated Initial Quantity: 50 (fifty) user licenses;

3.2.3.2. Short-term Licenses: Up to 10 (ten) additional short-term M365 Business Premium licenses as needed.

Note! The number of licenses to be purchased is not fixed and may vary both prior to contract signing and during the contract period to reflect actual business needs.

3.2.4. The contract must must provide a flexible licensing model that allows for an annual license count fluctuation of **±20%** from the estimated initial quantity (i.e., scaling down to 40 or up to 60 M365 E7 licenses) at any time without incurring financial penalties, early termination fees or requiring contract renegotiation.

3.2.5. Cloud Solution Provider (CSP) annual commitment with monthly billing.

3.3. Identity Consolidation

3.3.1. NATO StratCom COE currently utilizes three (3) separate on-premises Active Directory (AD) environments (managing stationary workstations, laptops, and email independently).

3.3.1.1. The Service provider must architect and execute an identity consolidation strategy to merge these three separate directories into a single, unified identity managed via Microsoft Entra ID. However, the configuration must ensure that stationary computers and laptops remain grouped separately, allowing for distinct user privileges, security policies, and access controls to be applied based on the device type and user or system role.

3.3.1.2. End-users must have a single set of credentials for their stationary workstation, laptop, and Microsoft 365 ecosystem.

3.4. Data Migration Scope

3.4.1. The service provider must execute a secure data migration from the existing on-premises infrastructure to the new Microsoft 365 tenant. The newly provisioned Microsoft 365 ecosystem tenant must be located within Europe. The Service Provider shall define a rollback and contingency plan prior to migration execution.

3.4.1.1. Email Migration: Migrate approximately 250–300 GB of total email data (across the 50 users) from an existing on-premises Microsoft Exchange Server to Exchange Online. Note: The specific version of Exchange will be disclosed to the winning bidder; service providers should price the migration based on standard industry tooling and contingencies. E-mail migrations strategies shall be reviewed and approved by the NATO StratCom COE.

3.4.1.2. File Server Migration: Perform a direct “lift and shift" migration of approximately 1 TB of data from a local file server to a newly provisioned SharePoint Online / OneDrive for Business environment.

3.4.1.3. Permissions Handover: The service provider is not responsible for complex SharePoint architecture or translating legacy NTFS permissions. NATO StratCom COE’s internal IT team will manage detailed folder permissioning and Access Control Lists (ACLs) post-migration themselves, following the instructions and guidance provided by the service provider.

3.4.2. As part of the implementation, the Service Provider must design and document a Backup and Disaster Recovery strategy utilizing the native capabilities included in the procured Microsoft 365 licenses.

3.5. Implementation and Security Base Configuration

3.5.1. The service provider is responsible for the foundational security configuration required to safely deploy M365 E7 and Copilot:

3.5.1.1. Data Loss Prevention (DLP): As a basic and mandatory requirement, the service provider must configure the foundational policies and base setup for Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender to protect sensitive organizational data and secure the environment against threats.

3.5.1.2. Security Tooling: Configure base policies for the Agent 365 security dashboard.

3.5.1.3. Oversharing Diagnostic: Prior to the organization-wide activation of Copilot, the service provider must run a comprehensive diagnostic to identify oversharing risks and expose legacy permission vulnerabilities.

3.5.1.4. Remediation: The service provider will provide this diagnostic report to NATO StratCom COE’s internal IT team. The internal IT team will be responsible for executing the actual remediation and fixing permissions before enabling Copilot.

3.6. User Acceptance Testing (UAT)

3.6.1. Prior to the full organization cutover, the Service Provider must execute a pilot migration for a small subset of users (e.g., 3 internal IT staff) to validate the data transfer process, identity consolidation, and login experience.

3.6.2. Following the full migration, a formal UAT period of at least 10 (ten) working days must be provisioned. During this time, NATO StratCom COE will validate the system against the predefined success criteria. The Service Provider must be on standby for priority incident resolution during this phase.

3.6.3. The migration and implementation will be successful and eligible for final project sign-off and milestone payment, when the following criteria are met and verified:

3.6.3.1. Data Integrity: 100% of the in-scope data is migrated to the Microsoft 365 tenant with no reported data loss or corruption, verifiable via migration batch logs.

3.6.3.2. Identity Resolution: End-users can successfully authenticate into stationary workstations, laptops, and the Microsoft 365 web/desktop applications using a single, unified set of Entra ID credentials.

3.6.3.3. Security Baseline Validation: Microsoft Defender and Purview DLP foundational policies are active, and the post-migration oversharing diagnostic confirms that legacy permission vulnerabilities have been identified and handed over to the internal IT team.

3.6.3.4. Knowledge Transfer: The mandatory 6-hour end-user training and the technical IT handover sessions have been completed.

3.6.4. In case the acceptance criteria are not met, the Service Provider shall remedy the deficiencies at no additional cost within an agreed timeframe.

3.7. Training and handover

3.7.1. End-User Training: A comprehensive six (6) hour training program (in-person or virtually) for NATO StratCom COE staff, introducing the new Microsoft 365 ecosystem, single sign-on experience, and practical Copilot functionalities to ensure effective adoption.

3.7.2. Technical IT Handover: A focused, technical handover sessions for NATO StratCom COE internal IT team. This session must cover the new Entra ID identity architecture, the M365 admin center baseline configuration, and a walkthrough of the dashboards so the internal team can take full ownership of the environment.

3.7.3. The Service Provider shall provide high-level technical documentation covering the newly deployed architecture and core configurations.

4. Tender Submission

4.1. To be considered for this procurement, service providers must submit a comprehensive proposal covering three main parts (Technical Delivery, Budget, and Administrative details). There must be only one proposal. The proposal must be provided strictly in the following order:

4.1.1. A written proposal (around 5-7 pages) describing the delivery of the system and how the service provider meets all requirements listed in Section 3 (Requirements).

4.1.2. A total budget for the full proposal and a budget breakdown, in EUR (with VAT and without VAT; other tax must be clearly specified for each budget position, marked as zero where not applicable). The budget should include milestones for suggested payments and must provide specific budget breakdowns for: a) Licenses b) Implementation c) Training d) Full Total Price.

4.1.3. A copy of the service provider's Certificate issued by the national Commercial Register or a national Register covering other types of legal entity (for example, civil society organizations), indicating the country of registration. If this is not applicable (for example, if the service provider is an individual), please provide an explanatory statement and an alternative document confirming your identity, also specifying the country in which the service provider operates.

4.1.4. Information regarding persons or entities that the service provider may choose to sub-contract for work on the Contract delivery (company or person's name, other relevant credentials, e.g. company registration number, website address, contacts, etc., and a short company profile or person's biography).

5. Timetable

General	
Deadline for submission	**23:59 hrs (Eastern European Time zone: UTC +02:00) on May 7, 2026**
Contract implementation date	Upon agreement
Questions	Questions arising from this document should be given to Edgars Sulcs until April 29, 2026
Full contact details	Edgars Sulcs, Kalnciema iela 11B, Riga LV-1048, email: edgars.sulcs@stratcomcoe.org

6. Respondent Instructions

6.1. A written proposal is required that complies with the indicated requirements (see Section 4. Tender Submission). The proposal should be submitted electronically using an official email of the entity, in PDF format.

6.2. The file(s) should be submitted only to: tender@stratcomcoe.org by 23:59 hrs (Eastern European Time zone: UTC +02:00) **on May 7, 2026**.

6.3. Submissions received after the deadline will not be considered. Proposals must be submitted exclusively to the designated submission address. Any proposal sent to a different address will not be accepted or taken into consideration.

6.4. The service provider is expected to supply the required information or state clearly any reason for being unable to do so.

6.5. Any assumptions used in preparing responses should be clearly stated. Any appropriate supporting documents (brochures, presentations) should be included.

6.6. If any of the requirements specified in Section 3 (Requirements) are not met, or if any of the requested documents in Section 4 (Tender Submission) are not submitted, the Contract Award Committee reserves the right to exclude the service provider from further participation in the procurement.

6.7. The Contract Award Committee reserves the right to reject any proposal that is considered abnormally low, including in cases where the service provider fails to provide a satisfactory justification for the proposed price upon request.

6.8. Prior to the conclusion of the contract, the potential service provider and all personnel assigned to the execution of the contract shall be subject to a security background check conducted by the competent National Security Authorities. A negative assessment shall result in the exclusion of the service provider from the procurement procedure.

6.9. Questions relating to clarification of the ITT will only be accepted in writing to NATO StratCom COE representative. Likewise, all responses from the NATO StratCom COE will be written and may also be made available to other service providers (subject to confidentiality). The NATO StratCom COE will attempt to answer any questions within two working days of receipt of that request; otherwise, it will respond within that timescale notifying the service provider of the estimated time to obtain the information.

6.10. The NATO StratCom COE reserves the right to modify the provisions of this ITT at any time prior to the scheduled date for written responses. Additional scope and requirements can be added. Notification of such changes will be provided to all service providers.

6.11. Should the service provider wish to propose a deviation from the specification please ensure that you clearly identify and highlight where appropriate in your response.

6.12. All information supplied in this tender to date; any further information supplied during the tender process will remain confidential and available only to the Contract Award Committee members.

7. Tender Assessments

7.1. Evaluation Criteria and Process. A set of evaluation criteria has been prepared by the NATO StratCom COE for the evaluation of every submission. At each stage an initial evaluation will consider whether or not every instruction and requirement contained within the ITT has been fulfilled.

7.2. Evaluation criteria are based on "best value", an objective assessment by the Contract Awarding Committee as to who offers the best combination of price and service:

7.2.1. Cost.

7.2.2. Level of compliance with the Requirements and Tender submission of the ITT.

7.2.3. Quality of service provision (based on the proposal).

7.2.4. The service provider is reminded that, throughout the process, the NATO StratCom COE will continuously assess all interactions with the service provider's organisation, including compliance with the prescribed procedures. The NATO StratCom COE reserves the right, at its sole discretion, to disqualify without further consideration any submission that fails to meet basic requirements.

7.3. The NATO StratCom COE reserves the right to modify the scope of this tender, after receiving the bids to include price estimates.

8. Decision Announcement to Participants

The NATO StratCom COE reserves the right to control the format and content of any such briefing, and to limit it in any way believed by the NATO StratCom COE to be appropriate (which includes, in exceptional circumstances, the right to refuse a briefing without giving any reasons for doing so).

9. Contract Details

Contractual and payment details are subject to negotiation with the selected service provider.