

**NCIA Pre-competitive Engagement Calling Notice -
Request for Information (RFI)**



**UNIFIED COMMUNICATIONS AND COLLABORATION
SOLUTION**

RFI-CO-424402-UCC

NCIA Pre-competitive Engagement Calling Notice - Request for Information (RFI) Unified Communications and Collaboration Solution

To: **Industry Partners**

1. The NATO Communications and Information Agency (NCIA) is conducting pre-competitive market engagement as market research to gather input on potential solutions to support the upcoming acquisition for the transition of NATO Enterprise voice, video teleconferencing and messaging services to an integrated Unified Communications and Collaboration (UCC) capability. To that end, NATO is issuing the attached Request for Information (RFI) RFI-CO-424402-UCC and holding a dedicated workshop at NATO Edge to solicit feedback from capable and interested industry partners.
2. This Calling Notice RFI is issued for planning purposes only and is not a request for bids. It is part of NCIA's effort to engage early to inform and ensure it has a clear understanding of the marketplace, available capabilities, and potential acquisition strategies.
3. We value your insight and invite you to review and comment on our draft high level problem statement (Annexes A and B) with a view to providing recommendations for improving performance outcomes, competition, and efficiency; and identifying any risks or concerns that should be considered during planning.
4. Feedback can be provided in writing in accordance with submission instructions and/or by attending a dedicated industry engagement [**Unified Communications and Collaboration Solution** Workshop at NATO Edge, taking place on 17-19 November in Izmir (Türkiye), where NCIA will respond to clarifying questions and invite comments from participants.
5. Submission instructions and additional details can be found in the enclosure to this RFI.
6. Only companies from a NATO member country can participate in or respond to this RFI (https://www.nato.int/cps/en/natohq/nato_countries.htm) or attend a dedicated workshop.
7. Should you have any questions or need clarification, please contact Lise Vieux-Rochat at CO-424402-UCC@ncia.nato.int
8. We thank you in advance for your time and input, and we look forward to engaging with you as we shape this potential acquisition.

For the Chief of Acquisition:

On behalf of Lise Vieux-Rochat
Senior Contracting Officer

Anamaria
Pascaru



Digitally signed by Anamaria
Pascaru
Date: 2026.10.22 13:54:51 +02'00'

Enclosure:

- Request for Information with Annexes A (Requested Information) and B (Problem statement)
- Distribution List

Distribution List

1. NATO Delegation (Attn: Infrastructure Adviser)

- | | | |
|-------------|---------------------|--------------------|
| 1. Albania | 12. Greece | 23. Poland |
| 2. Belgium | 13. Hungary | 24. Portugal |
| 3. Bulgaria | 14. Iceland | 25. Romania |
| 4. Canada | 15. Italy | 26. Slovakia |
| 5. Croatia | 16. Latvia | 27. Slovenia |
| 6. Czechia | 17. Lithuania | 28. Spain |
| 7. Denmark | 18. Luxembourg | 29. Sweden |
| 8. Estonia | 19. Montenegro | 30. Türkiye |
| 9. Finland | 20. Netherlands | 31. United Kingdom |
| 10. France | 21. North Macedonia | 32. United States |
| 11. Germany | 22. Norway | |

2. All NATEXs
3. SACT CAPDEV
4. ACO J6
5. CDT

Table of Contents

REQUEST FOR INFORMATION	5
1. Introduction	5
2. Submission Instructions.....	5
3. Industry Engagement.....	5
4. Disclaimer	6
5. Use of Information Provided through Responses	6
6. RFI Point of Contact.....	6
Annex A – Requested Information.....	7
Annex B – Problem statement	9
Annex C – Supplement to Problem Statement – Objectives and Key Success Criteria	12
Annex D - Supplement to Problem Statement - Network Environment for UCC Deployment	13
Annex E - Supplement to Problem Statement – NATO Service Ownership and Operating Models.....	14

REQUEST FOR INFORMATION

1. Introduction

1.1 NCIA is conducting pre-competitive market engagement as market research to gather input on potential solutions to support the upcoming acquisition for the transition of NATO Enterprise voice, video teleconferencing and messaging services to an integrated Unified Communications and Collaboration (UCC) capability. The scope includes implementation, enterprise integration, migration, and ongoing service support. To that end, we are issuing the attached Request for Information (RFI) RFI-CO-424402-UCC and holding a dedicated workshop at NATO Edge to solicit feedback from capable and interested industry partners.

1.2. This Calling Notice RFI is issued for planning purposes only and is not a request for bids. It is part of NCIA's effort to engage early to inform and ensure it has a clear understanding of the marketplace, available capabilities, and potential acquisition strategies.

2. Submission Instructions

2.1. Interested parties are invited to respond in accordance with the instructions below or provide feedback during Industry Engagement:

2.1.1. Submit responses via the email address CO-424402-UCC@ncia.nato.int (see para 6.) no later than **12:00 hours Central European Time (CET) on 03 December 2026**.

2.1.2. Responses should be submitted in PDF or Word format and must not exceed **15 pages**, including:

2.1.3. Responses to [Annex A](#) and comments on [Annex B](#) excluding:

- i. Cover page
- ii. Company brochures or product literature (if included)
- iii. Attachments such as past performance references

2.1.4. Use the following subject line for submission

- i. "Response to RFI [RFI-CO-424402-UCC]– [Company Name]"

2.1.5. All responses should address the items listed in [Annex A](#) – Requested Information.

2.1.6. Respondents are also encouraged to review, consider and where needed comment on Annex A through E.

3. Industry Engagement

3.1. Planned industry engagement will take place in the form of **Unified Communications and Collaboration Solution** Workshop at NATO Edge, taking place on 17-19 November in Izmir (Türkiye).

- 3.2. During the workshop NCIA will brief the high-level problem statement and, respond to clarifying questions and invite comments from participants, based on the questions shared (Annex 1) in the open forum as well as in bilateral meetings (schedule allowing).
- 3.3. More information on NATO Edge attendance and registration is available on event's official website - <https://www.natoedge.nato.int/> .

4. Disclaimer

- 4.1. This RFI is for planning and informational purposes only and shall not be construed as a solicitation or obligation on the part of the NCIA. NCIA does not intend to award a contract based on responses to this RFI. Respondents are solely responsible for all costs incurred in responding to this RFI. NCIA will consider and analyse all information received from this RFI and may use these findings to develop a future solicitation. The NCIA will consider all responses as confidential commercial information and will protect it as such.
- 4.2. NCIA reserves the right, at any time, to cancel this informal market survey, partially or in its entirety. No legal liability on the part of NCIA for payment of any sort shall arise and in no event will a cause of action lie with any prospective participant for the recovery of any costs incurred in connection with the preparation of documentation or participation in response hereto. All effort initiated or undertaken by prospective informal market survey participants shall be done considering and accepting this fact.

5. Use of Information Provided through Responses

5.1. Confidentiality of Responses

- 5.2. The NCIA may incorporate industry comments and responses, in part or in whole, into a future release of a solicitation. Should respondents include proprietary data in their responses that they do not wish to be disclosed to the public for any purpose, or used by NCIA (except for internal evaluation purposes), they must:

a. 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 NCIA internal evaluation purposes, unless otherwise expressly authorised by [insert company name]. This restriction does not limit the NCIA's right to use information contained in this data without restriction if it is obtained from another source. The data subject to this restriction are contained in sheets [insert numbers or other identification of sheets]

b. 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.

6. RFI Point of Contact

- 6.1. Lise Vieux-Rochat
- 6.2. CO-424402-UCC@ncia.nato.int .

Annex A – Requested Information

1. Respondents are encouraged to provide the following information in their response:

a. Company Information

- i. Legal Business Name
- ii. Address
- iii. Website
- iv. Primary Point of Contact
- v. Email address

b. Technical Capability

- i. Summary of relevant capabilities and past performance

c. Feedback and Recommendations

- i. Responses to the following RFI Questions
 1. Are we defining the right problem?
 2. Does the distinction between formal and informal collaboration solutions still make sense today?
 3. What UCC features and functionality do your products offer today, and what will be operational in 2-3 years?
 4. How would you migrate without disrupting current operations?
 5. What deployment and service model would you employ?
 6. How would essential communications continue when something fails?
 7. How would recording, information governance, and AI features work?
 8. How would you meet NATO's security requirements¹, and what is your experience with similar work?
 9. What drives your costs and schedule?
 10. What should we prove before scaling across the enterprise?
 11. What are we not asking or considering?
 12. What would do you foresee to be your challenges delivering on this scale?

¹ AC/35-D/2004-REV4, SECURITY COMMITTEE Primary Directive on CIS Security, 11 Nov.2024
https://newreccen.nr.ncia/RECCEN_Store_13/NCIARECCEN-1760597978-40600.pdf

- ii. Innovations or alternatives
- iii. Comments on the draft Problem Statement

d. Questions or Concerns

- i. Risks, concerns, or barriers
- ii. Suggestions for risk mitigation or enhancing competition

Annex B – Problem statement

Note: This is a DRAFT and subject to change. NCIA is seeking industry feedback.

1. Background

1.1. Formal collaboration capabilities are foundational to NATO Enterprise operations and planning, consultation, and coordination with internal and external parties. Over time, these services have expanded organically in response to evolving business needs, technology availability, and localized solution decisions – currently serving an enterprise of ~29,000 users, 750 meeting rooms, and 80,000 endpoints across around 57 entities. As a result, multiple independently implemented tools supporting Voice, Video, Instant Messaging, Presence, and Conferencing are deployed on aging or end-of-life infrastructure.

1.2. NCIA is evaluating a transition from these fragmented services to an integrated UCC capability. The project is part of the broader modernization of NATO Enterprise core digital workplace, and must align and integrate with these initiatives.²

2. The Problem

2.1. NCIA's fragmented and ageing collaboration capability causes several major issues:

2.1.1. Poor user experiences due to inconsistent functionality and usability across different platforms;

2.1.2. Complex and costly operations and service support, with limited visibility of service performance;

2.1.3. Limited integration between tools, constraining collaboration and workflows;

2.2. In parallel, the Alliance has established strategic directives that emphasize cloud adoption, scalability, innovation and industry partnerships. The current communications and collaboration environment is not fully aligned with these directives, relying heavily on bespoke, on-premises solutions.

3. The Vision

3.1. NATO users across the Enterprise will enjoy a powerful, modern collaboration and communication solution to call, meet, message, and share information, with coherent features and functionality across all content classifications and security domains. Service teams will efficiently and effectively support, secure, upgrade and expand this solution over time.

4. The Ask

4.1. Help NCIA make this transition while keeping operational services available and respecting the constraints of separate security environments.

² In particular the NATO Transatlantic Warfighting Cloud (NTWC), Protected Business Network (PBN), and Operational Network Extension (ON-X) initiatives. These will deliver informal collaboration solutions but do not cover formal collaboration solution. See Annex D for more details.

4.2. We are seeking partners that know how to:

- 4.2.1. Stand up and run a new UCC solution in parallel to existing infrastructure, to allow smooth transition;
- 4.2.2. Provide a consistent experience across supported devices and locations;
- 4.2.3. Work within the technical and security constraints of each environment;
- 4.2.4. Keep essential communications available during outages;
- 4.2.5. Integrate with enterprise services and approved external partners;
- 4.2.6. Reuse suitable assets rather than replace them by default; and
- 4.2.7. Establish clear service ownership, predictable costs, predictable lifecycles, and workable exit arrangements.

5. The Scope

5.1. **Core UCC Capabilities:**

The capability will deliver five (5) high-level requirements:

- 5.1.1. **UCC Foundation:** Core voice, video, messaging, presence, identity-linked contact discovery, and external collaboration capabilities that provide the foundation for the UCC user experience.
- 5.1.2. **Meetings:** Real-time collaboration for scheduled and formal consultation meetings, including high-quality audio and video conferencing, screen sharing, chat, recording, breakout sessions, and participant management.
- 5.1.3. **Digital Learning:** Hybrid and virtual learning, including instructor-led training, interactive classrooms, learner engagement tools, session recording, and attendance tracking.
- 5.1.4. **Digital Events:** Large-scale virtual events, including webinars, town halls, broadcasts, moderated sessions, registration, audience interaction, questions and answers, polling, event registration, analytics and event production.
- 5.1.5. **B2B/B2C Federation:** Secure federation and interoperability between enterprise organizations, together with controlled access to enterprise UCC services for eligible third-party users.

5.2. **Artificial Intelligence (AI)-Enabled Functions:**

5.2.1. NATO's strategic position is that AI will be treated as a feature integrated into all Enterprise ICT Services, and will not be standalone offerings. That said, AI functions must operate within enterprise controls for security, privacy, compliance, observability, and responsible AI use. A distinction between **available functionality, configurable security controls, and evidence supporting accreditation** would be greatly appreciated.

5.3. **Endpoint Interoperability:**

5.3.1 Respondents should address interoperability with existing standards-based endpoints and conferencing infrastructure, where such equipment is non-obsolete. NCIA also requests information about endpoint lifecycle modernization options, including Device-as-a-Service subscription models, hardware leasing, and trade-in and buy-back programs. These options will need to meet applicable NATO security, asset

management, and disposal requirements.

5.4 Security and Enterprise Integration:

5.4.1 All UCC services are expected to conform to a Zero-Trust security approach, complemented by a Data-Centric Security model that applies protection to individual data objects rather than relying solely on infrastructure boundaries.

5.4.2 The service will need to integrate with enterprise identity, directories, public-key infrastructure, calendaring, service management, and security monitoring.

5.4.3 Importantly, an integrated UCC capability **does not imply a single shared infrastructure** across security environments. Respondents should explain how a coherent user experience and support model could be delivered through appropriately segregated deployments, identifying which functions, integrations, and management capabilities are available in each environment. Dependencies on external connectivity, cloud services, or shared control planes should be explicitly identified.

5.5 Migration and Transition:

5.5.1 The scope is expected to include discovery, detailed design, site-readiness assessment, integration, pilots, phased migration, testing, training, and adoption support. Migration plans should provide for coexistence and rollback. Legacy services should be retired only after the replacement has been tested and accepted as ready for operational use.

5.6. Operating and Support Responsibilities:

5.6.1. Respondents should have a vision for an end-to-end operating and support model, identifying responsibilities across NCIA, participating organisations, suppliers, and third parties. This should cover service monitoring, incident and problem management, configuration and asset management, security updates, release testing, endpoint and room maintenance, spares and replacement arrangements, documentation, training, and knowledge transfer.

5.6.2. NCIA is and will remain bound by specific service level agreements targets (see Annex E), which any partner would be expected to uphold. NCIA is also open to new key performance indicators, especially those that measure customer/end-user satisfaction, service quality and Digital Employee Experience (DEX), and resilience.

5.7. Resilience and Recovery:

5.7.1. NATO's work requires resilient service provision, and the UCC solution will be expected to handle a range of degradations (e.g. loss of wide-area or external connectivity, hosting, identity, or central management/licensing services). Demonstrated failover, fallback, and recovery planning will be essential.

6. Dependencies and Out-of-Scope:

6.1. Broader enterprise cloud platforms, backbone transport, and mission-network connectivity are not assumed to be part of this UCC acquisition. However, NCIA welcomes information about necessary integrations, site readiness, and infrastructure requirements that would be essential to meeting the UCC vision.

6.2. Public telephony, external federation, guest access, and mobile or remote access apply only where authorized for the relevant environment. Cross-classification information transfer is not assumed to be in scope.

Annex C – Supplement to Problem Statement – Objectives and Key Success Criteria

1. **Successful delivery and migration.** The UCC platform is fully operational and compliant with the approved Target Architecture. All priority users, services, and workloads are migrated without material business disruption;
2. **Better collaboration and adoption.** Authorized users collaborate within and across agencies without unnecessary tool switching. Agreed adoption and service utilization targets are met;
3. **Reliable services.** Essential communications remain available during defined failures, recovery is tested, and operational KPIs and service quality thresholds are sustained;
4. **Validated security.** Security and Zero-Trust controls operate across all services, users, devices, and workloads. Access, audit, and information-handling controls meet accreditation requirements, with verified multi-tenant segregation and policy enforcement across organizational and community domains;
5. **Effective integration and automation.** Enterprise systems and approved external networks interoperate, with stable AI-enabled services and automation;
6. **Controlled legacy retirement.** Obsolete platforms and duplicated infrastructure are decommissioned without adverse operational impact;
7. **Scalability and lifecycle value.** Services accommodate changing demand, new endpoints, and future capabilities, with manageable costs and clear pricing, operating responsibilities, supplier dependencies, and exit arrangements;
8. **Operational readiness.** Service management, SLA monitoring and adherence, and incident management are fully functioning. Users, administrators, and support teams are prepared before production and throughout incremental improvements, supporting long-term steady-state operations.

Specific performance targets and acceptance thresholds will be established through requirements validation, informed by industry feedback.

Annex D - Supplement to Problem Statement - Network Environment for UCC Deployment

1. *What is the Protected Business Network (PBN)?*

The Protected Business Network (PBN) is intended to provide a common, secure network and cloud environment across the NATO Enterprise. It combines a multi-cloud operating model with standardized engineering practices to simplify the delivery and maintenance of digital services.

The planned scope includes a **baseline NATO RESTRICTED digital workplace, including informal collaboration services** for everyday communication and teamwork. The UCC capability should integrate with this baseline, identifying opportunities for reuse and any additional services needed.

2. *What is the Operational Network and Extension (ON-X)?*

The Operational Network and Extension (ON-X) is intended to bring existing NATO SECRET environments into a more integrated, scalable platform, improving interoperability and service management. It uses air-gapped cloud infrastructure to host and process information up to NATO SECRET and deliver secure enterprise services.

The planned scope includes a **baseline NATO SECRET digital workplace, including informal collaboration services**, operating within the environment's security and accreditation constraints. UCC should integrate with this baseline while identifying any functional, management, or support limitations specific to the classified environment.

3. *What is the Transatlantic Warfighting Cloud (TWC)?*

The Transatlantic Warfighting Cloud (TWC) is a NATO Enterprise initiative, driven by Allied Command Transformation (ACT) together with NCIA, the Cyber and Digital Transformation (CDT) Division and SHAPE, to bring both unclassified and classified information **up to NATO SECRET** into secure cloud environments. It aims to give the Alliance a shared operational advantage by making data and AI-enabled tools available to support faster, better-informed decision-making, from headquarters down to the tactical edge. More than an IT upgrade, the TWC is intended to accelerate the pace of operations, protect Allied data and allow warfighters to draw on the collective strength of all 32 Allies. NATO is currently engaging with industry on both sides of the Atlantic to identify the technologies and approaches needed to deliver this capability.

Annex E - Supplement to Problem Statement – NATO Service Ownership and Operating Models

NATO currently has a number of different service ownership models in place.

Model	Ownership and operation
COCO Contractor-Owned, Contractor-Operated	The contractor owns and operates the solution under agreed service levels and NATO oversight.
CONO Contractor-Owned, NATO-Operated	The contractor owns the solution, while NATO operates it, with clearly defined supplier maintenance and support responsibilities.
NONO NATO-Owned, NATO-Operated	NATO owns and operates the solution, with supplier implementation, maintenance, and specialist support as required.

Operating Models may vary by service or environment. Classified deployments must preserve NATO operational control and meet security, accreditation, and air-gapped requirements. Note that contractor ownership does not authorize classified access or administrative privileges.

SLA Details

Current NATO SLA targets are as follows:

Priority/ Severity	Description	Response Time	Restoration Time	Resolution Time
Critical	Loss of service	1 hour	4 hours	3 calendar days
Major	Service or performance affected	4 hours	24 hours	5 calendar days
Medium	Neither service nor performance affected	1 business day	3 business days	10 calendar days

- **Response Time:** Time to begin troubleshooting, diagnostics, and remedial action.
- **Restoration Time:** Maximum time to restore service.
- **Resolution Time:** Time to provide a conclusive fix, such as a software patch or upgrade.

Service Performance and Accountability

NCIA welcomes industry recommendations that turn these targets into a practical, measurable service offering. Respondents should highlight how their approach delivers reliable performance, clear accountability, and value for NATO:

- A. **Measurement:** Define when service clocks start and stop, support hours, business-day calendars, and any proposed pause conditions requiring NCIA agreement.
- B. **Service commitments:** Recommend availability, quality, capacity, and recovery targets by service, deployment environment, and operating model.
- C. **Performance assurance:** Explain monitoring, reporting, maintenance exclusions, escalation, and corrective action. Propose remedies for missed commitments, including service credits where appropriate.
- D. **Accountability:** Distinguish end-to-end outcomes from supplier commitments and NATO responsibilities. Identify third-party dependencies and explain how performance will be verified in air-gapped environments.
- E. **Commercial options:** Present alternative service levels and their pricing, highlighting the trade-offs between cost, performance, and operational needs.

Resilience in Practice

Beyond meeting incident targets, the service must demonstrate how essential communications would continue during disruption. Respondents should address loss of:

- A. Wide-area or external connectivity;
- B. A hosting location;
- C. Identity services; and
- D. Central management or licensing services.

For each scenario, explain which local and enterprise calling—including emergency calling—conferencing, and messaging functions remain available, for how long, and with what limitations. Describe fallback, failover, and recovery arrangements, supported by a practical approach to demonstrating their effectiveness.

Final operating models and SLA commitments remain subject to requirements validation, security approval, affordability, and the acquisition strategy.